Oracle Identity Management
- *Buyer's Guide for Compliance Solutions*

An Oracle White Paper
Dec 2008

ORACLE

Oracle Identity Management
- *Buyer's Guide for Compliance Solutions*

Introduction 3
Compliance Primer 4
- Compliance Reference Model 5
- Policy & Process Definition 6
- Preventive Controls 6
- Detective & Corrective Controls 7
- Controls Validation 7

Identity Management Compliance Checklist 8
- Policy & Process Definition 8
- Preventive Controls 9
- Detective & Corrective Controls 11
- Controls Validation 14

Oracle Identity Management 15
Conclusion 16
Appendix-A HIPAA & Compliance Reference Model 17
Appendix-B GLB & Compliance Reference Model 20
Appendix-C SOX & Compliance Reference Model 22

INTRODUCTION

Numerous laws and regulatory mandates focus on corporate governance and accountability around sensitive information (specifically financial, non-public information and protected healthcare information). This has significantly impacted the underlying IT systems that support the applications and repositories holding this sensitive information. Organizations are continuously looking for help in preventing fraud and protecting sensitive information. The fact that key corporate executives carry personal liability in the event of non-compliance virtually ensures compliance to be a key initiative in any large organizations. Additionally, there are other internal cost-containment requirements that can be effectively met by defining and implementing a sound auditing and compliance methodology. Most corporations agree that compliance leads to better corporate governance and management.

The fact that key corporate executives carry personal liability in the event of non-compliance virtually ensures compliance to be a key initiative in any large organizations.

This document focuses on three of the most important regulatory compliance mandates - Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLB) and Health Insurance Portability & Accountability (HIPAA). The document presents an overview of SOX, GLB and HIPAA; translates these mandates into identity management requirements and challenges; defines and describes the reference model; and concludes by applying the reference model to each of these three mandates and general identity compliance challenges.

Identity Management (IdM) solutions focus on access rights, user activity and storage of sensitive data, and help organizations understand and control who has access to what information – and how, when and why they access such information. Because of this, IdM is an integral piece of the puzzle in achieving regulatory compliance.

The paper will describe the applicability of IdM solutions to compliance by presenting the following:

1. Compliance Primer with a Reference Implementation Model
2. Compliance Checklist
3. Mandate Specific Details

COMPLIANCE PRIMER

Although stronger identity control is clearly warranted in the audited organization, the problematic element is determining what is considered adequate and prudent control. Examining several compliance mandates, IT implementers may question the imprecise language. The following are examples of regulatory ambiguity:

Due to ongoing changes in existing mandates, auditing practices and the continuous introduction of new mandates, organizations need a sustainable compliance deployment/implementation model with flexibility to comply with changes or new mandates.

- SOX (from the Public Company Accounting Oversight Board [PCAOB] Standard 2): "Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of [assetsj"

  What is "*reasonable assurance*"?

- HIPAA: "Maintain reasonable and appropriate administrative, physical, and technical safeguards to ensure the integrity and confidentiality of the information"

  What is "*reasonable and appropriate*"?

- GLBA: "Safeguards … shall be reasonably designed"

  How does one know when "*reasonably designed*" is achieved?)

Due to ongoing changes in existing mandates, auditing practices and the continuous introduction of new mandates, organizations need a sustainable compliance deployment/implementation model with flexibility to comply with changes or new mandates. Rather than planning the identity management deployment around specific paragraphs of the regulations, organizations should plan for a solution that ensures the confidentiality (sometimes referred to as privacy in context of employees and consumer's information), integrity, timeliness and security of sensitive data by being able to answer the following questions:

1. Who has or had access to what?
2. How and when was a person granted access?
3. What did they do with their access rights?

This approach avoids the challenges posed by the imprecise language from various regulations and results in a better chance of achieving compliance.

At a high level, the three mandates discussed here are intended to address and protect information in the listed areas:

Regulatory Mandate	
SOX	Financial
HIPAA	Electronic Private Healthcare Information (ePHI)
GLB	Non-Public Personal Information

To protect these types of sensitive data using identity management solutions, the following challenges must be addressed:

- Define and track changes to various policies, procedures and controls related to access rights.
- Track ongoing violations to the policies and processes related to access rights.
- Monitor the timeliness of violation or exception detection mechanisms and the corresponding remediation activity.
- Audit access activity for all resources hosting sensitive information.
- Analyze unauthorized attempts to access or change sensitive information.
- Analyze the incremental effectiveness of controls around access rights.

Compliance Reference Model

Oracle has developed an implementation reference model for identity management. This reference model presents a sustainable framework by applying identity management technologies and solutions to regulatory compliance requirements. In addition to helping organizations achieve regulatory compliance, the reference model helps customers achieve significant business optimizations. The reference model presents a 4-step approach to achieving compliance. At the heart of each step is the Audit and Operational data stored in various database repositories.

The 4 steps in the reference model are:

1. Define policies and processes
2. Implement Preventive Controls to enforce policies and processes
3. Implement Detective Controls to detect exceptions, and corrective controls to remediate anomalies.

4. Validate all policies and controls by measuring their effectiveness, and mediate any risks identified during the validation process by changing the policies and processes to improve the quality of the controls.

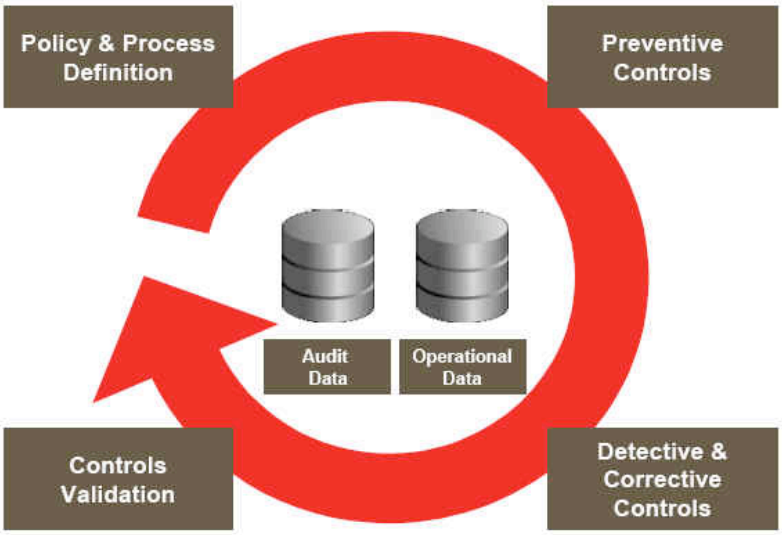

Figure 1.

Policy & Process Definition

Organizations attempt to proactively enforce the intended behavior by documenting policies and procedures. While policies and procedures cannot explicitly prevent undesired behavior from occurring, they set the tone by encouraging proper behavior by every employee.

Examples include policies that define which individuals within the organization should have specific levels of access to various systems that support financial transactions.

Preventive Controls

When most people think about controls, they are probably thinking about **Preventive Controls**. When properly designed and implemented, preventive controls can prevent the undesirable behavior from ever occurring.

An example is a preventive control ensuring that only the CFO and the Controller have the ability to commit transactions exceeding a defined value in a corporate billing system.

Detective & Corrective Controls

While policies, processes and preventive controls can prevent undesirable activities from occurring, no system of controls is perfect. Inevitably situations arise where an inappropriate action has been taken – either through an innocent error or with a deliberate fraudulent intent. **Detective Controls** are used to identify situations when such activity has already occurred. They provide the safeguards to cover any of the gaps or deficiencies that may have been ignored by the Preventive Controls that are in place.

A common example of Detective Controls is ongoing verification that ensures that the correct level of access is being enforced for all users in the enterprise.

Corrective Controls are most commonly used in conjunction with Detective Controls. These types of controls are put in place to ensure that once an anomaly is discovered, a set of corrective measures is in place to remove and correct the anomaly – or to bring the appropriate attention to the right audience. An example of a Corrective Control is the automated escalation of a delayed internal audit to another person in the firm.

Controls Validation

To achieve regulatory compliance, measuring the effectiveness of preventive and detective controls is as important as implementing them. Validation of controls, when combined with preventive and detective controls to enforce the company's policies, helps organizations to achieve repeatable, sustainable, and cost-effective compliance. It is the validation that demonstrates the value of preventive, detective and corrective controls to senior IT management and business executives, and communicates the continuous incremental improvement in the effort – allowing organizations to integrate enforcement and automate continuous compliance measurement of controls while gaining communication efficiencies among the operational, IT and business teams and the executives.

In most corporate entities that comply with S-O 404, attestation is typically handled by use of manual processes and spreadsheets, which can be very time consuming and costly. Such manual processes are prone to human errors and involve repetitive efforts at every audit. By automating these routine tasks, organizations can realize significant time and cost savings in executing the processes required to demonstrate full compliance with industry regulations.

IDENTITY MANAGEMENT COMPLIANCE CHECKLIST

This section presents a baseline list of compliance related requirements for an IdM solution. These requirements are grouped based on the 4-step approach described above.

Policy & Process Definition

☑	**Provisioning Policies**	Ability to define rule based policies to determine the list of applications a user should be provisioned to and his or her entitlements in those applications
☑	**Denial Policies**	Ability to define what resources and applications should be denied to a user or a set of users, as part of provisioning policies.
☑	**Access Policies**	Ability to define rule based policies to determine who has access to which web resources.
☑	**Role Based Access Control (RBAC)**	Ability to define provisioning entitlements and access rights in terms of roles. Additional ability to map group membership rules to the roles.
☑	**Policy History**	Ability to provide complete policy history so that the auditors and administrators may easily find the definition of policy that was effective on a given day.

☑	**Approval Workflows**	Ability to request & approve the access to applications or entitlements not acquired through automated provisioning & access policies.
☑	**Approval Policies**	Ability to define the list of approvers for each resource in provisioning requests. Ability to utilize roles in approval policies.
☑	**Administrative Policies**	Ability to define rule based policies for administering various identity entities i.e. roles, organizations and resources
☑	**Segregation of Duty (SOD) Policies**	Ability to define policies that prevent a user from acquiring a conflicting combination of roles, resources or entitlements in a single resource.

Preventive Controls

☑	**Web Single Sign-On**	Ability to support single sign-on across multiple web applications and heterogeneous web servers spread across multiple DNS domains extending to partner and consumer applications.
☑	**Strong Authentication**	Ability to support advanced authentication mechanism to prevent authentication attacks such as phishing, trojans, proxy attacks and other threats.

☑	**Real-time Fraud Prevention**	Ability to perform sophisticated risk analysis to trigger real-time alerts and follow-up actions (for example, challenge the user) to prevent fraudulent transactions in real-time.
☑	**Authoritative Source**	Ability to designate a set of resources or applications as the authoritative sources for user provisioning.
☑	**Authoritative Reconciliation**	Ability to trigger provisioning workflows based on reconcile with the authoritative resources.
☑	**User On-Boarding Workflow**	Ability to define automated or approval based workflows based on provisioning policies to create user's account in various applications.
☑	**User Transfer Workflow**	Ability to define automated or approval based workflows to adjust user's accounts in various applications based on changes in user's capacity in the organization.
☑	**User Termination Workflow**	Ability to de-provision user's account from applications at the termination of employment.
☑	**Password Synchronization**	Ability to synchronize user's password across all applications, thereby requiring fewer passwords that each user must maintain.

☑	**Policy Retrofits**	Ability to adjust user's account in various applications based on ongoing changes in various provisioning policies.
☑	**Role Mining**	Ability to take existing enterprise data about users, entitlements and the relationships between them and identify patterns in existing entitlements and user memberships to suggest candidate roles for the purpose of provisioning and access control.
☑	**Preventive Segregation of Duty Checks**	Ability to check for SOD violation at real-time during events such as entitlement provisioning or role grants.
☑	**LDAP Firewall**	Ability to provide virtual LDAP access to identity data in various LDAP and other repositories, and to the client applications located in network's DMZ.
☑	**Directory Aggregation**	Ability to provide an aggregated, virtual view of identity data from multiple sources without requiring data consolidation.

Detective & Corrective Controls

☑	**Reconciliation For Exception Detection**	Ability to reconcile with the fine-grained entitlements in all resources and generate exception reports based on the deviations to the policies in the entitlements.

☑	**Rogue Account Detection**	Ability to detect explicitly created application accounts in exception of documented provisioning policies.
☑	**Entitlement Exception Detection**	Ability to detect explicitly granted entitlements in various applications in exception of documented provisioning policies.
☑	**Detective Segregation of Duty Checks**	Ability to detect SOD violations in granted entitlements and roles in various applications based on pre-defined SOD rules.
☑	**Exception Tracking**	Ability to store the state transitions of an exception as it gets cleared.
☑	**Attestation Configuration**	Ability to periodically review user's entitlements in various applications.
☑	**Attestation Schedule**	Ability to configure frequency of attestation processing.
☑	**Attestation of Fine-Grained Entitlements**	Ability to attest to user's fine grained entitlements (various roles, responsibilities, profiles, privileges and other application functional security artifacts) in all resources and applications.
☑	**Attestation Scope**	Ability to define filtering criteria for users, resources and entitlements in attestation process definition.

☑	**Attestation Delegation**	Ability to delegate the review of data to be attested to, to other users. Ability to remove attestation requests from non-responsive reviewers and assign it to other reviewers.
☑	**Historical Snapshots**	Ability to store point-in-time snapshot of user attributes, approvals, workflows, policy history and attestation related data for audit purposes.
☑	**Configurable Audit Policies**	Ability to configure which discrete Policies events (within the processes of identity administration, provisioning, exceptions, approvals, attestation and web access etc) need to be audited.
☑	**Centralized Audit**	Ability to store all audit information for identity administration, approvals, provisioning and web access events in a central database repository.
☑	**Remediation**	Ability to perform contextual remediation activities from within detection controls i.e. de provisionin users based on the outcome of attestation and exception reports.

Controls Validation

☑	**Access Rights Reporting**	Ability to report on user's current (who has what) and historical (who had what) access rights.
☑	**Exception Reporting**	Ability to report on current and historical rogue accounts and exceptions in user's fine-grained entitlements.
☑	**Provisioning Context Reporting**	Ability to report on how a user's entitlements were provisioned — for example, provisioning policies, policy change, approval, discretionary provisioning, reconciliation etc.
☑	**Remediation Reporting**	Ability to report on current and historical remediation activities.
☑	**Change Reporting**	Ability to report on changes to all identity entities including policy definition, user attribute, role definition, role membership rules, organization attributes, delegated administrative and approval policies, approval workflows and others.
☑	**Attestation Dashboard**	Ability to view all historical and current attestation requests and their outcome in a single dashboard.
☑	**Compliance Dashboard**	Ability to view exception, remediation and other related metrics corresponding to the applications with mandate specific sensitive data.

ORACLE IDENTITY MANAGEMENT

Oracle Identity Management provides a market-leading set of solutions to tackle various aspects of identity management through a comprehensive suite of products:

Oracle Access Manager delivers critical functionality for access control, single sign-on, and user profile management in the heterogeneous application environment. It provides the ability to define and enforce access policies and analyze and report on user's historical access activity (successful/failed attempts to log-in or access a resource)

Oracle Entitlements Server (formerly BEA AquaLogic Enterprise Security) externalizes and centralizes fine-grained authorization policies for enterprise applications and web services – resulting in comprehensive, reusable, and fully auditable authorization policies and a simple, easy-to-use administration model.

Oracle Adaptive Access Manager provides added security to any existing access management solution by providing a strong yet easy-to-deploy multifactor authentication support through Adaptive Strong Authenticator - and proactive, real-time fraud prevention through Adaptive Risk Manager.

Oracle Identity Federation enables cross-domain single sign-on through its self-contained and flexible multi-protocol federation server – allowing customers to easily create trust relationships between partners and agencies by connecting users seamlessly and securely.

Oracle Identity Manager delivers critical functionality for user provisioning across heterogeneous applications. It provides the ability to define provisioning & SoD policies and approval workflows. It provides the ability to detect various exceptions including rogue accounts, entitlement exceptions and SoD violations. Additionally it provides a comprehensive set of operational and historical reports based on rich set of operational and historical snapshot data maintain in its repository.

Oracle Role Manager delivers enterprise class role lifecycle management capabilities to provide the authoritative source for the relationships between business users, organizations, and entitlements, thus enabling automation of role based provisioning and access control across the IT infrastructure. Automated tools for role mining helps enterprises to identify candidate roles through existing entitlement patterns.

Oracle Virtual Directory provides Internet and industry standard LDAP and XML views of existing enterprise identity information, without synchronizing or moving data from its native locations.

Oracle Internet Directory is a robust and scalable LDAP V3-compliant directory service that leverages the high availability capabilities of the Oracle RDBMS.

The components in the Oracle Identity Management suite are "hot pluggable" so that organizations deploying components of the suite can pick and choose which services they deploy, and in which order. Suite components embrace open standards and can easily be deployed into existing infrastructures. In addition, when deployed together, these components can form the basis of cohesive and effective enterprise security architecture. Furthermore, these components are designed to help strengthening regulatory compliance and alleviating the associated costs.

CONCLUSION

Today, compliance is a major driver for deploying IdM applications. When considering IdM application options, customers should carefully evaluate product's quality and vendor's vision in delivering a compliance centric solution. The selected solution should provide strong capabilities to not only define and enforce policies, but also to detect and remediate exceptions to me policies in a timely fashion. Additionally, as compliance is often related to the auditing activities performed by internal and external auditors, the selected solution must be able to retain all historical records and render them in reports and dashboard formats on demand basis. When these factors are considered, Oracle Identity Management, with its broad and comprehensive identity administration, access management and directory service products, is the ideal choice to satisfy your enterprise compliance requirements.

APPENDIX-A HIPAA & COMPLIANCE REFERENCE MODEL

"HIPAA" is an acronym for the Health Insurance Portability & Accountability Act of 1996 (August 21), Public Law 104-191, which amended the Internal Revenue Service Code of 1986. Also known as the Kennedy-Kassebaum Act, the Act includes a section, Tide II, entitled Administrative Simplification, requiring improved efficiency in healthcare delivery by standardizing electronic data interchange, and Protection of confidentiality and security of health data through setting and enforcing standards. Virtually all healthcare organizations — including all healthcare providers, health plans, public health authorities, healthcare clearinghouses, and self-ensured employers — as well as life insurers, information systems vendors, various service organizations, and universities are affected by this law.

Overall HIPAA compliance requirements include the following:

1. Building initial organizational awareness of HIPAA.

2. Comprehensive assessment of the organization's privacy practices, information security systems and procedures, and use of electronic transactions.

3. Developing an action plan for compliance with each rule.

4. Developing a technical and management infrastructure to implement the plans.

5. Implementing a comprehensive implementation action plan, including:

    a. Developing new policies, processes, and procedures to ensure privacy, security and patients' rights.

    b. Building business associate agreements with business partners to support HIPAA objectives.

    c. Developing a secure technical and physical information infrastructure.

    d. Updating information systems to safeguard protected health information (PHI) and enable use of standard claims and related transactions.

    e. Training of all workforce members.

    f. Developing and maintaining an internal privacy and security management and enforcement infrastructure, including providing a Privacy Officer and a Security Officer.

The following table maps the HIPAA regulation paragraphs to the components of reference model proposed above.

Regulation Section	Policies	Preventive Controls	Detective Controls
§164.306.a.1	Provisioning Policies Access Policies SoD Policies	Provisioning & Approval Workflows Policy-Based Retrofits	Rogue A/C Detection Entitlement Exception Attestation

Regulation Section	Policies	Preventive Controls	Detective Controls
§164.306.a.2	Configure Threats as SoD Policies	Provisioning and Approval Workflows Policy-Based Retrofits	Rogue A/C Detection Entitlement Exception Attestation
§164.306.a.4			Rogue A/C Detection Entitlement Exception
§164.308.a.1.i		Provisioning & Approval workflows Policy Retrofits	Rogue A/C Detection Entitlement Exception Attestation Reports & Dashboards
§164.308.a.1.ii.D			Historical Snapshots Attestation Reports & Dashboards
§164.308.a.3.i	Provisioning Policies Access Policies SoD Policies	Provisioning and Approval Workflows Policy Retrofits	Rogue Account Detection Entitlement Exception Detection
§164.308.a.3.ii.A		Approval Workflows	Attestation
§164.308.a.3.ii.B	Provisioning Policies Access Policies SoD Policies		Entitlement Exception Detection Rogue Account Detection
§164.308.a.3.ii.C		Employee Termination Workflow	Rogue Account Detection
§164.308.a.4.ii.A	SoD Policies for ePHI	Provisioning & Approval workflows	Entitlement Exception Detection Attestation
§164.308.a.4.ii.B	Provisioning Policies	Approval and provisioning workflows	
§164.308.a.4.ii.C			Attestation
§164.308.a.5.ii.C			Historical Snapshots Reports & Dashboards

Regulation Section	Policies	Preventive Controls	Detective Controls
§164.312.a.1	Provisioning Policies Access Policies SoD Policies	Provisioning and Approval Workflows Policy Retrofits	Entitlement Exception Detection Resource Centric Attestation
§164.312.a.2.i		Unique ID generation	
§164.312.a.2.ii	Role Assignment through Provisioning Policies	Provisioning workflow	

APPENDIX-B GLB & COMPLIANCE REFERENCE MODEL

On February 1, 2001, the U.S. Treasury Department issued guidelines interpreting the privacy and security requirements of the Gramm-Leach-Bliley (GLB) Act of 1999 (otherwise known as the Financial Modernization Act of 1999). The GLB Act was established primarily to repeal restrictions on banks affiliated with securities firms, but it also requires financial institutions - including any organization that works with people such as preparers of income tax returns, consumer credit reporting agencies, real estate transaction settlement services, and debt collection agencies and people that receive protected information from financial institutions to adopt strict privacy measures relating to customer data. Financial services holding companies can be created to offer a frill range of financial products based on tight regulatory principles.

There are three provisions of the GLB Act that restrict the collection and use of consumer data, specifically nonpublic personal information (NPI). NPI is any "personally identifiable financial information" that a financial institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise "publicly available." NPI is:

- Any information an individual gives you to get a financial product or service (for example, name, address, income, Social Security number, or other information on an application);

- Any information you get about an individual from a transaction involving your financial product(s) or service(s) (for example, the fact that an individual is your consumer or customer, account numbers, payment history, loan or deposit balances, and credit or debit card purchases);

OR

- Any information you get about an individual in connection with providing a financial product or service (for example, information from court records or from a consumer report).

NPI does not include information that you have a reasonable basis to believe is lawfully made "publicly available." In other words, information is not NPI when you have taken steps to determine:

- That the information is generally made lawfully available to the public; and

- That the individual can direct that it not be made public and has not done so. For example, while telephone numbers are listed in a public telephone directory, an individual can elect to have an unlisted number. In that case, her phone number would not be "publicly available".

The third provision, the Safeguards Rule, went into effect during 2003 and requires included institutions to take proactive steps to ensure the security of customer information. The GLB Act requires financial institutions to reevaluate their security policies and take action if discrepancies are discovered.

Following are key areas in information security that the GLB Act requires financial institutions to address:

- Evaluate IT environments and understand the security risks - define those risks internal and external to the organization.

- Establish information security policies to assess and control risks - these include authentication, access control, and encryption systems.
- Conduct independent assessments - third-party testing of the institutions' information security infrastructure.
- Provide training and security awareness programs for employees.
- Scrutinize business relationships to ensure they have adequate security.
- Establish procedures to upgrade security programs that are in place.

From a technical perspective, the security requirements put forth with the GLB Act seem enormous, but these requirements can be easily met with a sound security policy that is enforced across the enterprise as well as across products that allow an enterprise to achieve the desired result.

The following table maps the GLB regulation paragraphs to the components of reference model proposed above.

Regulation Section	**Policies**	**Preventive Controls**	**Detective Controls**
§314.1.a	Provisioning Policies Access Policies SoD Policies	Provisioning and approval workflows Policy Retrofits	Entitlement Exception Detection Rogue Account Detection Attestation Reporting
§314.3	Provisioning Policies Access Policies SoD Policies		
§314.4(b)			Rogue Account Detection Attestation Operational & Historical Reporting
§314.4(c)		Provisioning/Approval Workflows	Rogue Account Detection
§314.4(e)		Policy Retrofits	

APPENDIX-C SOX & COMPLIANCE REFERENCE MODEL

On February 1, 2001, the U.S. Treasury Department issued guidelines interpreting the privacy and security requirements of the Gramm-Leach-Bliley (GLB) Act of 1999 (otherwise known as the Financial Modernization Act of 1999). The GLB Act was established primarily to repeal restrictions on banks affiliated with securities firms, but it also requires financial institutions - including any organization that works with people such as preparers of income tax returns, consumer credit reporting

The U.S. Public Company Accounting Reform and Investor Protection Act of 2002, better known as the Sarbanes-Oxley (SOX) Act has been called the most far-reaching corporate reform legislation since the 1930's. The Sarbanes-Oxley Act requires major changes in corporate governance, accounting and financial reporting practices. It was passed to address major corporate accounting scandals, which severely damaged investor confidence in the securities markets. With this regulation, for the first time in legislative history, named individuals within a publicly traded firm can now be held legally and financially liable for failing to comply with the directives laid out in the Act. The Act specifies higher levels of corporate accountability where CEOs and CFOs are required to certify - in writing - the veracity of their financial reports.

Of all the legislative drivers, Sarbanes-Oxley is the most far-reaching in terms of the requirements for compliance and the number of firms that it impacts. This is due to several factors including:

- For the first time, company executives can personally be held legally and financially liable for acts of wrongdoing.
- The Act impacts domestic and foreign companies who have listed securities being traded in an exchange in the United States. This spans almost the entirety of the Global 2000, including firms that are overseas-based.

The cost of ensuring compliance with all elements of the Act is incredibly high in terms of hard cash and the sheer amount of effort and manpower required.

Section 302 and 404 of SOX are most relevant to information security, identity access and management.

SEC.302
The Commission shall, by rule, require, for each company filing periodic, that the principal executive officer or officers and the principal financial officer or officers, or persons performing similar functions, certify in each annual or quarterly report filed or submitted under either such section of such Act that–

- The signing officer has reviewed the report and based on the officer's knowledge, the report does not contain any untrue statement of a material fact or omit to state a material fact necessary in order to make the statements made, in light of the circumstances under which such statements were made, not misleading;

Based on such officer's knowledge, the financial statements, and other financial information included in the report, fairly present in all material respects the financial condition and results of operations of the issuer as of, and for, the periods presented in the report

- The signing officers—
    - Are responsible for establishing and maintaining internal controls;

- Have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared;

- Have evaluated the effectiveness of the issuer's internal controls as of a date within 90 days prior to the report; and

- Have presented in me report meir conclusions about me effectiveness of their internal controls based on their evaluation as of that date;

- The signing officers have disclosed to the issuer's auditors and the audit committee of the board of directors (or persons fulfilling the equivalent function)—

  - All significant deficiencies in the design or operation of internal controls which could adversely affect the issuer's ability to record, process, summarize, and report financial data and have identified for the issuer's auditors any material weaknesses in internal controls; and

  - Any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer's internal controls.

- The signing officers have indicated in the report whether or not there were significant changes in internal controls or in other factors that could significantly affect internal controls subsequent to the date of their evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses.

SEC. 404
The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall--

- Sate the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

- Contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

- Each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

The following table maps the SOX regulation paragraphs to the components of reference model proposed above.

Regulation Section	Policies	Preventive Controls	Detective Controls
§302	Provisioning Policies Access Policies	Employee On-Boarding, Transfer and Termination Policy Retrofits	Attestation History Policy History
§404	SoD Policies		Reports & Dashboards Attestation Rogue Account Detection Entitlement Exception Detection Historical Snapshots Monitor Exceptions Detection & Remediation Activities

Oracle Identity Management - Buyer's Guide for Compliance Solutions

Revised - Dec 2008
Author: Viresh Garg
Contributing Author: Stephen Lee

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
oracle.com