IDENTITY and ACCESS MANAGEMENT

ENABLING SARBANES-OXLEY COMPLIANCE

White Paper
July 2009

Abstract

The Sarbanes-Oxley Act of 2002 (Sarbox) has had a profound effect on businesses. This paper offers an overview of the act and its implications, reviews the role of identity and access management (IAM) in meeting the requirements of Sarbox, and highlights IAM products and services available from Sun. Additionally, a look at best practices and guidance on how to get started with IAM is provided.

Table of Contents

Chapter 1

Executive Summary

The *Sarbanes-Oxley Act of 2002* (Sarbox) was intended to make corporate governance practices more transparent and to improve investor confidence. It addressed financial control and financial reporting issues raised by the corporate financial scandals, focusing primarily on two major areas: *corporate governance and financial disclosure*.

The potential impact to public companies affected by this act include:

- Severe potential penalties in cases of non-compliance
- High financial costs to comply with regulatory requirements
- Potential diversion of executive attention as effort is focused on compliance activities rather than essential business priorities
- Potential business improvement when compliance activities contribute to more efficient business practices

Information Technology (IT) can play a major role in enabling compliance with Sarbox. IT and its related processes generate the majority of data that makes up financial reports that are critical to demonstrate the effectiveness of compliance efforts and provide assurance to executives that Sarbox requirements are being met.

Sarbox requirements for fraud reduction, policy enforcement, risk assessment and compliance auditing are supported directly by identity and access management (IAM) technology and methods. By streamlining the management of user identities and access rights, automating enforcement of segregation of duties policies, and automating time-consuming audits and reports, IAM solutions can help support strong security policies across the enterprise while reducing the overall cost of compliance.

IAM solutions from Sun Microsystems are particularly well-suited to addressing the long-term efficiency and economic viability of processes associated with Sarbox compliance. Sun offers a pragmatic approach to IAM that eschews excessive complexity in favor of simple, open, and proven technology. Sun solutions are designed specifically to enable four key components of efficient and cost-effective compliance:

1. Minimize risk
2. Automate processes
3. Prevent fraud
4. Provide comprehensive auditing and reporting

In the seven years since the passage of the Sarbox act, practical experience in the field has yielded several recommended best practices for implementing IAM systems to enable compliance. Drawing from multiple Sun white papers and other references to provide a current view of Sarbox compliance requirements, applicable technology and best practices, this document outlines best practices and recommended approaches for initiating an IAM/compliance strategy.

Chapter 2

Sarbanes-Oxley Act of 2002

Overview

In the wake of the accounting scandals of the early 2000s—including those related to Enron, WorldCom, Global Crossing, Arthur Andersen and others—the *Sarbanes-Oxley Act of 2002* (Sarbox) grew out of the premise that if corporate governance practices were made more transparent, investor confidence would be enhanced.

Signed into law on July 30, 2002, Sarbox was designed to address financial control and financial reporting issues raised by the corporate financial scandals. Sarbox focuses primarily on two major areas: *corporate governance and financial disclosure*.

The purpose of Sarbox 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.

Provisions of Sarbox detail criminal and civil penalties for noncompliance, certification of internal auditing, and increased financial disclosure requirements. Sarbox requires CEOs and CFOs of public companies to swear under oath that the financial statements they make are accurate and complete. Other areas of the act cover ethical behavior, board composition, and the independence of auditors. Senior executives are deemed personally responsible for compliance and must testify to the accuracy of their companies' accounts.

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. Since 2006, all publicly-traded companies have been required to submit an annual report of the effectiveness of their internal accounting controls to the SEC.

An over-arching *Public Company Accounting Oversight Board* (PCAOB) was also established by Sarbox. According to this organization's Web site, the PCAOB is "a private, nonprofit corporation created by the Sarbox Act of 2002 to oversee the auditors of public companies. The PCAOB was created to protect investors and the public interest by promoting informative, fair, and independent audit reports.... The PCAOB consists of five members who are appointed by the Securities and Exchange Commission."

Complying with Sarbox requires a holistic look at business and IT infrastructure, starting with financial processes and reaching back to the operational processes that promote them. Identity and Access Management (IAM) concepts and technology play a key role in enabling more cost-effective compliance with Sarbox regulations.

Compliance Requirements

When it comes to system security and the control of access to systems and applications, Sarbox is not explicitly prescriptive. However, while Sarbox does not prescribe a solution to the compliance issue, it does make clear what obligations the company is under in order to be compliant. For example, Section 404(a) of the act requires establishing "adequate internal controls" around financial reporting and its governance. These internal controls ultimately break down into a series of processes that companies must adhere to in the preparation of financial reports as well as in the protection of the financial information that goes into making the reports. This financial information must be protected as it is stored in various locations throughout the enterprise (including enterprise applications, database tools, and even accounting spreadsheets).

Current standards approved by the PCAOB require management to:

- Assess both the design and operating effectiveness of selected internal controls related to significant accounts and relevant assertions, in the context of material misstatement risks
- Understand the flow of transactions, including IT aspects, sufficient enough to identify points at which a misstatement could arise
- Evaluate company-level (entity-level) controlsthat correspond to the components of the *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) framework, which focuses on financial controls
- Perform a fraud risk assessment
- Evaluate controls designed to prevent or detect fraud, including management override of controls
- Evaluate controls over the period-end financial reporting process
- Scale the assessment based on the size and complexity of the company
- Rely on management's work based on factors such as competency, objectivity, and risk
- Conclude on the adequacy of internal controls over financial reporting

Key Sections

Sarbox is arranged into eleven titles, each divided into several sections. The sections generally considered most pertinent to IAM compliance activities are shown in the following table.

SECTION	TITLE	SUMMARY
302	Corporate Responsibilities for Financial Reports	Periodic statutory financial reports are to include certifications by the principal CEO or CFO or persons performing similar functions that: • The signing officers have reviewed the report • The report does not contain any materially untrue statements or material omission or information that could be considered misleading • The financial statements and related information fairly present the financial condition and the results in all material respects • The signing officers are responsible for establishing and maintaining internal controls, have evaluated these internal controls within the previous ninety days, and have reported on the effectiveness of the internal controls • A list of all deficiencies in the internal controls and information on any fraud that involves employees who are involved with internal activities • Any significant changes in internal controls or related factors that could have a negative impact on the internal controls Organizations may not attempt to avoid these requirements by reincorporating their activities or transferring their activities to locations outside of the United States.
401	Disclosures in Periodic Reports	Financial statements published by companies are required to be accurate and presented in a manner that does not contain incorrect statements or state materially incorrect information. These financial statements shall also include all material off-balance sheet liabilities, obligations or transactions.

SECTION	TITLE	SUMMARY
404	Management Assessment of Internal Controls	Companies are required to publish in their annual reports an "Internal Control Report" concerning the scope and adequacy of the internal control structure and procedures for financial reporting. This statement shall also assess the effectiveness of such internal controls and procedures. Any shortcomings in these controls must also be reported. The registered accounting firm shall, in the same report, attest to and report on the assessment on the effectiveness of the internal control structure and procedures for financial reporting.
409	Real Time Issuer Disclosures	Companies are required to disclose to the public, on a rapid and current basis, information on material changes in their financial condition or operations. These disclosures are to be presented in terms that are easy to understand, supported by trend and qualitative information of graphic presentations as appropriate.
802	Criminal Penalties for Altering Documents	Severe criminal penalties may apply to any one who knowingly alters, destroys, conceals, covers up, falsifies, or makes a false entry in any record or document related to disclosure of information covered by the Sarbox.
902	Attempts and Conspiracies to Commit Fraud Offenses	Any person who attempts or conspires to commit an offense will be subject to the same penalties as those prescribed for the offense.

Table of Contents

The complete table of contents from the Sarbox Act of 2002 is shown below to help provide context for the sections addressed by IAM. A common misconception is that IAM solves all Sarbox compliance issues. In reality, IAM addresses only a small part of the overall regulation.

To download the entire report in PDF format, see Sarbox Act of 2002 Report.

A navigable HTML version of the Act is available on SarbaneSarboxleySimplified.com.

TITLE XI — CORPORATE FRAUD AND ACCOUNTABILITY

Sec. 1101. Short title

Sec. 1102. Tampering with a record or otherwise impeding an official proceeding

Sec. 1103. Temporary freeze authority for the Securities and Exchange Commission

Sec. 1104. Amendment to the Federal Sentencing Guidelines

Sec. 1105. Authority of the Commission to prohibit persons from serving as officers or directors

Sec. 1106. Increased criminal penalties under Securities Exchange Act of 1934

Sec. 1107. Retaliation against informants

Chapter 3

Business Impact

Potential Noncompliance Penalties

The threat of severe civil and criminal penalties for not complying with Sarbox requirement are onerous. Noncompliance penalties range from the loss of exchange listing and loss of director and officer insurance to multimillion dollar fines and imprisonment. Such penalties and resultant media coverage can result in a lack of investor confidence. A CEO or CFO who submits a wrong certification is subject to a fine up to $1 million and imprisonment for up to ten years. If the wrong certification was submitted "willfully," the fine can be increased up to $5 million and the prison term can be increased up to twenty years.

High Financial Costs

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; 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 work flows 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.

Diversion of Executive Attention

Efforts to comply with Sarbox requirements pose a number of logistical, operational, and economic challenges for companies seeking to comply with this set of regulations. The severity of potential penalties for non-compliance may prompt executives to divert attention and resources away from from revenue generation and cost-control initiatives and toward compliance activities. This can reduce overall effectiveness of the enterprise.

Potential Business Improvement

Complying with Sarbox requires a holistic look at business and IT infrastructure, starting with financial processes and reaching back to the operational processes that promote them. Some argue that such assessment of fundamental business processes, even though forced by the threat of penalties for non-compliance, leads to systemic improvement in business efficiency.

Some CIOs are using Sarbox compliance as a launch pad for updating systems, smoothing operations, and staying ahead of the competition.

Chapter 4

The Role of IAM in Sarbox Compliance

Information Technology and Sarbox Compliance

Information Technology (IT) can play a major role in enabling compliance with Sarbox. IT and its related processes generate the majority of data that makes up financial reports critical to demonstrate the effectiveness of compliance efforts and provide assurance to executives that Sarbox requirements are being met. An effective governance and compliance program requires the prevention, detection, and remediation of fraudulent or negligent activity through internal controls. Companies must move beyond manual processes and spreadsheets and implement technology to automate and monitor critical corporate processes.

Effective deployment of IT systems and process can provide the following benefits:

- **Correct information**. IT must provide an infrastructure that can collect and present the correct important data, in a comprehensible form, from many distinct reporting systems including purchasing, sales, general ledger, etc., running on a variety of computing platforms.
- **Accurate information**. The information from such reporting systems must accurately reflect the numbers flowing through a company's transaction systems.
- **Risk Awareness**. Correct and accurate information, presented appropriately, can enable firms to assess the risks related to business processes that affect financial reporting.
- **Audit efficiency**. IT can be used to automate processes that enable Sarbox compliance, reducing manual labor requirements for collecting, evaluating and presenting data.
- **Breadth of coverage**. Automated methods can assure that controls apply uniformly to multiple applications, across multiple business units.
- **Redundancy reduction**. IT automation can reduce or eliminate redundant manual or siloed processes associated with audit compliance.
- **Error reduction**. IT automation can verify manual processes and validate key financial processes that exist solely on spreadsheets and desktops.
- **Consistency and repeatability**. IT automation can assure that the financial information presented to executives is consistent and audit procedures are repeatable from audit period to audit period, increasing executive confidence that 1) the reports they are certifying come from well-maintained, secure, and error-free software applications and processes, and 2) those processes reflect a concerted effort to streamline operations and control costs.
- **Sustainability**. By implementing work flow tracking and accountability and providing documented prevention, detection, and remediation of fraudulent or negligent activities, IT can act as an efficient watchdog across the enterprise to help confirm

that policies are being enforced and allow for sustainable compliance.

- **Business efficiency**. Any investments made toward Sarbox compliance should also improve the business and provide a return on investment (ROI). IT can add significant value in the automation of processes and controls; improvements here can result in more reliable, efficient, auditable, and sustainable enforcement of corporate policies and controls.

The Specific Role of IAM

IAM is the IT and management discipline focused on controlling user access to data, applications, networks and other resources. Sarbox requirements for fraud reduction, policy enforcement, risk assessment and compliance auditing are supported directly by IAM. By streamlining the management of user identities and access rights, automating enforcement of segregation of duties policies, and automating time-consuming audits and reports, IAM solutions can help support strong security policies across the enterprise while reducing the overall cost of compliance.

While the previous section outlines general ways IT can support compliance efforts, this section addresses specific ways that IAM technology and methods can enable Sarbox compliance. IAM provides the following key enablers:

- **Assign and control user access rights**. Securely managing the assignment of user access rights is critical to Sarbox compliance, particularly in distributed and networked environments typical of modern business. Decentralized provisioning is not only inefficient and costly, it also increases the risk of audit policy and regulatory violations. 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 or provisioning ensures regulatory compliance, thus preventing audit policy violations.
- **Enforce segregation of duties (SOD) policies**. Segregation of duties (also known as separation of duties), has as its primary objective the prevention of fraud and errors. This objective is achieved by disseminating the tasks and associated privileges for a specific business process among multiple users. Linking provisioning and auditing at the business role level is essential to complying with Sarbox rules regarding SOD or erroneous aggregation of privileges. IAM methods can prevent, detect, and resolve access rights conflicts to reduce the likelihood that individuals can act in a fraudulent or negligent manner. Once violations are identified, notification and remediation steps are automatically initiated based on corporate policies.
- **Adjust user access rights when responsibilities change**. Business risk is 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 SOD violations. Automated provisioning

effectively eliminates many of these risks, especially when combined with auditing and role management capabilities.

- **Revoke user access upon termination**. IAM systems can automate the process of immediately revoking user access rights upon termination or suspension. This eliminates a commonly-exploited security gap and opportunity for policy violation that may occur after an employee or contractor has been dismissed.
- **Provide uniform access policy**. IAM can provide administration and enforcement of common user access policies across a wide span of diverse systems, improving executive confidence in how the enterprise complies with Sarbox requirements.
- **Manage access based on business roles**. Provisioning and auditing at the business role level, rather than just at the IT access control level, ties user access rights more closely to business processes. With a role management solution, managers can approve access rights that have a meaningful business context, thus reducing the risk of managers inadvertently creating SOD violations by granting carte blanche access to their direct reports.
- **Manage allocation of user credentials**. Managing user names, passwords and other user access credentials is essential to assuring that only authorized users are granted access to information systems. IAM technology can provide enterprise-wide control of user credentials, including the enforcement of uniform password policies (e.g. password strength, periodic change).
- **Verify access rights**. While automated user access provisioning is designed to accurately assign access rights, Sarbox requires that such access rights be confirmed by audit. IAM can provide the ability to both assign access rights according to established polices and then periodically verify that access rights are still compliant with those same policies.
- **Conduct periodic compliance assessments**. Sarbox requires periodic audits of access rights and privileges. Re-certification is a process where managers approve direct reports' access to enterprise resources and applications. IAM can provide the ability to automatically present managers with the correct information to attest to each employee's access rights needs. By applying role management principles, this re-certification process can enable the approving manager to work at the business-role level, attesting to those entitlements quickly and accurately because they are given in a meaningful business context.
- **Enforce secure access policies**. While automated identity administration, provisioning and auditing are essential to Sarbox compliance, these methods don't actually enforce the use of security policies when a user accesses the controlled systems. IAM Access Management technology can enforce user access policy at the point of entry to an application or other system, in harmony with established policy. Examples of such enforcement include Web access management (including single sign-on or SSO), enterprise single sign-on (ESSO), and Web service security.
- **Provide automated reports**. Sarbox requires the delivery of accurate, timely and complete reports that executives can use to assess compliance with established

requirements. IAM can provide scheduled and ad-hoc compliance reports, including automated violation notifications, comprehensive work flow processes, and audit assessment reports. Such reports can generated across multiple systems and enterprise applications.

IAM Role in Key Sarbox Sections

The ways IAM enables compliance are mapped to key Sarbox sections in the table below.

SECTION	TITLE	IAM COMPLIANCE ENABLERS
302	Corporate Responsibilities for Financial Reports	• Provide automated reports.
401	Disclosures in Periodic Reports	• Provide automated reports.
404	Management Assessment of Internal Controls	• Assign and control user access rights. • Enforce Segregation of Duties (SOD) policies. • Adjust user access rights when responsibilities change. • Revoke user access upon termination. • Provide uniform access policy. • Manage access based on business roles. • Manage allocation of user credentials. • Verify access rights. • Conduct periodic compliance assessments. • Enforce secure access policies. • Provide automated reports.
409	Real Time Issuer Disclosures	• Conduct periodic compliance assessments. • Provide automated reports.
802	Criminal Penalties for Altering Documents	• Revoke user access upon termination. • Provide automated reports.
902	Attempts and Conspiracies to Commit Fraud Offenses	• Enforce Segregation of Duties (SOD) policies.

Sun IAM Products

IAM solutions from Sun are particularly well-suited to addressing the long-term efficiency and economic viability of processes associated with Sarbox compliance. Sun's pragmatic approach to IAM helps organizations achieve compliance by simplifying, rather than further complicating, the technology environment. The three key aspects of this approach are:

- **Simple**. Sun IAM solutions are 100% Pure Java™ technology and easy to deploy, configure, and use.
- **Open**. Open architecture makes applying Sun IAM solutions to multiple networked resources faster and simpler.
- **Proven**. Sun manages billions of user identities, and its solutions have received positive recognition from industry analysts and others.

Sun solutions are designed specifically to enable four key components of efficient and cost-effective compliance:

- Minimize risk
- Automate processes
- Prevent fraud
- Provide comprehensive auditing and reporting

A highly scalable IAM solution that combines provisioning, identity auditing, role management, and access 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.

Additional details about how the Sun IAM products enable Sarbox compliance are provided in the product-specific sections below.

Sun Identity Manager

- **Identity Administration**. Sun Identity Manager provides complete management of the identity life cycle for user identities and security credentials for all managed systems. This provides a centralized facility for uniformly administering user access rights across a broad enterprise and extending beyond the enterprise to encompass customers and partners.
- **Automated Provisioning and De-provisioning**. Sun Identity Manager can automatically assign user privileges based on roles or business rules. When a user has a change in responsibility, user access rights can be automatically changed or

revoked as occasion requires.

- **Credential Management**. Sun Identity Manager provides a complete facility for managing the assignment and maintenance of user names, passwords, or other security credentials, including uniform enforcement of password policies.
- **Complete visibility into current compliance exposures**. Sun 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**. Pre-configured 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.
- **Internet scale provisioning and identity auditing**. With Sun 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 applications and services to customers quickly, without compromising security or compliance controls. The solution has been tested in environments with millions of users.

Sun Role Manager

- **Identity Data Warehouse**. Sun Role Manager software maintains a central repository called the identity warehouse that contains all users and their access permissions or entitlements. This forms the basis for the automation of the access-certification control and the ability to answer the fundamental question of who has access to what.
- **Integrated provisioning and auditing**. 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
- **Business role provisioning and auditing**. Sun Identity Manager 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 mining and definition**. Sun Role Manager is the only role product that approaches role mining and definition from both 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. Sun Role Manager software provides for complete role life cycle management.

Sun OpenSSO Enterprise

- **Access Management.** Sun Open SSO Enterprise provides Web access management capability to centralize and enforce SSO and security policy both for internal Web applications and extranet authentication—and do so in a repeatable, scalable manner. This reduces security risk while at the same time lowering operational expenses.
- **Federation.** Sun Open SSO Enterprise enables the establishment of federated identity relationships in order to extend access and enforce security policy across domain boundaries. Support is provided for all major federation protocols, including SAML, WS-Federation, WS-Trust, WS-Security, WS-Policy, Liberty ID-FF, and WS-I BSP. Features like a multi-protocol federation hub that "translates" different federation protocols and the Fedlet, a lightweight means of implementing federation with service providers, provide flexibility and extensibility of this federation platform.
- **Web Services Security.** Web services deployment is new for many companies, and so far, little attention has been paid to securing them in a standardized, repeatable way. Security is becoming increasingly important as web services come to the forefront. From check-imaging services on retail banking Web sites to stock ticker Web services to movie listings on social networking sites, Web services are becoming ubiquitous in the networked world.
- **Scalability.** Sun Open SSO Enterprise provides Internet-scale access management and federation to extend access control and security policy enforcement to tens of millions of users beyond enterprise boundaries.

Sun Directory Server Enterprise Edition

- **Identity Repository.** Sun Directory Server Enterprise Edition (DSEE) is a high-performance, highly scalable directory for enterprise and carrier-grade environments. It includes robust security controls, including complete visibility into access requests, flexible replication capabilities for availability in distributed environments, and integrated data services, including virtualization and distribution.
- **Scalability.** DSEE provides an Internet-scale identity repository to extend access control and security policy enforcement to hundreds of millions of users beyond enterprise boundaries.
- **Security.** DSEE holds user credentials in a secure, encrypted way. The directory can provide a foundation to manage credentials and enforce password policy. An API is provided to extend controls to external management systems if desired. Credential usage can be also tracked at the directory level through multiple logs. Because of its inherent structure and replication capabilities, user credentials can be managed with the context of data privacy rules across multiple nationalities.
- **Identity Consolidation.** The Virtual Directory capability of DSEE supports the virtual consolidation of user identities from multiple repositories, thus simplifying access, streamlining operations and reducing the complexity of audit-compliance efforts.

Primary IAM Enablers

The following table outlines how the key IAM enablers are are mapped to relevant Sarbox sections, and highlights which Sun IAM products apply to each primary enabler.

SECTION	TITLE	IAM COMPLIANCE ENABLERS	SUN IAM PRODUCTS
302	Corporate Responsibilities for Financial Reports	• Provide automated reports.	• Identity Manager • Role Manager
401	Disclosures in Periodic Reports	• Provide automated reports.	• Identity Manager • Role Manager
404	Management Assessment of Internal Controls	• Assign and control user access rights • Enforce SOD policies • Adjust user access rights when responsibilities change • Revoke user access upon termination • Provide uniform access policy • Manage access based on business roles • Manage allocation of user credentials • Verify access rights • Conduct periodic compliance assessments • Trigger compre-hensive workflow processes to assess compliance • Enforce secure access policies • Provide automated reports	• Identity Manager • Role Manager • OpenSSO Enterprise • Directory Server

SECTION	TITLE	IAM COMPLIANCE ENABLERS	SUN IAM PRODUCTS
409	Real Time Issuer Disclosures	• Conduct periodic compliance assessments. • Provide automated reports.	• Identity Manager • Role Manager
802	Criminal Penalties for Altering Documents	• Revoke user access upon termination. • Provide automated reports.	• Identity Manager • Role Manager
902	Attempts and Conspiracies to Commit Fraud Offenses	• Enforce SOD policies.	• Identity Manager • Role Manager

Learn More about Sun Identity and Access Management Solutions

To find out more about the identity management products and services available from Sun, please visit sun.com/software/identity.

Chapter 5

Related Regulatory Compliance Issues

Of course, compliance involves more than just Sarbox. It also includes consideration of the interaction between multiple national, international, industry, and local regulations, as well as best practices, guidelines and frameworks, and changing legal precedents. To achieve sustainable compliance, this complex and confusing mix can be approached most effectively as a single compliance program that addresses people, processes, and technology.

Some of the other regulations that companies might need to address in their compliance programs are:

Health Insurance Portability and Accountability Act

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.

Gramm-Leach-Bliley Act

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 Sarbox and HIPAA, this requirement applies equally to information online and on paper.

State-Level Legislation

State-level legislation has also been widespread in the last few years—and 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.

Payment Card Industry Data Security Standards

The Payment Card Industry Data Security Standards (PCI DSS) is not a government regulation, but a worldwide security standard assembled by the Payment Card Industry Security Standards Council. It was created to help organizations prevent credit card fraud, hacking, and other security vulnerabilities. The key objectives for PCI DSS are:

- Protect cardholder data
- Secure systems and access
- Track and monitor all network resources and cardholder data

International Traffic in Arms Regulations

International Traffic in Arms Regulations (ITAR) require companies that supply products to the U.S. Federal Government to know if people accessing sensitive data are U.S. citizens or foreigners. They must know where the data is being accessed from at any time (inside the U.S. or outside). They must know the combination of who is accessing (US citizen or not) and where they are accessing the data. This applies to all data: data at rest on a server, data in motion like emails, data at end-points like on a laptop or thumb drive. They need to restrict access to all this data for not only the employees and contractors, but any supplier that is supplying components and suppliers that may be supplying product to the suppliers.

Access Control must extend to:

- Employees
- Internal IT
- Program Partners/Suppliers
- Customers who have access to systems
- IT vendors

Chapter 6

Best Practices for the IAM/Compliance Journey

In the seven years since the passage of the Sarbox act, practical experience in the field has yielded several recommended best practices for implementing IAM systems to enable Sarbox compliance. We recommend the following:

1. **Understand requirements**. By developing a better understanding of compliance requirements, how compliance affects IT, and how IT in general and IAM specifically can help support governance and compliance, companies can establish efficient, cost-effective, and sustainable programs that address all of these complex requirements within a holistic compliance framework.

2. **Recognize IT's critical role**. In many companies, IT has evolved to become the critical backbone behind almost every operation, but many people still view technology as a cost rather than an investment or asset. By understanding the key roles that IT plays in support of compliance, enterprises can maximize the value of their technology investment.

3. **Understand the role of IAM**. IAM plays a critical role in compliance with Sarbox requirements, particularly in the areas of minimizing risk, automating processes, prevent fraud and providing comprehensive auditing and reporting. However, it does not automatically satisfy all Sarbox requirements. Recognizing the value and the limitations of IAM in the entire spectrum of Sarbox compliance is essential.

4. **Think program, not project**. Sarbox compliance is a journey, not a short-term event. Companies must begin to approach compliance as a long-term program, not a single project. An effective and holistic compliance program should also incorporate governance and risk management. Boards of directors and executives are frequently being held to higher standards than ever before as they are expected to be knowledgeable about, and held liable for, everything going on within the enterprise.

5. **Develop a strategy**. The only way to effectively address the wide spectrum of compliance requirements is to integrate them into a common compliance strategy that is intertwined with the business itself. A business-driven, risk-based, and technology-enabled compliance strategy can help create enterprise value by rationalizing unnecessary complexities, driving consistency and accountability across the enterprise, and identifying opportunities for a possible enhancement of operational performance and information quality.

6. **Establish a governance process**. Compliance efforts affect a broad spectrum of an enterprise. Stakeholders from many organizations, often with conflicting priorities, have vested interests in the outcomes of a compliance strategy. The

governance process must provide representation from the impacted functional areas of the organization. A governance board should have appropriate representation from IT, security, audit, application owners, human resources, and business process owners. The board should be accountable for the project objectives and be vested with authority to make program decisions. The board should be empowered to:

- Establish a statement of purpose for the program
- Promote and give visibility to the program throughout the larger organization
- Act as a mechanism for quickly making decisions regarding program scope, issues, and risks
- Monitor the program health on an ongoing basis

7. **Implement your strategy in phases**. By segmenting the overall solution into manageable parts, an organization can realize quick, visible business benefits and progressively realize overall program objectives in an orderly, measurable way. Implementing in manageable phases also makes it easier to battle issues such as scope creep or requirements drift.

8. **Give real-time visibility**. Real-time views into the functioning of controls across these systems and across the enterprise, through job-specific dashboards or portal views, can provide insight into compliance status, progress, and risks. Effective communications with all stakeholders is essential.

9. **Unify disparate compliance efforts**. Many companies are beginning to realize the potential of technology to support sustained compliance and are actively looking to combine existing fragmented, reactive, and inefficient governance and compliance efforts into a single sustainable compliance program. Bringing together compliance, governance, and risk management under a holistic framework can result in a centralized compliance organization with the understanding, structure, and ability to help optimize the company's compliance efforts in a sustainable, strategic, and cost-effective manner.

10. **Assess progress and adjust as necessary**. Each phase of the progressive implementation of the compliance strategy will yield more in-depth understanding about the compliance process as it pertains to the specific enterprise. Implementing methods of continual process improvement will yield progressively refined results.

Chapter 7

How to Get Started with Sarbox and IAM

The previous section addressed the general best practices for implementing IAM to address Sarbox compliance. Some questions may remain: "How do I get started? How does this really apply to my company? What must I do to take the first step?"

We recommend the following pragmatic steps to getting started with a Sarbox compliance and IAM strategy.

1. **Understand the landscape.** Take the time to understand how Sarbox and other regulations apply to your company, how IT can help you comply with those regulations, and how IAM plays a critical a role in the compliance process. Seek to understand how Sarbox compliance will be a journey, not a short-term project for your company. Armed with this knowledge, you will be able to outline just what your company must do to comply.

2. **Assess where you are.** Review what progress you have made to date.

   - Do you have IAM and compliance plans and projects in place?
   - Where are you on the road to completion?
   - What has worked for you?
   - What improvements do you need to make?
   - What areas need the most emphasis?

   Answering these questions will allow you to set priorities and outline a strategy that will work for your company. Using Sun Professional Services to conduct an Identity Management Workshop for your company as outlined in the next section is an excellent way to help you answer these questions.

3. **Set specific, measurable objectives.** Based on your understanding of Sarbox requirements and a knowledge of where your company is on the compliance journey, you should set specific objectives that can be achieved in a phased approach. This will enable you to assess progress against short-term, measurable goals, not long-term, broadly stated intentions.

4. **Outline your strategy.** Define specifically how your company will progressively accomplish the objectives you set. Subdivide the overall program into short, meaningful projects or phases that will allow you to show progress on a regular basis and make appropriate adjustments as you go along. Outline a road map, such as the one illustrated below, for your IAM/compliance journey.

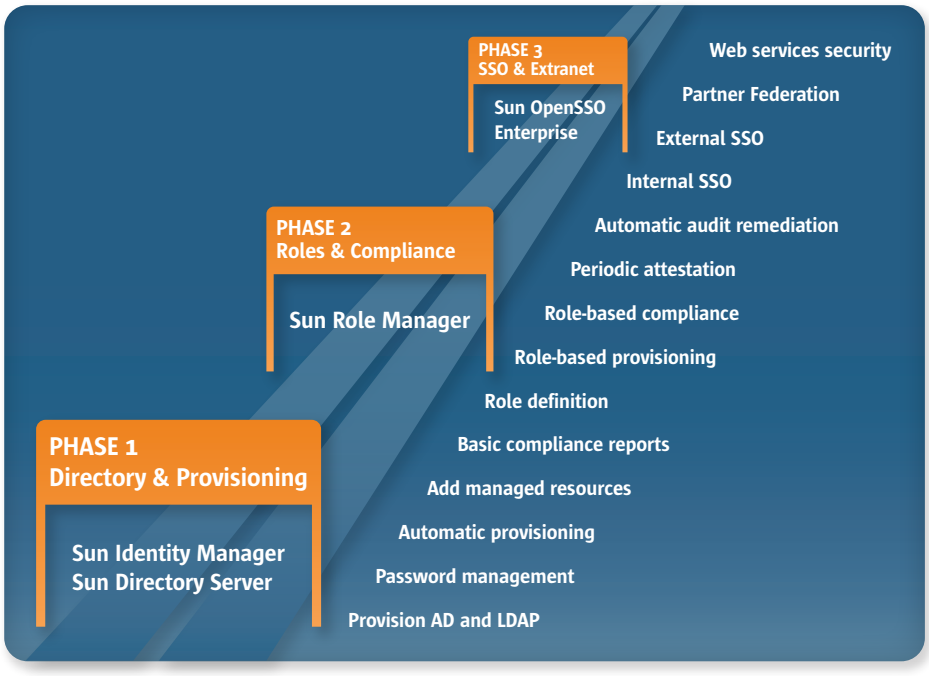

Figure 1. Plan IAM Implementation in Phases.

This diagram is only an illustration of the need to plan IAM deployment in phases. The sequence and content of phases is highly dependent on individual company objectives and requirements

5. **Lay a foundation.** Build a basic infrastructure for IAM upon which a complete IAM system can be built. For example, in the preceding diagram, projects to establish a unified directory infrastructure and automated provisioning lay a solid foundation upon which to implement role-based provisioning and automated audit control remediation.

6. **Implement "quick wins".** Implement functionality first that allows you to gain business value quickly, demonstrate the effectiveness of the IAM foundation you laid, and secure ongoing support for the IAM/Compliance strategy. Success in these early stages will provide insight and experience that will make succeeding phases easier to implement.

7. **Adjust the plan, but stay the course.** As you proceed through the IAM/compliance journey, your business and external forces affecting your business will change. Take the time to assess your progress in light of these changing conditions and adjust your strategy and overall road map as necessary. Don't give up. Work for the real business benefits (not just penalty avoidance) that can come from a well-implemented IAM/compliance strategy.

Chapter 8

The Sun IAM Workshop

As explained in the previous section, a key step in starting the IAM/compliance journey is assessing where your company is right now as a precursor to setting specific objectives and outlining a strategy.

The Sun Identity Management Workshop, a standard service offered by Sun Professional Services, can help you do such an assessment. This service offering helps you to assess your current situation and begin to establish a strategy and roadmap for your IAM/compliance program. It is typically performed within three to four business weeks, or longer for complex projects. Sun Professional Services consultants work with your organization onsite for 9 days if your identity management projects are with 1,000 user configurations or more, and 6 days for projects with fewer than 1,000 user configurations. A few days after the workshop, Sun consultants will provide a workshop report,and discuss relevant best practices and proven methodologies with your staff.

The workshop incorporates best practices, identifies potential pitfalls, and leverages Sun's proven strategies for mitigating risks associated with complex enterprise identity management projects. The service can identify potential technical and business risks involved with an identity management implementation. It is designed to:

- Provide a short engagement that's focused on educating your staff on Sun's identity management best practices
- Increase the probability of project success by teaching best practices and identifying red flags specific to your project
- Provide architectural oversight for your identity management project, whether or not you utilize Sun's delivery organization
- Deliver a service for all appropriate Sun Java™ Identity Management customers, regardless of implementation provider (Sun, partner, or customer)

The Basic Process

Pre-project Workshop

First, Sun collaborates with you to conduct a pre-project workshop at your location. Sun consultants apply our proven delivery methodology, which segments the project into a sequence of well-scoped, well-defined, achievable, measurable efforts to align with your business needs and associated technical objectives. You'll learn about Sun's best practices and delivery methodology for identity management projects, as well as some common identity management project implementation pitfalls. Once the pre-project workshop is completed, you'll receive an assessment and validation of the overall high-level approach and feasibility of the proposed solution.

Workshop Report

During the next step, Sun Professional Services consultants create an IAM Workshop Report that encapsulates the information derived from multiple collaborative sessions between Sun and key business and technical counterparts in your organization. The workshop report outlines common goals and objectives for the IAM deployment and provides the foundation for subsequent deliverables.

Program Road Map

Sun also provides you with a program road map that describes a recommended approach to the next steps of your IAM deployment. The road map is developed based on the application of Sun's proven identity management deployment methodology, which has been repeated in numerous deployment engagements. You also receive hardware sizing information for your specific project.

Collaboration with Partners

Sun consultants can collaborate with Sun certified specialty partners who are accredited to maximize the success of enterprise identity management solutions. By aligning with Sun, partners can help effectively set up identity management projects, reduce exposure to risk, and provide architectural oversight for your identity management projects. The following section highlights a few of the partners we work with.

For more information on the Getting Started with Sun Identity Management Workshop, see sun.com/service/identityworkshop.

Chapter 9

Case Studies

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

Sun-on-Sun: Improving Compliance and Efficiency

Like any public company operating today, Sun must comply with Sarbox on an ongoing basis, including having sufficient controls on the monitoring and enforcement of user access to critical business applications and systems.

These expectations include enforcement of segregation of duties, minimizing the distribution of superuser privileges, and having managers conduct periodic access reviews of user entitlements. Such requirements are a must-have for complying with Sarbox, in addition to bringing value to the organization through improved operational efficiency, decreased risk for fraud, and cost reductions that can result from streamlined management of user entitlements.

Sun Microsystems, in coordination with systems integrator Deloitte & Touche, deployed products from the Sun IAM portfolio to address Sarbox compliance, specifically with regard to reducing excessive access and enforcing segregation of duties among end users. The goal was threefold:

1. Prevent conflicts of interest
2. Protect the security and privacy of sensitive application information
3. Maintain the integrity of transactions

To manage regulatory compliance and improve operational efficiency, Sun defined the following parameters for a technology solution. The solution had to:

- Accelerate the processes for provisioning users (for example, adding new access and removing access) when their roles within the organization change. This would reduce the potential risk for excessive or inappropriate access and enable greater operational efficiencies.
- Establish a single, centralized point of control over user access to resources, and provide a single view into that access to facilitate compliance.
- Be operable across disparate systems to enable extending the solution to support additional systems.
- Offer ease of deployment into the Oracle 10.7 system and other legacy systems with no system reconfiguration, new APIs, or additional software. This would minimize the investment and time required to implement the solution.
- Enable managers and application owners to conduct periodic access and

certification reviews.

- Be able to automate the process of remediation, collaboration, and escalation to resolve potential segregation-of-duties conflicts.
- Perform checks proactively for potential segregation-of-duties conflicts and excessive superuser access.
- Provide reports for managers, administrators, and executives.

Project Architecture

The following diagram illustrates Sun's implementation of provisioning and compliance software.

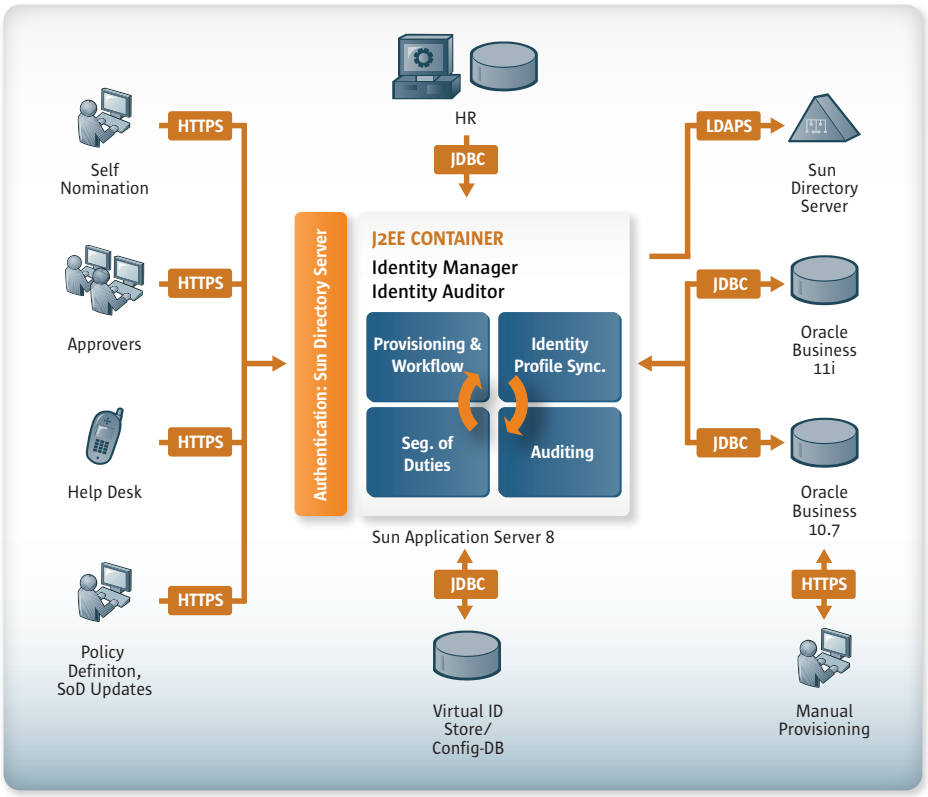

Figure 2. Sun Identity Management Architecture

Provisioning requests for Oracle 11i and Oracle 10.7 resources coming in from multiple sources are automatically checked for potential segregation-of-duties conflicts before the requests are granted. HR identity information is updated in near real-time instead of in batch process, dramatically improving the speed and efficiency with which provisioning requests can be granted.

Today, this deployment of Sun IAM software enables Sun to manage 50,000 user identities in 160 countries and plays an important role in Sun's compliance with Sarbox. In addition, the deployment successfully addresses costly inefficiency issues associated with provisioning resources for Sun users.

Benefits to Sun and Sun Customers

The following diagram illustrates Sun's implementation of provisioning and compliance software.

Sun end users and management. With this deployment of Sun software for provisioning and auditing, Sun achieved its goals for compliance and efficiency.

Compliance. The Sun Identity Manager software is now making it possible to easily prevent and detect compliance violations among end users—violations that could have been overlooked if provisioning and auditing processes continued to be conducted manually. Now, the person responsible for approving a provisioning request immediately receives a full analysis that shows whether approval will violate segregation-of-duties controls. This is the result of the identity management solution providing comprehensive visibility into user access privileges whenever access requests are submitted. Users are also automatically deprovisioned from the Oracle applications whenever their employment terminates or if they fail to use the application within any six-month period.

Efficiency. Sun is now seeing faster update cycles when changes are made to end users' identity data. Changes take effect in the enterprise directory in 10 to 20 minutes, and frequently in less time. For those who are responsible for reviewing and approving access requests, the process takes two or three minutes instead of 15 minutes. The implementation also enables greater efficiency, enabling employees to get up and running with new responsibilities more quickly—and it greatly reduces the risk of human error in the process.

Sun customers and prospective customers. Post-project review is a formal part of Deloitte & Touche's IAMethods methodology. After all deliverables have been completed, Deloitte & Touche and Sun personnel involved with the deployment took stock to determine lessons learned and to capture best practices resulting from this deployment. This practice can result in significant benefits for current and future customers.

For more information, see Sun Microsystems Sun-on-Sun Case Study: *Improving Compliance and Efficiency with Sun Identity Auditing and Other Sun Identity Management Capabilities*, January 2008 (.pdf).

Other Examples

The following describe Sarbox challenges faced by Sun customers.

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 Sarbox, 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 Sarbox 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 Sarbox auditor doing a routine review of access, thus putting the company at risk for failing the audit and being charged with violating Sarbox 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 Sarbox requirements requiring SOD and prohibiting erroneous aggregation of privileges.

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.

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 de-provisions 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. Now, when someone leaves the benefits area of HR to join another department, that employee's HR benefits role are de-provisioned and a new role is assigned based on the new job.

Chapter 10

References

The following sources were used in preparation of this white paper and can provide additional background and insight into this subject.

1. Sarbanes-Oxley Act of 2002 (.pdf)
2. Sun Microsystems White Paper: The Role of Identity Management in Sarbanes-Oxley Compliance, October 2004 (.pdf)
3. Sun Microsystems White Paper: Role Management: The Key to Cost Effective Compliance and Provisioning, May 2008 (.pdf)
4. Sun Microsystems Sun-on-Sun Case Study: Improving Compliance and Efficiency with Sun Identity Auditing and Other Sun Identity Management Capabilities, January 2008 (.pdf)
5. Discover the Hidden Benefits of Sarbanes-Oxley January 2006 (Sun Web site article)
6. Case Study: Building Acceptance and Adoption of COBIT at Sun Microsystems 2005 (ISACA Web site article)
7. Sun Microsystems and Deloitte White Paper: Raising the Bar for Governance and Compliance—Understanding, Aligning, and Realizing Your Technology's Capabilities February 2006 (.pdf)
8. Getting PCI DSS Compliance Right: How Identity Management can help secure information access (.pdf)
9. Public Company Accounting Oversight Board (website)
10. Sarbanes-Oxley 101—Info Guide to the Sarbanes-Oxley Act of 2002 (website)
11. A Guide to the Sarbanes-Oxley Act (website)
12. Sarbanes-OxleySimplified.com (website)
13. Wikipedia—Sarbanes-Oxley Act (website article)
14. Getting Started with Sun Identity Management Workshop (website)
15. Sun Identity and Access Management Software (website)
16. Deloitte Enterprise Role Lifecycle Management (.pdf)
17. Accenture Solution for Control and Compliance (.pdf)
18. About the COSO Framework: Background and Essential Facts (website)
19. SOX-online: The Vendor-Neutral Sarbanes-Oxley Site (website)
20. International Traffic in Arms Regulations 2008 (website)

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA Phone 1-650-960-1300 or 1-800-555-9SUN (9786) Web sun.com

Printed in USA 07/09 #562889