



Auditing Oracle Applications Primer for Internal Auditors

Detailed in this paper are some key concepts that internal auditors need to understand when auditing Oracle Applications. We hope this information will be valuable to you and your company.

Application Security Design

Most implementations do not take a proper approach to designing security. Often they use standard responsibilities and menus rather than a risk-based 'principle of least privilege' approach. Access is commonly given based on seeded responsibilities and menus with menu and function exclusions applied. Often, this results in excessive access to setups and functions that are not appropriate for all users. Also, the use of seeded menus and responsibilities introduces 'upgrade risk.' Upgrade risk in this context refers to the risk of new functionality and access to data being introduced when patches are provided by Oracle that grant new access to users that has not been properly evaluated. This could lead to segregation of duties violations, inappropriate access to sensitive functions, or inappropriate access to sensitive data.

Generally, too little attention is paid to access to concurrent programs and access to sensitive data contained in standard reports. We recommend a 'principle of least privilege' approach including defining request group requirements for each responsibility individually. During many implementations standard request groups such as All Reports/Payables are used for all responsibilities within that module, which leads to excessive exposure to concurrent programs (those that update data or run interfaces) and access to sensitive data (like sensitive employee data stored in AP).

We make the following recommendations:

- Take a risk-based approach to design security that takes into account risks related to segregation of duties, access to sensitive functions, and access to sensitive data.
- Discuss the approach to security with your system administrators and IT management to make sure the principle of least privilege was followed and is being followed in the design of security. This includes only giving access to those functions in Oracle that a user needs, not using a seeded menu and backing out those functions that don't seem appropriate.
- Discuss the upgrade risks associated with the use of standard menus or standard responsibilities with IT management.
- Join the [internal controls repository](#) and download the white paper "Risk Based Assessment of UAC and SOD White Paper"
- Discuss the methodology used for determining which concurrent programs and reports are granted to a given responsibility.

- Join the [internal controls repository](#) and review the information in the file called “Reports with Access to Sensitive Data” which can be found in the Internal Controls Content folder. Participate in the development of public domain content by adding to this list.

IT Security

Oracle provides guidance in its Metalink Note (Note 189367.1 for 11i, Note 403537.1 for R12) called “Best Practices for Securing your E-Business Suite” that companies often are not aware of or don’t take the time to follow the guidance.

We make the following recommendations:

- Monitor security resources that can be found at www.integrity.com, www.solutionbeacon.com, and www.petefinnigan.com.
- Download a [primer](#) on IT security from Integrity
- Discuss the guidance in Oracle’s best practices document with IT management to determine where your company may have deficiencies.
- Consider having a firm specializing in Oracle Application security give you an assessment of your security.
- Join the public domain [listserver](#) we host related to internal controls and security in an Oracle Applications environment. Review the archives and use the listserver to post questions.

SQL Forms and Utilities: Diagnostics

A user can execute SQL statements without a database login by embedding a SQL statement in several forms, most of which are documented in Appendix B of Oracle’s Best Practices for Securing your E-Business Suite” document. A user can also access the database directly when given access via the Utilities: Diagnostics profile option.

Activity in the SQL forms can only be monitored through the use of a trigger-based or a log-based auditing solution. Not all trigger based solutions can effectively audit the activity because the SQL statement is stored in a column with a data type of ‘LONG’. When evaluating trigger-based auditing solutions, make sure you asked about this distinction and see a demo of the functionality related to auditing SQL forms.

We make the following recommendations:

- Consult with ERP Seminars when evaluating solutions to audit this data as we are working with several companies to develop public domain content for monitoring these forms and other forms with various levels of risk.
- Join the [internal controls repository](#) that we host and download the white paper titled “Accessing the Database Without a Database Login”

Internal Controls and Security Deficiencies

We have developed a list of common internal controls and security deficiencies in the Oracle E-Business Suite and ways companies mitigate the risks associated with the deficiencies. Having an understanding of these deficiencies will most likely lead to a list of development efforts you would recommend to management that may include the following:

- Forms personalization to provide preventive controls related to some identified risks
- Custom reports or queries for monitoring of certain risks
- Implementation of a solution to monitor or prevent SOD and user access control risks
- Implementation of a solution to provide trigger-based or log-based auditing to provide a detailed audit trail for risks such as SQL forms, development and security activity, monitoring of setups related to application controls, and in support of your change management process

We make the following recommendations:

- We recommend that you join the [internal controls repository](#) and download the content to review. You should evaluate this list of deficiencies and discuss the risk identified in this list with your end users and management.
- Participate in the development of this public domain list of deficiencies so other end users can share in this knowledge

Sensitive Data in Non-Production Environments

Sensitive data is just as important to protect in non-production environments as it is in your production environment. However, companies often provide more liberal access to employees and contractors at the application and database layers in non-production environments which leaves sensitive data excessively exposed.

We make the following recommendations:

- Sensitive data should be scrambled during the cloning process. Scrambling involves changing the data from its original value to a different value. For example, changing all salaries to an hourly rate of \$7.00/hour
- Download a listing of common sensitive data and in which tables and columns in the database it is stored by joining the [internal controls repository](#) and access the file “Oracle Apps Sensitive Data” in the Internal Controls Content folder in the Files section.
- Participate in the development of this public content so other end users can share in this knowledge
- Look for our full white paper on this topic that will be released soon. Sign up for our email list on our [website](#).

Application Controls

We have written a white paper discussing the impact of the Institute of Internal Auditor's guidance on the Auditing of Application Controls that would be helpful for you to read.

We make the following recommendations:

- Join the [internal controls repository](#) and download the white paper "Auditing Application Controls"
- Download the [IIA guidance](#) to review

Change Management

We have identified several challenges related to the change management process common to most companies. We use the Institute of Internal Auditor's guidance provided in the Global Technology Audit Guide called "Change and Patch Management Controls: Critical for Organizational Success".

Here is a listing of common change management challenges:

- Profile Options not being considered
- Changes to security not being considered
- Failure to take into account access to sensitive data in security process changes
- Failure to take into account request groups access in design of security
- Forms-based setups not being considered
- Change made in various forms that allow SQL statements embedded in them are not required to go through change management process
- Excessive access to forms requiring change management
- Failure to clearly document who is responsible for implementing change
- Failure to test for unauthorized changes
- Failure to remediate issues that allowed the unauthorized changes
- Failure to maintain documentation
- Poor impact analysis leading to a poor testing process

We make the following recommendations:

- Look for our full white paper on this topic that will be released soon. Sign up for our email list on our [website](#).
- Download the [IIA guidance](#) to review

Other Resources and White Papers

There are other sources of information for internal auditors. We make the following recommendations:

- Stay current with information for auditors at [AuditNet](#)
- Request other white papers at the [Oracle Users Best Practices Board](#)
- Access other white papers not available to the public by joining the [internal controls repository](#) and checking the White Papers folder in the Files section
- Consider purchasing my book “Oracle E-Business Suite Controls: Application Security Best Practices” – see link at [ERP Seminars home page](#).

Comments and feedback regarding this paper should be addressed to the author at jhare@erpseminars.com or by completing a [reviewer feedback form](#).

About the Author

Jeffrey T. Hare, CPA CISA CIA is one of the leading experts on the development of internal controls and security in an Oracle Applications environment. Jeffrey founded ERP Seminars and the Oracle Users Best Practices Board and is leading the efforts for the development of a public domain internal controls repository. See a full bio for [Jeffrey](#).

Version Control

Version	Updated by	Date	Comments
1.0	Jeffrey Hare	25-Jan-08	Initial release
2.0	Jeffrey Hare	5-Jan-10	Updated for book and for reference to R12 best practices document