

DBA Guide to Understanding Sarbanes-Oxley

Stephen Kost
Integrigy Corporation

Introduction

The Sarbanes-Oxley Act never mentions the words database or data, however, DBAs must ensure their databases are in compliance with Sarbanes-Oxley. Sarbanes-Oxley Section 404 simply states that management has the responsibility “for establishing and maintaining an adequate internal control structure and procedures for financial reporting.” How does this sentence relate to a database being compliant with Sarbanes-Oxley? Well, directly it doesn’t. But since the Oracle Applications database contains data related to financial reporting and manipulation of this data “could adversely affect the [company’s] ability to record, process, summarize, and report financial data”, the Oracle Applications database must be compliant with the requirements of Sarbanes-Oxley for effective internal controls as stated in Sections 302 and 404 of the Act.

Ensuring compliance is not an easy task because DBAs generally think in terms of SQL statements, initialization parameters, and ratios, not internal controls, risk, attestation, governance, and weaknesses. Unfortunately, there is no database initialization parameter `SOX_COMPLIANCE=TRUE`, rather many aspects of operating and maintaining the database and Oracle Applications must be performed in a Sarbanes-Oxley compliant manner.

The most frustrating aspect for DBAs is that there are no definitive requirements, checklists, or guidelines on how an Oracle Applications implementation must comply with Sarbanes-Oxley. From Section 404, the phrase “an adequate internal control structure and procedures for financial reporting” must be interpreted and extended to the database. Unfortunately, it is not clear who should provide this interpretation: external auditors, internal auditors, management, IT, etc. In most cases, the external audit firm provides “their” version of requirements in the form of a Sarbanes-Oxley assessment and findings. Often this assessment is performed by audit generalists who do not have experience with Oracle Applications, but instead understand financial controls and business processes. These findings are then forced on the DBA to remediate, usually in a short timeframe with little understanding or direction on what is truly required.

This whitepaper will assist DBAs in working through Sarbanes-Oxley compliance issues by providing a framework for understanding what truly is required in terms of operational procedures, auditing and logging, access controls, and change management. Practical tips will be offered for many of the difficult to remediate issues identified by external auditors including when to remediate with manual procedures or automated solutions and when to push back on the auditors.

What is Sarbanes-Oxley?

The Sarbanes-Oxley Act of 2002 (SOX) provides for a new set of corporate governance rules and regulations for public companies. Two sections, (1) Section 302 “Corporate Responsibility for Financial Reports” and (2) Section 404 “Management Assessment of Internal Controls”, specifically address internal controls over financial reporting. The Sarbanes-Oxley Act is high-level and only addresses such requirements as corporate officers “are responsible for establishing and maintaining internal controls” and are required to periodically assess and report on the effectiveness of such internal controls. There are no details on what are effective internal controls and to what extent internal controls are required for “financial reporting”. The Securities and Exchange Commission (SEC) and the Public Company Accounting Oversight Board (PCAOB) are required by the Act to develop the final rules regarding compliance for the establishment, maintenance, and assessment of internal controls over “financial reporting”.

Section 302 requires the Chief Executive Officer and Chief Financial Officer on a quarterly or annual basis to have “designed internal controls” over financial reporting, “evaluated the effectiveness” of internal controls, and reported to the Audit Committee and external auditors “all significant deficiencies in the design or operation of internal controls which could adversely affect the ability to record, process, summarize, and report financial data and have identified for the [external] auditors any material weaknesses in the internal controls” and to report “any fraud”.

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 for financial reporting” and that management has performed “an assessment of the effectiveness of the internal control structure and procedures for financial reporting.” In addition, the external auditor must independently assess the corporation’s internal control report.

So after looking at the Sarbanes-Oxley Act, you have only learned that “internal controls” are required for “financial reporting” and that the “internal controls” must be assessed on an annual basis. The SEC and PCAOB are responsible for implementing the actual rules. The SEC final rules require corporations to use a recognized internal control framework and specifically references the Sponsoring Organizations of the Treadway Commission (COSO) internal control framework. We are finally getting somewhere – a framework and usually frameworks are good things.

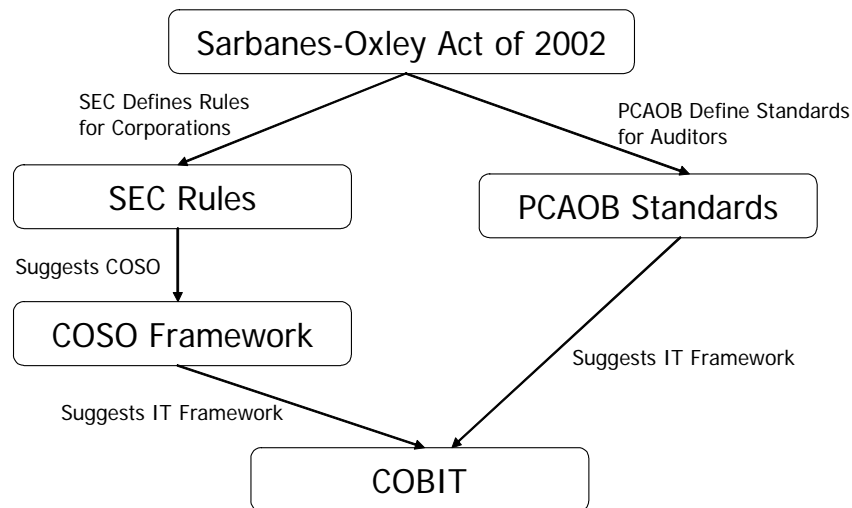


Figure 1. Sarbanes-Oxley Act and Related Control Frameworks

COSO provides an comprehensive framework for defining and evaluating internal controls, but only addresses IT controls in a very general manner and does not provide any specific requirements for IT control objectives or activities. IT general controls are defined as “Policies and procedures that help ensure the continued, proper operations of computer information systems. They include controls over data-center operations, systems software acquisition and maintenance, access security, and application system development and maintenance. General controls support the functioning of programmed application controls. Other terms sometimes used to describe general controls are general computer controls and information technology controls.” COSO identifies five essential components of effective internal control – (1) control environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring.

The PCAOB as part of its rule making process released “Auditing Standard No. 2” that emphasizes the important of IT controls, but does not provide any details on what IT controls are required. The PCAOB auditing standards look for each corporation to develop IT controls that support their internal control program.

Both the PCAOB auditing standards and COSO suggest, in a roundabout way, the use of an IT control framework. The most widely recognized IT control framework is the Information Systems Audit and Control Association (ISACA) framework Control Objectives for Information and related Technology (COBIT). Many corporations have adopted COBIT as their standard IT control framework, especially related to SOX compliance. To assist companies, the ISACA has developed a whitepaper "IT Control Objectives for Sarbanes-Oxley", which maps COBIT to Sarbanes-Oxley compliance.

COBIT is framework for IT governance for the entire organization and provides high-level control objectives for applications and infrastructure, but 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, but does provide any level of detail. An example of a COBIT control objective is –

DS5.3 Identity Management

All users (internal, external and temporary) and their activity on IT systems (business application, system operation, development and maintenance) should be uniquely identifiable. User access rights to systems and data should be in line with defined and documented business needs and job requirements. User access rights are requested by user management, approved by system owner and implemented by the security-responsible person. User identities and access rights are maintained in a central repository. Cost-effective technical and procedural measures are deployed and kept current to establish user identification, implement authentication and enforce access rights.

Other sources of guidelines and best practices for IT controls are ISO 17799 (security related) and the Information Technology Infrastructure Library (ITIL). Both provide varying levels of detail, but still are too high-level for immediate use by the DBA.

Sarbanes-Oxley Compliance

As you can see, 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. It is important to understand the foundation for the SOX compliance requirements, since these requirements may differ from organization to organization. Some companies may choose to implement only COSO and not an IT controls framework such as COBIT, while other companies may choose to use multiple control frameworks. Essentially, because every business assesses risks differently, the controls each business requires will be different.

While understanding the principles and requirements for SOX compliance for the corporation helps, it does not answer the questions of what must be done to the database, applications servers, applications, and operations to achieve SOX compliance.

Looking at SOX Compliance

There are really two groups of people who look at SOX compliance – (1) corporate officers who must attest to the corporation's internal controls and (2) external auditors that assess the effectiveness of such internal controls. Corporate officers rely on internal audit and SOX compliance teams to catalog and assess the corporation's internal controls.

For external auditors, the PCAOB standards require auditors to understand the flow of transactions (how transactions are initiated, authorized, recorded, processed, and reported), which may involve IT systems and applications. In most cases, the external audit firm provides "their" version of requirements in the form of a Sarbanes-Oxley assessment and findings. Often this assessment is performed by audit generalists who do not have experience with Oracle Applications, but instead understand financial controls and business processes.

Reactive vs. Proactive SOX Compliance

Most Oracle Applications implementations take a reactive approach to SOX compliance. Few companies take a proactive approach to SOX compliance and put in place a set of general IT controls and application controls that will meet the stringent requirements of SOX.

The IT organization most likely performed a SOX self-assessment and provided appropriate documentation on policies and procedures to a SOX compliance team. Some control weaknesses or deficiencies were probably identified and hopefully corrected. Depending on the knowledge and experience of the IT internal auditors or external audit firm, even a controls review of the Oracle Applications implementation may have been performed. Usually, the Oracle Applications controls review focused on segregation of duties and other functional aspects of the application. The auditors may have “poked around” the DBA’s realm and potentially identified some weaknesses in terms of generic account usage, default passwords, etc. Most companies have a reactive approach to SOX compliance Oracle Applications, with the exception of segregation of duties and other functional internal controls. The approach for Oracle Applications related IT general controls is if the auditors find it, we will fix it.

SOX is a WRITE Event

The first and foremost concept when thinking about SOX is that SOX is primarily focused on write events, not read 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. Processing includes the actual manipulation of the data such as GL Posting, but also includes changes to the programs and reports.

Think about every way that financial data may be inserted, updated, and deleted in Oracle Applications. Now add in the all the programs, interfaces, reports, and configuration settings that affect how the data is processed and reported. The scope can be staggering in terms of the number of ways and methods that data is changed in Oracle Applications – even the simplest use of the APPS account must now be scrutinized.

Even though SOX compliance may not be focused on read events, unauthorized querying or viewing of Oracle Applications data may be an issue in terms of HIPAA, GLBA, US and European privacy laws, and SEC rules. Also, a strong argument can be made that SOX compliance includes read events since fraud and other financial manipulation may only require knowledge of bank account numbers or financial results prior to public release. This argument can be countered with the following – (1) by implementing a strong set of internal controls for write events, these controls will probably prevent or detect most unauthorized inquiry or query access to the data, (2) the risk to the corporation of the write events probably far exceeds the limited risk of such unauthorized query access, and (3) unauthorized query access probably will not result in a material weakness in the audit report.

About SOX Compliance

The foundation of SOX compliance is about risk. Internal controls are about controlling and reducing risk. Unfortunately, the way a DBA views risk is much different than management or an external auditor. For a DBA, risk is about having backups, able to recover from disk failures, potential performance issues with a developers SQL statement, and the possible impact of the latest Oracle patch. For management and external auditors, risk is viewed in terms of cost/benefit and fraud.

SOX compliance should be done in the context for an enterprise-wide SOX initiative or as part of an IT project. However, these initiatives and projects are either documentation driven exercises or do not drive to the level of detail required for most Oracle Applications implementations. Since Oracle Applications is often the financial system of record, the auditors (both internal and external) will focus on this application

much more than all other applications and systems. Since external auditors are required to examine the flow of key transactions through the organization and IT systems, most likely such transactions will require the financial system to garner close scrutiny. Thus, the DBA often is required to meet a higher standard of SOX compliance than the rest of the IT department.

What are Internal Controls

Internal control is a process designed to provide reasonable assurance regarding the achievement of objectives. Controls can be classified as preventative or detective and the processes used to implement a control can be either automated or manual. **Preventative controls** are designed to discourage errors and irregularities from occurring. **Detective controls** are designed to find errors and irregularities after they have occurred.

IT Controls can be grouped into two categories: IT General Controls and Application Controls. IT General Controls are related to common IT services like disaster recovery, incident response, change management, system development, and computer operations. Application Controls are embedded in the application and designed to achieve accuracy and validity and include authorization, input edits, reconciliations, and approvals.

When designing and implementing controls, the preference for a preventative vs. detective or manual vs. automated control is entirely related to the context and risk associated with the activity being controlled. DBAs tend to prefer automated, preventative controls since in the database administration world automation of processes and prevention of issues are goals. There is nothing wrong with manual, detective controls, especially with low risk activities and when the cost of automating such a control can not be justified.

Internal Controls for Oracle Applications

If you map COSO, COBIT, ISO 17799, and PCAOB Auditing Standard #2 to the general IT and application controls required for an Oracle Applications implementation, you will have a matrix that looks like the following –

		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

Figure 2. Oracle Applications IT Control Objectives

This matrix does not provide a complete set of IT control objectives for an Oracle Applications implementation for every organization, but does provide a foundation in which to evaluate the set of IT controls required across most organizations. Only the IT controls required for the technical aspects of maintaining and operating Oracle Applications are included. Application level controls that can be considered functional, such as functional segregation of duties, reconciliations, etc., are not included. Also, general IT controls, such as IT governance, are not included.

1. Security

Internal controls must be maintained for secure access to the application and to prevent unauthorized access at the application, database, and operating system level. Security related internal controls are mostly preventative controls that attempt to stop an unwanted event from occurring. Detective controls are also used, such as the periodic review of user accounts and access privileges by management.

Password management is covered by COBIT, but does not include any details on what is required in terms of a password policy. ISO 17799 does have more detailed guidance on password usage. The critical issue for password management is that the passwords for all database accounts and application users adhere to the enterprise password policy. The auditor should only assess adherence to the enterprise password policy for both database accounts and application users, not mandate specific password characteristics such as password length. The one exception is that Oracle does not support using database password profiles for registered database accounts in Oracle Applications. Since this would be non-adherence to the enterprise password policy, a management approved manual policy and procedure must be documented for the password requirements for these database accounts and the periodic changing of the passwords. Due to weaknesses in the Oracle database password algorithm, it is strongly recommended the minimum password length for these database accounts be 9 and the passwords are changed every 90 days or when cloning the database to development and test environments.

1.1 User Management

- Essential for effective control and segregation of duties is the 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.). For strict adherence to the enterprise password policy may require a custom password validation routine (Signon Password Custom profile option).
- The new user account creation policy and procedure should require new accounts to be created with a unique password and require the password to be changed upon first login.

1.2 Segregation of Duties

- Segregation of duties for functional responsibilities should be evaluated on a routine basis and on a periodic basis appropriate managers should review all responsibility assignments.
- 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 system administrators and limited to only necessary functions. "System Administrator" should be limited and only used when required. Especially important is access to functions that allow for the execution of SQL statements (e.g., creating alerts).

1.3 Database Security

APPS Account

- The APPS account and all other Oracle Applications database accounts should be limited only to the DBA group or a subset of the DBA group.
- All DBAs and support staff should have individual database accounts with no write access to the database when performing daily support and troubleshooting activities.
- A change control ticket should be required for any usage of the APPS or other Oracle Applications database accounts.
- Consider creating an "APPSIF" database account with insert, update, and delete privileges to Oracle Applications and custom interfaces tables that may need to be directly updated. A change control ticket should be required for any access to this database account. A database login trigger can be used to automatically enable a trace of the session.

Database Passwords

- All database accounts should require periodic password changes and conformance to the enterprise password policy.
 - Registered Oracle Applications database accounts should have a manual policy and procedure requiring changing every 90 days or during a routine maintenance window.
 - All other database accounts should have database password profiles enabled with a custom password authentication function to enforce the enterprise password policy.

Privileges and Access

- All database accounts should be reviewed on a periodic basis to verify appropriate access.
- All database privileges should be reviewed on a periodic basis to verify appropriate privileges.

1.4 Operating System Security

- All access to the standard Oracle operating system accounts *oracle* and *applmgr* should be controlled and the appropriate logs maintained to identify the individual accessing these shared accounts. It is not practical or feasible within Oracle Applications to require individual administrators to use only named UNIX accounts.
 - Use tools like sudo or Symark Powerbroker to provide detailed tracking of commands and usage and mapping usage to individual operating system accounts

- All usage should be tied to a change control ticket.
- 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

By default, the Oracle Database and Oracle Applications are not compliant with SOX. In the default installation, there is no auditing enabled for either the Oracle Database or Oracle Applications. Oracle Applications maintains creation and last modified information for almost every record, but generally does not provide any history of changes to records. For SOX compliance, a history of changes to critical configuration settings and controls is required.

When enabling auditing, performance is always a valid concern. For the most part, auditing non-transactional tables should only have a minimal performance impact. Auditing transactional, high-volume tables can and will have a severe performance impact. Prior to enabling any auditing, careful review of the exact tables and audit settings is required. Assume at least 1-5% performance impact in terms of additional database writes and table space for a minimum set of SOX auditing at the database and application level. Many auditors look for auditing to be enabled on transactional tables such as vendors (especially addresses), which most likely will require discussions with management to assess the risk and potential impact on performance (and the cost of hardware upgrades).

Configuring and enabling auditing is the simple part. Oracle does not provide any tools to manage the audit data, such as archiving, purging, and reporting. Procedures, scripts, and reports must be developed in order to have any gain meaningful results from audit data. The complexity and effort required to develop these procedures, scripts, and reports should be supported by management (i.e., resources and dollars) based on management's assessment of risk.

2.1 Application Auditing

Auditing Configuration Settings

- Signon:Audit should be set to FORM.
- FND_UNSUCCESSFUL_LOGINS should be continuously monitored for repeated unsuccessful logins.
- In 11.5.10 and onwards, Page Access Tracking should be enabled.

Oracle Applications AuditTrails

- Oracle Applications AuditTrails is required for key user management tables like FND_USER, FND_RESPONSIBILITY, FND_FORM_FUNCTIONS, FND_MENU, FND_RESP_FUNCTIONS, FND_USER_RESP_GROUPS, etc. to maintain a history of changes.
- FND_ORACLE_USERID should be audited to have a history of password changes to the registered Oracle Applications database accounts, since changing of these passwords is a manual control and a balancing detective control is required.

2.2 Database Auditing

Database Session Auditing

- Database session auditing should be enabled.
- All access to the APPLSYSUB account not from an application server (ADI is an exception to this rule) should generate an alert.
- All access to the APPS account and all other Oracle Applications database accounts (e.g., GL) not by the application (web, forms, or concurrent manager server) should be limited and directly attributable to a change control ticket.

SYS and SYSTEM Auditing

- All access to the SYS and SYSTEM accounts should be audited using the database initialization parameter AUDIT_SYS_OPERATIONS and all usage directly attributable to a change control ticket.

Other Auditing

- The FND_PROFILE_OPTIONS and FND_PROFILE_OPTION_VALUES tables can not be audited using the Oracle Applications AuditTrail functionality, therefore, custom database triggers need to be created to track changes to these two tables.
- “AUDIT SYSTEM AUDIT;” will provide an audit trail of changes to the auditing.
- “AUDIT PROFILE;” will capture any changes to the database profiles.
- “AUDIT USER;” will provide an audit trail of changes to the database accounts, including add, changes, and deletes.
- No other auditing should be mandatory for SOX compliance, but it is recommended to enable the following database audits: ALTER SYSTEM, ALTER DATABASE, and PUBLIC DATABASE LINK.

3. Change Management

Change control is critical to SOX compliance since not only changes to data should controlled, also any changes to the programs and reports that manipulate or summarize financial data must controlled. Policies and procedures must be in place that provide management approvals and detailed tracking of such changes. Auditors typically will review changed objects, such as programs or reports, and trace the paper trail of these changes back through the change management process. Not having a well-documented change management process and poor or missing change control documentation may result in a weakness or deficiency.

Change management should include all changes to all layers of the technology stack including the application, database, application servers, operating system, and hardware. Changes may include configuration of the application, object migrations (program, reports, etc.), database schema changes, database configuration changes, and patches.

Each change must be logged, assessed, and authorized prior to implementation to ensure the integrity and stability of the system and application. The key characteristics of a change management process are that it is formal (well-documented), changes are handled in a standardized manner, and changes are assessed in a structured way for impacts on the system and its functionality. Even in a well-controlled change management process, emergency changes are perfectly acceptable as long as there is a defined and documented process for such changes.

Most organizations do have mature change control processes, but often lack the appropriate documentation, lack a formal process for emergency changes, or do not require all changes to use the change management process. One notable exception to the change management process for many organizations is changes to application profile options. Since the profile options may affect the processing of financial data, they should be included in the change management process. However, in many organizations, users outside of IT (usually super-users) have access to change the profile options of a module, thus it is difficult to implementation change control for profile options.

4. Monitoring and Troubleshooting

Monitoring and troubleshooting is often included in the scope of SOX compliance because a poorly managed environment could affect the accuracy and completeness of financial reporting. As an example, a daily interface program for journal entries that does not complete successfully and is not detected, may result in a misstatement (probably not material) of financials results.

The auditor is typically looking at how are the system and application monitored for key activities and events related to financial processing. Are interface logs reviewed on a daily basis or is an alerting

mechanism in place in case of interface failures or errors? Does a problem resolution process exist that includes both functional users and IT? When errors do occur in financial programs (e.g., posting) or interfaces, how are the errors resolved (direct table updates, changes to the interface file, etc.)?

5. Availability

The loss of data, including transactions, could affect the accuracy and completeness of financial reporting. Also, in adherence to SEC rules and regulations, a public company must accurately and timely file financial reports, therefore, appropriate disaster recovery and business continuity plans must be in place. Since the SEC defines the rules for SOX, backup and recovery and business continuity are fully in scope for SOX compliance.

The auditor will be primarily looking that documented policies and procedures exist and that these policies and procedures are tested on a periodic basis. The following policies and procedures should be in place

- Backup storage and retention policies and procedures
- Backup and recovery procedures
- Backup and recovery test plans and results
- Disaster recovery and contingency plans
- Disaster recovery test plans and results

Working with Auditors

The job of the auditor is to assess the effectiveness of the internal controls in place and to identify weaknesses or deficiencies in the internal controls. It is important to note that the external auditing standards state inadequate documentation of a control process should be considered a deficiency, so every control process must also have the appropriate documentation. Often the audit is performed by audit generalists who do not have experience with Oracle Applications, but instead understand financial controls and business processes. The findings are then forced on the DBA to remediate, usually in a short timeframe with little understanding or direction on what is truly required.

It can be very frustrating for DBAs to work with auditors who do not understand Oracle Applications. In these situations, many of the findings and identified weakness are not applicable to an Oracle Applications environment or are completely unsupported by Oracle. These findings create the proverbial fire drill for the DBA in which significant effort must be put into research and documentation.

One such example is the often cited auditor finding of the O7_DICTIONARY_ACCESSIBILITY being set to TRUE (it may be set to FALSE only in 11.5.10 and onwards). The finding is actually a valid risk and does pose a security threat especially with the APPLSYSPUB account. However, changing of the parameter is unsupported by Oracle and not recommended. In these types of situations, a valid response is "... management is willing to accept the risk versus the risk of Oracle Corporation not supporting the application ...". For documentation purposes, you will need the CIO's signoff and a TAR may have to be opened with Oracle to provide a paper trail.

Management is able to accept risk when the potential risk is manageable or the cost of remediation is out of proportion to the risk. As an example, the Oracle Database and Oracle Applications have significant limitations in terms of securing the audit trail and logging data. The Oracle Database audit data can be stored in secure location, but it makes reporting and monitoring difficult. The Oracle Applications audit data is stored in shadow tables in the database, therefore, the DBA has full access to modify the audit data. Solutions to these issues, usually add-on products, can cost \$100-500K. Management has the option to assess this risk and to accept the risk of DBAs potentially altering the audit data versus the potential cost of implementing a costly logging and auditing solution.

Manual controls and acceptance of risk are possible solutions to a finding, especially those findings that are difficult or impossible to remediate in Oracle Applications. A prime example is the use of the APPS

account for maintenance and troubleshooting. In order to remediate the issue of excessive privileges associated with the APPS account, one company put in place manual controls that (1) only allowed 2 DBAs to have access to the APPS password, (2) database session auditing was enabled and a log of non-application use of the APPS is reviewed monthly by the DBA manager, and (3) each use of the APPS account must be documented in a change control ticket. This weakness was remediated with the combination of management accepting the risk of 2 DBAs having the APPS password with unlimited access to the data and manual controls to monitor the usage of the account. The auditor then assessed the new manual controls by sampling several usages of the APPS account to ensure change control tickets existed.

References

- Sarbanes-Oxley Act of 2002 - <http://www.sec.gov/about/laws/soa2002.pdf>
- COSO Internal Control – Integrated Framework - www.coso.org
- ISACA COBIT 4.0 - www.isaca.org
- PCAOB Auditing Standard #2 - www.pcaob.org
- Integriy Guide to Auditing in Oracle Applications - <http://www.integriy.com/info/IntegriyOracleAppsAuditing.pdf>

About the Author

Stephen Kost is the Chief Technology Officer for Integriy Corporation. He has been presenting on Oracle Applications security for the past 5 years and has worked with Oracle Applications since 1992 in many roles including DBA, technical architecture, IT security auditor, and system administrator. For the past 2 years, he has assisted many companies in their Sarbanes-Oxley compliance efforts related to Oracle Applications.