An Oracle White Paper
March 2010

Identity and Access Management: Enabling Sarbanes-Oxley Compliance

ORACLE

Executive Overview

The Sarbanes-Oxley Act of 2002 (SOX) made corporate governance practices more transparent in an effort to improve investor confidence. IT can play a major role in enabling compliance with SOX. IT and its related processes generate the majority of the data that makes up the financial reports that are critical to demonstrate the effectiveness of compliance efforts and provide assurance to executives that the organization is meeting SOX requirements. Identity and access management (IAM) technology and methods provide direct support for the SOX requirements for fraud reduction, policy enforcement, risk assessment, and compliance auditing. Oracle offers a pragmatic approach to IAM that eschews excessive complexity in favor of simple, open, and proven technology.

Introduction

SOX addressed financial control and financial reporting issues raised by corporate financial scandals by focusing primarily on two major areas: corporate governance and financial disclosure. The potential impacts to public companies include

- Severe potential penalties in cases of noncompliance
- 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

By streamlining the management of user identities and access rights, automating enforcement of segregation of duties (SoD) 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 Oracle are particularly well suited to address the long-term efficiency and economic viability of processes associated with SOX compliance. The design of Oracle solutions enables four key components of efficient and cost-effective compliance:

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

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

Sarbanes-Oxley Act of 2002

In the wake of the accounting scandals of the early 2000s—including those related to Enron, WorldCom, Global Crossing, and Arthur Andersen—SOX grew out of the premise that if corporate governance practices were made more transparent, investor confidence would be enhanced.

The purpose of SOX 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.

SOX provisions detailed criminal and civil penalties for noncompliance, certification of internal auditing, and increased financial disclosure requirements. SOX 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. Deemed personally responsible for compliance, senior executives must testify to the accuracy of their companies' accounts.

This legislation affects every publicly traded company, big or small, domestic or foreign, that has registered under the Securities Exchange Act of 1934 or has a pending registration statement under the Securities Act of 1933. Failure to comply with SOX 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 U.S. Securities and Exchange Commission (SEC).

SOX also established the overarching Public Company Accounting Oversight Board (PCAOB). The PCAOB is a private nonprofit corporation created to oversee the auditors of public companies. The PCAOB protects investors and the public interest by promoting informative, fair, and independent audit reports.

The PCAOB consists of five members appointed by the SEC. Complying with SOX requires a holistic look at business and IT infrastructure, starting with financial processes and reaching back to the operational processes that promote them. IAM concepts and technology play a key role in enabling more cost-effective compliance with SOX regulations.

Compliance Requirements

When it comes to system security and the control of access to systems and applications, SOX is not explicitly prescriptive. However, although SOX does not prescribe a solution to the compliance issue, it does make clear what obligations the company is under 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 is stored in various locations throughout the enterprise, including enterprise applications, database tools, and even accounting

spreadsheets. To protect this information, 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) controls that 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

Eleven titles make up SOX, each divided into several sections. Several of these sections are the most pertinent to IAM and compliance activities, as illustrated in Table 1.

TABLE 1. THE SECTIONS MOST CLOSELY ASSOCIATED WITH IDENTITY AND ACCESS MANAGEMENT AND COMPLIANCE ACTIVITIES

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.
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. Companies must report any shortcomings in these controls. 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 must be 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 Sarbanes-Oxley.
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.

Sarbanes-Oxley Table of Contents

A look at the complete table of contents from SOX provides context for the sections addressed by IAM. A common misconception is that IAM solves all SOX compliance issues. In reality, IAM addresses only a small part of the overall regulation.[1]

Title I—Public Company Accounting Oversight Board

Sec. 101. Establishment; administrative provisions

Sec. 102. Registration with the Board

Sec. 103. Auditing, quality control, and independence standards and rules

Sec. 104. Inspections of registered public accounting firms

Sec. 105. Investigations and disciplinary proceedings

Sec. 106. Foreign public accounting firms

[1] To download the entire SOX report in PDF format, go to pcaobus.org/About/History/Documents/PDFs/Sarbanes_Oxley_Act_of_2002.pdf.

Sec. 107. Commission oversight of the Board

Sec. 108. Accounting standards

Sec. 109. Funding

Title II—Auditor Independence

Sec. 201. Services outside the scope of practice of auditors

Sec. 202. Preapproval requirements

Sec. 203. Audit partner rotation

Sec. 204. Auditor reports to audit committees

Sec. 205. Conforming amendments

Sec. 206. Conflicts of interest

Sec. 207. Study of mandatory rotation of registered public accounting firms

Sec. 208. Commission authority

Sec. 209. Considerations by appropriate State regulatory authorities

Title III—Corporate Responsibility

Sec. 301. Public company audit committees

Sec. 302. Corporate responsibility for financial reports

Sec. 303. Improper influence on conduct of audits

Sec. 304. Forfeiture of certain bonuses and profits

Sec. 305. Officer and director bars and penalties

Sec. 306. Insider trades during pension fund blackout periods

Sec. 307. Rules of professional responsibility for attorneys

Sec. 308. Fair funds for investors

Title IV—Enhanced Financial Disclosures

Sec. 401. Disclosures in periodic reports

Sec. 402. Enhanced conflict of interest provisions

Sec. 403. Disclosures of transactions involving management and principal stockholders

Sec. 404. Management assessment of internal controls

Sec. 405. Exemption

Sec. 406. Code of ethics for senior financial officers

Sec. 407. Disclosure of audit committee financial expert

Sec. 408. Enhanced review of periodic disclosures by issuers

Sec. 409. Real time issuer disclosures

Title V—Analyst Conflicts of Interest

Sec. 501. Treatment of securities analysts by registered securities associations and national securities exchanges

Title VI—Commission Resources and Authority

Sec. 601. Authorization of appropriations

Sec. 602. Appearance and practice before the Commission

Sec. 603. Federal court authority to impose penny stock bars

Sec. 604. Qualifications of associated persons of brokers and dealers

Title VII—Studies and Reports

Sec. 701. GAO study and report regarding consolidation of public accounting firms

Sec. 702. Commission study and report regarding credit rating agencies

Sec. 703. Study and report on violators and violations

Sec. 704. Study of enforcement actions

Sec. 705. Study of investment banks

Title VIII—Corporate and Criminal Fraud Accountability

Sec. 801. Short title

Sec. 802. Criminal penalties for altering documents

Sec. 803. Debts nondischargeable if incurred in violation of securities fraud laws

Sec. 804. Statute of limitations for securities fraud

Sec. 805. Review of Federal Sentencing Guidelines for obstruction of justice and extensive criminal fraud

Sec. 806. Protection for employees of publicly traded companies who provide evidence of fraud

Sec. 807. Criminal penalties for defrauding shareholders of publicly traded companies

Title IX—White-Collar Crime Penalty Enhancements

Sec. 901. Short title

Sec. 902. Attempts and conspiracies to commit criminal fraud offenses

Sec. 903. Criminal penalties for mail and wire fraud

Sec. 904. Criminal penalties for violations of the Employee Retirement Income Security Act of 1974

Sec. 905. Amendment to sentencing guidelines relating to certain white-collar offenses

Sec. 906. Corporate responsibility for financial reports

Title X—Corporate Tax Returns

Sec. 1001. Sense of the Senate regarding the signing of corporate tax returns by chief executive officers

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

Business Impact

Because of the potential penalties and costs associated with noncompliance, as well as the business benefits and protections associated with compliance, some organizations are using SOX compliance as a launchpad for updating systems, smoothing operations, and staying ahead of the competition.

Potential Noncompliance Penalties

The threats of severe civil and criminal penalties for not complying with SOX requirements 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 the ensuing media coverage can result in a lack of investor confidence. A CEO or CFO who submits a wrong certification is subject to a fine of up to US$1 million and imprisonment of up to 10 years. Submitting the wrong certification "willfully," can result in a fine increase of up to US$5 million and an increase of up to 20 years in the prison term.

High Financial Costs

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

much good has come from the new regulations dictated by SOX, corporate cleanup and compliance has come at a cost. For public companies, the costs associated with compliance do not seem to be declining with time.

Why is the cost of compliance so high? Tighter regulations, 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 when done manually. These costs only worsen in larger organizations.

A robust IAM and role management solution can mitigate and reduce costs. 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 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 SOX 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 noncompliance could prompt executives to divert attention and resources away from revenue generation and cost control initiatives and toward compliance activities. This could reduce the overall effectiveness of the enterprise.

Potential Business Improvement

Complying with SOX 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 noncompliance, leads to systemic improvement in business efficiency.

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

The Role of Identity and Access Management in Sarbanes-Oxley Compliance

IT can play a major role in enabling compliance with SOX. IT and its related processes generate the majority of data compiled in the financial reports critical to demonstrating the effectiveness of compliance efforts and providing assurance of compliance to executives. 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, and general ledger, 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 allow firms to assess the risks related to business processes that affect financial reporting.
- **Audit efficiency.** IT can automate processes that enable SOX compliance, reducing manual labor requirements for collecting, evaluating, and presenting data.
- **Breadth of coverage.** Automated methods can ensure 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 ensure 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 workflow 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 the enforcement of policies and allow for sustainable compliance.

- **Business efficiency.** Any investments made toward SOX compliance can also improve the business and provide an 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 Identity and Access Management

IAM is the IT and management discipline focused on controlling user access to data, applications, networks, and other resources. IAM directly supports SOX requirements for fraud reduction, policy enforcement, risk assessment, and compliance auditing. By streamlining the management of user identities and access rights, automating enforcement of SoD 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.

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

- **Assign and control user access rights.** Securely managing the assignment of user access rights is critical to SOX compliance, particularly in distributed and networked environments typical of modern business. Decentralized provisioning is not only inefficient and costly, but it also increases the risk of audit policy and regulatory violations. Automated provisioning allows for 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.
- **Enforce segregation of duties policies.** Segregation of duties (SoD), also known as separation of duties, has as its primary objective the prevention of fraud and errors. Disseminating the tasks and associated privileges for a specific business process among multiple users achieves this objective. Linking provisioning and auditing at the business role level is essential to complying with SOX 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. The identification of violations automatically initiates the notification and remediation steps, based on corporate policies.
- **Adjust user access rights when responsibilities change.** Business risk is introduced when employees change jobs and access is not 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 can occur after the dismissal of an employee or contractor.

- **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 SOX 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 full access to their direct reports.
- **Manage allocation of user credentials.** Managing usernames, passwords, and other user access credentials is essential to ensuring that only authorized users have access to information systems. IAM technology can provide enterprisewide control of user credentials, including the enforcement of uniform password policies (for example, password strength, periodic changes).
- **Verify access rights.** Although the design of automated user access provisioning accurately assigns access rights, SOX requires that an audit confirm such access rights. 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.** SOX requires periodic audits of access rights and privileges. Recertification 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 recertification process can allow the approving manager to work at the business role level, quickly and accurately attesting to those entitlements given in a meaningful business context.
- **Enforce secure access policies.** Although automated identity administration, provisioning, and auditing are essential to SOX compliance, these methods do not actually enforce the use of security policies when a user accesses the controlled systems. IAM 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, enterprise single sign-on, and Web services security.
- **Provide automated reports.** SOX 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 workflow processes, and audit assessment reports. The generation of such reports occurs across multiple systems and enterprise applications.

The Role of Identity and Access Management in Key Sarbanes-Oxley Sections

IAM solutions from Oracle are particularly well suited to address the long-term efficiency and economic viability of processes associated with SOX compliance.

TABLE 2. KEY SARBANES-OXLEY SECTIONS MAPPED TO THE IDENTITY AND ACCESS MANAGEMENT ENABLERS

SECTION	TITLE	IDENTITY AND ACCESS MANAGEMENT AND 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 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 SoD policies.

Identity and Access Management Products from Oracle

Oracle'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

- **Comprehensive, best-in class solutions.** Oracle leads the industry with award-winning identity management offerings that constitute the most comprehensive solution offered by any vendor. Not only do customers get a complete end-to-end solution, but they also benefit from proven best-in-class functionality.
- **Hot pluggable.** Oracle's IAM solutions are built on open standards technology and are, therefore, easy to deploy, configure, and use. The open architecture ensures interoperability with all major systems for enterprisewide security.
- **Service-oriented security.** Oracle's industry-leading approach of modular identity services, which can be consumed centrally by all applications, means that developers can now seamlessly weave security into their applications, enabling rapid time to market and increased business agility.

Oracle designs solutions 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 of the intrinsic length of the provisioning process and the compliance process, a converged solution makes it possible to consolidate centralized provisioning with compliance checking, enabling prevention and not just detection. Role management provides the additional layer necessary for the provisioning and auditing processes, leading to increased efficiencies and greater controls over users' access.

The following product-specific subsections offer additional details about how the Oracle IAM products enable SOX compliance.

Oracle Identity Administration Solution

Oracle Identity Manager provides role-based user provisioning, allowing customers to use business roles for both identity lifecycle management and identity auditing across enterprise and extranet environments.

- **Identity administration.** Oracle Identity Manager provides complete management of the identity lifecycle 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 deprovisioning.** Oracle 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.** Oracle Identity Manager provides a complete facility for managing the assignment and maintenance of usernames, passwords, or other security credentials, including uniform enforcement of password policies.
- **Internet scale provisioning and identity auditing.** With Oracle 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. Oracle Identity Manager's scalability is proven across multiple customer examples.

Oracle Identity and Access Governance Solution

Oracle Identity Analytics provides comprehensive role governance and identity compliance capabilities to streamline operations, enhance compliance, and reduce costs.

- **Identity Warehouse.** The Oracle Identity Analytics Identity Warehouse is a central repository 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.** Oracle Identity Analytics, combined with Oracle Identity Manager technology, is the only truly integrated solution that addresses provisioning and auditing at the business role level. Its capabilities specifically allow companies to meet three major business objectives: compliance, cost control, and automated provisioning.
- **Business role auditing and impact analysis**. Oracle Identity Analytics enables auditing and analytics at the business role level, enforcing compliance and providing greater insights and controls over the identity auditing processes. Integration with Oracle Identity Analytics ensures Oracle Identity Manager can consume predefined roles that are functional for provisioning and auditing.
- **Complete visibility into current compliance exposures.** Oracle Identity Analytics' compliance dashboard displays a summary view of compliance metrics at all times and 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 Oracle Identity Analytics. In addition, the solution provides reports on policy violations (like SoD), remediation, and exceptions, and enables custom reports of audit data.

Oracle Access Management Solutions

Oracle provides the industry's most comprehensive set of access management solutions for securing applications, data, digital assets, Web services or service-oriented architecture (SOA), and cloud-based services. Oracle offers the following key solutions in access management:

- **Web access management.** Oracle Access Manager provides Web access management capability to centralize and enforce single sign-on and security policy for both internal Web applications and extranet authentication—and in a repeatable, scalable manner. This reduces security risk while at the same time lowering operational expenses.
- **Federation.** Oracle Identity Federation with Fedlet enables the establishment of federated identity relationships to extend access and enforce security policy across domain boundaries. Provided support is available for all major federation protocols, including Security Assertions Markup Language (SAML), Web Services (WS)-Federation, WS-Trust, WS-Security, WS-Policy, Liberty Identity Federation Framework, and WS-Interoperability Basic Security Profile. Features like a multiprotocol 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.** Oracle Web Services Manager is to Web services what Oracle Access Manager is to Web applications. Oracle Web Services Manager is designed to protect access to multiple types of resources, including standards-compliant Web services (Java Platform, Enterprise Edition [Java EE]; Microsoft .NET; PL/SQL); SOA composites, including BPEL and enterprise service bus processes; and Oracle WebCenter's remote portlets.
- **Security Token Service.** A Security Token Service (STS) establishes a trust relationship between online partners through Web services. The STS provides both standard (for example, SAML, Kerberos) and proprietary (for example, Oracle's PeopleSoft and Oracle's Siebel) security token issuance, validation, and exchange. The STS is part of Oracle Identity and Access Management Suite Plus and Oracle Access Management Suite Plus.
- **Enterprise access control.** Oracle Enterprise Single Sign-On Suite is a Microsoft Windows desktop-based suite of products providing unified authentication and single sign-on to both thick- and thin-client applications, with no modification required to existing applications. Using Oracle Enterprise Single Sign-On Suite, enterprise users benefit from single sign-on to all of their applications, whether users are connected to the corporate network, traveling away from the office, roaming between computers, or working at a shared workstation.
- **Entitlements management.** Oracle Entitlements Server is a fine-grained authorization engine that externalizes, unifies, and simplifies the management of complex entitlement policies. Oracle Entitlements Server secures access to application resources and software components (such as URLs, Enterprise JavaBeans, and Java Server Pages) as well as arbitrary business objects (such as customer accounts or patient records in a database). Oracle Entitlements Server provides a centralized administration point for complex entitlement policies across a diverse range of business and IT systems.
- **Strong authentication and fraud prevention.** Oracle Adaptive Access Manager provides resource protection through real-time fraud prevention, software-based multifactor authentication, and unique authentication strengthening. Oracle Adaptive Access Manager consists of two primary components that together create one of the most powerful and flexible weapons in the war against fraud. Adaptive Strong Authenticator provides multifactor authentication and protection mechanisms for sensitive information such as passwords, tokens, account numbers, and other credentials. Adaptive Risk Manager provides real-time and offline risk analysis and proactive actions to prevent fraud at critical log-in and transaction checkpoints.

Oracle Directory Services Solutions

Oracle Directory Services provides identity virtualization, storage, and synchronization services for high-performance enterprise and carrier-grade environments.

- **Hot pluggable.** Oracle Directory Server Enterprise Edition offers best-of-breed Lightweight Directory Access Protocol (LDAP)–based services recommended for heterogeneous applications and multivendor environments.

- **Completely integrated.** Oracle Internet Directory provides Oracle Fusion Middleware components, Oracle Fusion applications, and in-house enterprise applications with a highly scalable LDAP-based mechanism for storing and accessing identity data such as user credentials (for authentication), access privileges (for authorization), and profile information.
- **Virtual synchronization.** Oracle Virtual Directory is designed to provide real-time identity aggregation and transformation, without data copying or data synchronization. Oracle Virtual Directory hides the complexity of underlying data infrastructures by providing industry-standard LDAP and XML views of existing enterprise identity information, without moving data from its native location.

Oracle Platform Security Services

Oracle Platform Security Services provides enterprise product development teams, systems integrators, and independent software vendors with a standards-based, portable, integrated, enterprise-grade security framework for Java Platform, Standard Edition (Java SE) and Java EE applications. Oracle Platform Security Services insulates developers from the intricacies of tasks not directly related to application development by providing an abstraction layer in the form of standards-based application programming interfaces. Oracle Platform Security Services is the security foundation for Oracle Fusion Middleware: all Oracle Fusion Middleware 11*g* components and Oracle Fusion applications "consume" the Oracle Platform Security Services framework's services.

Primary Identity and Access Management Enablers

Table 3 maps key IAM enablers to relevant SOX sections, and highlights that Oracle IAM products apply to each primary enabler.[2]

TABLE 3. KEY IDENTITY AND ACCESS MANAGEMENT AND COMPLIANCE ENABLERS AND THE ORACLE PRODUCTS THAT FACILITATE SARBANES-OXLEY COMPLIANCE

SECTION	TITLE	IDENTITY AND ACCESS MANAGEMENT AND COMPLIANCE ENABLERS	ORACLE IDENTITY AND ACCESS MANAGEMENT PRODUCTS
302	Corporate Responsibilities for Financial Reports	Provide automated reports.	• Oracle Waveset • Oracle Identity Analytics
401	Disclosures in Periodic Reports	Provide automated reports.	• Oracle Waveset • Oracle Identity Analytics

[2] To find out more about the identity management products and services available from Oracle, please visit oracle.com/identity.

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 comprehensive workflow processes to assess compliance. • Enforce secure access policies. • Provide automated reports.	• Oracle Waveset • Oracle Identity Analytics • Oracle OpenSSO • Oracle Directory Server Enterprise Edition
409	Real Time Issuer Disclosures	• Conduct periodic compliance assessments. • Provide automated reports.	• Oracle Waveset • Oracle Identity Analytics
802	Criminal Penalties for Altering Documents	• Revoke user access upon termination. • Provide automated reports.	• Oracle Waveset • Oracle Identity Analytics
902	Attempts and Conspiracies to Commit Fraud Offenses	Enforce SoD policies.	• Oracle Waveset • Oracle Identity Analytics

Related Regulatory Compliance Issues

Of course, compliance involves more than just SOX. It also includes consideration of the interaction among multiple national, international, industry, and local regulations, as well as best practices, guidelines, and frameworks and changing legal precedents. To achieve sustainable compliance, it is most effective to approach this complex and confusing mix 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 described in the following subsections.

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 US$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 SOX 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 passed regulations can extend into states other than the originating state. 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. 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 from where the data access occurs (inside the United States or outside). They must know the combination of who is accessing the data (U.S. 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 e-mails), and data at endpoints (on a laptop or thumb drive). They need to restrict access to all this data for not only the employees and contractors, but also any supplier that is supplying components and suppliers that might 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

Managing Total Organizational Risk

To manage total organizational risk, businesses and governments must centrally manage identities, access controls, and risk to eliminate redundant processes and ensure that application security management does not happen in a siloed approach. They must have an enterprisewide view of GRC, identities, and access controls that includes answers to these critical questions:

- **Governance.** How do we ensure adequate executive oversight of business activities critical to the confidence of shareholders, employees, and regulatory bodies?
- **Compliance.** How do we ensure conformity with legal and regulatory requirements, corporate policies and procedures, and industry technology standards?
- **Risk.** How do we close loopholes and eliminate workarounds to internal controls?
- **Identities.** How do we ensure that employees and suppliers are who they say they are and have not contravened laws that could prohibit them from work?
- **Access control.** How do we ensure that customers, employees, partners, and suppliers have appropriate access to systems and that no employees have security profiles across systems that inappropriately conflict?

Best Practices for the Identity and Access Management and Compliance Journey

Since the passage of SOX in 2002, practical experience in the field has yielded several recommended best practices for implementing IAM systems to enable SOX compliance. Oracle recommends the following:

- **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.
- **Recognize information technology'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.
- **Understand the role of identity and access management.** IAM plays a critical role in compliance with SOX requirements, particularly in the areas of minimizing risk, automating processes, preventing fraud, and providing comprehensive auditing and reporting. However, it does not automatically satisfy all SOX requirements. Recognizing the value and the limitations of IAM in the entire spectrum of SOX compliance is essential.
- **Think program, not project.** SOX 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. Because of new higher standards, boards of directors and executives must be knowledgeable about, and assume liability for, everything going on within the enterprise.

- **Develop a strategy.** The only way to address the wide spectrum of compliance requirements effectively is to integrate them into a common compliance strategy 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.
- **Establish a governance process.** Compliance efforts affect a broad spectrum of an enterprise. Stakeholders from many organizations, often with conflicting priorities, have stakes 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
- **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.
- **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.
- **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 governance, risk, and compliance (GRC) 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.
- **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.

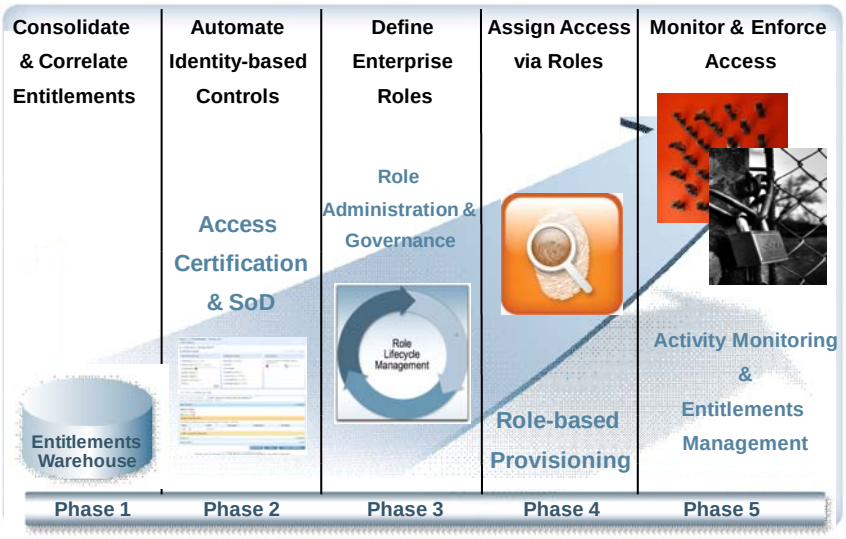
How to Get Started with Sarbanes-Oxley and Identity and Access Management

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

Oracle recommends the following steps to getting started with a SOX compliance and IAM strategy.

- **Understand the landscape.** Take the time to understand how SOX 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 SOX 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.
- **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.
- **Set specific, measurable objectives.** Based on your understanding of SOX requirements and knowledge of where your company is on the compliance journey, you should set specific objectives achievable in a phased approach. This will allow you to assess progress against short-term, measurable goals, not long-term, broadly stated intentions.
- **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 roadmap, such as the one in the figure, for your IAM and compliance journey.



It is necessary to plan your IAM implementation in phases. The sequence and content of each phase is highly dependent on individual company objectives and requirements.

- **Lay a foundation.** Build a basic infrastructure for IAM upon which you can build a complete IAM system. For example, in the figure, projects to establish a unified directory infrastructure and provisioning consolidated entitlements warehouse lay a solid foundation upon which to implement role-based provisioning, automated audit control remediation, and strong access controls.
- **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 and compliance strategy. Success in these early stages will provide insight and experience that will make succeeding phases easier to implement.
- **Adjust the plan, but stay the course.** As you proceed through the IAM and 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 roadmap as necessary. Do not give up. Work for the real business benefits (not just penalty avoidance) that can come from a well-implemented IAM and compliance strategy.

Case Studies

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

Ensuring Segregation of Duties at a Financial Services Company

Situation

Maria, an accountant working in the accounts receivable (A/R) group, takes the opportunity to move to another group within the company, where she will work in the accounts payable (A/P) department.

When she starts her new job, provisioning quickly grants her access to the appropriate network resources to fulfill her new responsibilities.

Meanwhile, she continues to have access to resources tied to her old position. This puts the company in violation of the SoD requirements of SOX, 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 SOX 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

Automated provisioning occurs without an audit, so 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 SOX auditor doing a routine review of access, thus putting the company at risk for failing the audit and being charged with violating SOX requirements for SoD.

Solution

The company deploys Oracle Identity Manager, which automates policy-based provisioning. By verifying role- and entitlement-level SoD policies defined in Oracle Identity Analytics, when an employee leaves one area to join another, instant provisioning for new responsibilities and deprovisioning for resources associated with the previous position occur automatically, simply by assigning the employee a new business role. This eliminates the risk of violating SOX requirements requiring SoD and prohibiting erroneous aggregation of privileges.

Automating Recertification at a Major Financial Services Company

Situation

A major financial services company has more than 90,000 employees with access to more than 1,000 different applications, 6,000 servers, and 500 databases. With more than 1 million user accounts across the enterprisewide infrastructure, the company CIO needs to sign off on employee access certification. The 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. Certification occurs through a process of manually generating reports and sending them to users' managers and application owners for review and approval.

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 accelerated its certification review process by implementing Oracle Identity Analytics to automatically track approvals, notify managers when it's time for a review, and escalate when reviewers fail to respond. Further streamlining this process are access reviews performed at the business role level, instead of reviewing and approving raw lists of IT entitlements. Oracle Identity Analytics also generates reports that capture all approvals and document all remediations for auditing purposes. By automating processes to streamline access review, Oracle Identity Analytics has saved the company more than €3.5 million (US$5.3 million). The company was able to complete 90 percent of the certifications in one week and was able to reduce the three-month-long certification process to just two weeks.

Protecting Employee Privacy at a Global Technology Company

Situation

Charles leaves his position in the human resources (HR) 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. Then, it is still a few days before someone handling provisioning becomes aware 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 a fine for the company due to HIPAA violations.

Solution

In addition to dismissing Charles, the company can implement Oracle Identity Manager. The solution has combined provisioning, auditing, and role management capabilities that allow much-tighter controls over access to private employee data. With Oracle Identity Manager, when someone leaves the benefits area of HR to join another department, that employee's previous HR benefits role gets deprovisioned and a new role assignment takes place, based on the new job.

Conclusion

SOX has had a profound effect on business. It addresses financial control and financial reporting issues raised by corporate financial scandals, focusing primarily on two major areas: corporate governance and financial disclosure. IT plays a major role in enabling compliance with SOX implementation of IAM systems, supports strong data security and compliance policies across the enterprise, and reduces the overall cost of compliance. Oracle offers a pragmatic approach to IAM that circumvents excessive complexity in favor of simple, open, and proven technology.

Oracle is committed to developing practices and products that help protect the environment

Identity and Access Management:
Enabling Sarbanes-Oxley Compliance
March 2010

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
Sun.com