



# DBA Guide to Understanding Sarbanes-Oxley

**Stephen Kost**  
*Integrigy Corporation*



# Agenda

- What is Sarbanes-Oxley?
- Sarbanes-Oxley Compliance
- Oracle Applications SOX Compliance Model
  - Security
  - Auditing
  - Change Management

## Sarbanes-Oxley Act of 2002

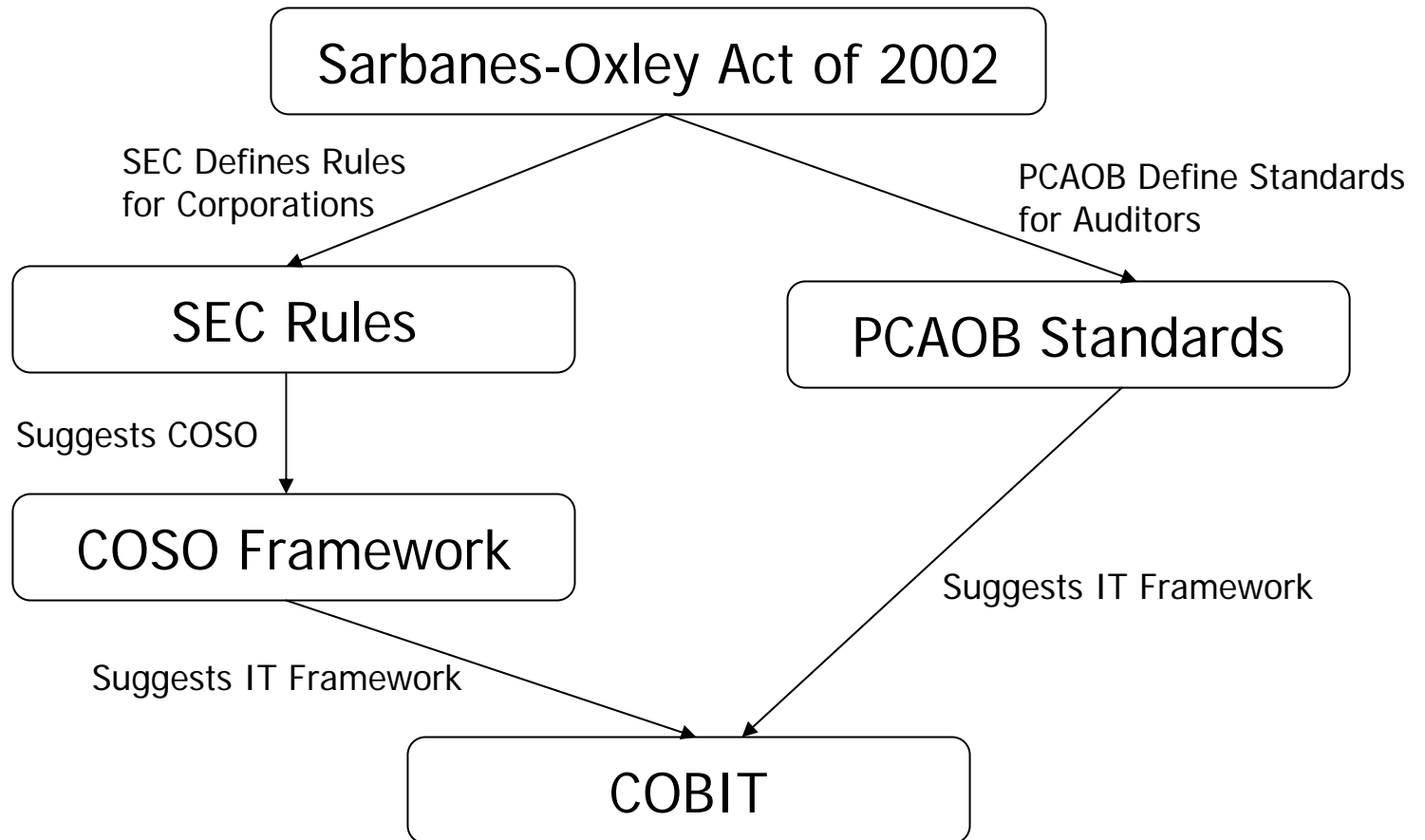
- **Section 302** requires the Chief Executive Officer and Chief Financial Officer on a periodic basis to have –
  - “designed internal controls” over financial reporting
  - “evaluated the effectiveness” of such internal controls
- **Section 404** requires a corporation’s annual report to contain an internal control report that states –
  - “the responsibility of management for establishing and maintaining an adequate internal control structure and procedures”
  - management has performed “an assessment of the effectiveness of the internal control structure and procedures for financial reporting”

## SEC Rules and COSO

- The actual SOX rules are implemented by the SEC
  - The SEC final rules require corporations to use a recognized internal controls framework
  - The Sponsoring Organizations of the Treadway Commission (COSO) internal controls framework is specifically mentioned
- COSO provides a framework for defining and evaluating internal controls
  - Only addresses IT controls in a very general manner
  - COSO suggests using an IT controls framework, like COBIT

## PCAOB

- The Public Company Accounting Oversight Board (PCAOB) develops the rules for external auditors and released “Auditing Standard #2”
  - Emphasizes the importance of IT controls
  - Does not provide any details on what IT controls are required – each corporation to develop IT controls that support their internal control program
  - Most audit firms have adopted COBIT as the standard IT Controls Framework



# COBIT

- COBIT is a controls framework for IT governance for the entire organization and provides high-level control objectives for applications and infrastructure
  - The control objectives are not to a level that can be immediately implemented by a DBA or system administrator
  - The control objectives provide high-level characteristics for what the implemented internal control should include
- ISACA's "IT Control Objectives for Sarbanes-Oxley" maps COBIT to Sarbanes-Oxley compliance

## Sarbanes-Oxley Compliance

- There is no single point of reference or comprehensive guidelines for SOX compliance
- The definition of SOX compliance is defined by the corporation referencing a set of internal controls frameworks
- Because every business assesses risks differently, the controls each business requires will be different

# Sarbanes-Oxley Compliance

- SOX compliance is about risk
  - Internal controls are about controlling and reducing risk
- SOX compliance should be done in the context for an enterprise-wide SOX initiative
- Oracle Applications is often the financial system of record
  - The financial system will most likely garner close scrutiny
  - Often required to meet a higher standard of SOX compliance than the rest of the IT department

# Looking at SOX Compliance

- Corporate officers (CEO, CFO, ...)
  - Must attest to the corporations internal controls
  - Rely on internal audit and SOX compliance teams to determine if internal controls are in place
- External Auditors
  - Assess the effectiveness of such internal controls
  - Must understand the flow of transactions through the corporation and IT systems

## SOX is a WRITE Event

- SOX is primarily focused on write events
  - SOX is most concerned with any and all changes to the financial data and the processing of the financial data
  - The processing of financial data includes the programs, reports, and configuration settings that may affect how the data is processed or reported
- Unauthorized querying or viewing of data may be an issue in terms of HIPAA, GLBA, US and European privacy laws, and SEC rules

# What are Internal Controls

- Internal control is a process designed to provide reasonable assurance regarding the achievement of objectives
- Preventative or Detective
  - Preventative = discourage errors and irregularities from occurring
  - Detective = find errors and irregularities after they have occurred
- Automated or Manual

		Oracle Applications Technical Components		
		Oracle Applications	Database	Operating System
Access	1. Security	1.1 User Management	1.3 Database Security	1.4 OS Security
		1.2 Segregation of Duties		
	2. Auditing	2.1 Application Auditing	2.2 Database Auditing	2.3 OS Auditing
Changes	3. Change Management	3.1 Object Migrations	3.4 Schema Changes	3.7 Change Control
		3.2 Application Configuration	3.5 Database Configuration	
		3.3 Application Patches	3.6 Database Patches	3.8 OS Patches
Operations	4. Monitoring and Troubleshooting	4.1 Application	4.2 Database	4.3 Operating System
	5. Availability	5.1 Application	5.2 Database	5.3 Operating System

# 1. Security

- Security must be addressed at the application, database, and operating system levels
- Individual accounts for accountability
  - Must map generic accounts to individuals (e.g., APPS)
- Periodic review of access privileges
- Password management
  - Must meet enterprise-wide password policy, not some other standard

## 1.1 User Management

- Use of named and unique accounts for all users
- Adherence to the enterprise security policy for passwords for all application accounts (length, complexity, failure lock-out, etc.)
  - May require use of custom password validation
- New accounts should be created with a unique password and require the password to be changed upon first login

## 1.2 Segregation of Duties

- Do not use SYSADMIN
- System administrators and developers should have inquiry-only functional responsibilities
- Developers and other support staff should have no access to production to register programs, change profile options values, etc.
- Custom system administration responsibilities should be created for IT and limited to only necessary functions

## 1.3 Database Security

- APPS account only used for maintenance
  - All usage requires a change ticket
  - Access limited to a small group of DBAs
- DBAs and support staff have named, read-only database accounts
- Create an “APPSIF” database account with insert, update, and delete privileges to interface tables
  - All usage requires a change ticket

## 1.4 Operating System Security

- *oracle* and *applmgr* should be controlled and the appropriate logs maintained to identify the individual accessing these shared accounts
  - Use sudo or PowerBroker to control and log access
- All access to interface accounts should be controlled and the appropriate logs maintained and monitored to ensure only authorized processes and users are transmitting interface files

## 2. Auditing

- The Oracle Database and Oracle Applications are not compliant with SOX out of the box
  - No default auditing enabled
  - Oracle Applications only has created by and last updated by
- Performance is a significant concern with auditing
  - Only audit non-transactional tables
- Enabling auditing is the easy part
  - Need to develop procedures, scripts, and reports to archive, purge, alert, and report on the audit data

## 2.1 Application Auditing

- Oracle Applications AuditTrails uses database triggers and shadow tables
- Need to audit and maintain a history of changes to users, responsibility assignments, and security setup (menus, functions, etc.)
- Signon:Audit should be set to FORM
  - This can actually be very useful if a segregation of duties issue arises

## 2.2 Database Auditing

- Database session auditing should be enabled
  - Monitor for access to APPLSYSPUB not from app servers
  - Review all access to APPS not from app or DB servers
- Set `AUDIT_SYS_OPERATIONS = TRUE` to audit
- Need to create custom audit triggers on `FND_PROFILE_OPTIONS` and `FND_PROFILE_OPTION_VALUES`
  - Not auditable by Oracle Applications AuditTrails
- Audit `USER`, `PROFILE`, and `SYSTEM AUDIT`

## 3. Change Management

- Change management is critical to SOX compliance
  - Auditors may review changed objects and trace the paper trail
- Must include all changes to the application, database, application servers, operating system, and hardware
- Often changes to Profile Options are not included in the change management process
  - Profile options change the configuration of the application and processing of financial data

## Working with the Auditors

- Auditors role is to assess effectiveness of the internal controls and to identify weaknesses or deficiencies
  - Audits often performed by audit generalists
  - May have limited or no knowledge of Oracle Applications
  - Findings may be not be correctable in Oracle Applications
- Manual controls and acceptance of risk by management are possible solutions to audit findings
  - Unsupported by Oracle is a valid management response
  - May need to put in place compensating controls

## Conclusion

- No definitive references, rules, or guidelines exist for SOX compliance
  - SOX compliance is based on the corporation's assessment of risk and adopted controls framework
- SOX is primarily a Write event
  - DBAs must think about the controls related to every way financial data and processes may be changed
- Most SOX compliance requirements can be readily implemented
  - Control of the APPS account and other privileged users can be challenging due to the design of Oracle Applications

## Contact Information

**Integrigy Corporation**  
P.O. Box 81545  
Chicago, Illinois 60681  
888/542-4802

**Website:** [www.integrigy.com](http://www.integrigy.com)

**Sales:** [sales@integrigy.com](mailto:sales@integrigy.com)

**Development:** [development@integrigy.com](mailto:development@integrigy.com)

**Support:** [support@integrigy.com](mailto:support@integrigy.com)

**Security Alerts:** [alerts@integrigy.com](mailto:alerts@integrigy.com)