



## **Auditing Application Controls: Interpreting IIA's Guidance for Users of Oracle Applications**

This newsletter focuses on an interpretation of the Institute of Internal Auditors (IIA) Global Technology Auditing Guide called “Auditing Application Controls.” This guide was published in July 2007 and is another excellent resource published by the IIA. The target audience is internal auditors and we will do our best to interpret this document for all parties involved including finance and IT management. The guide can be downloaded at:

<http://www.theiia.org/guidance/technology/gtag/gtag8/>.

Referring to the PCAOB guidance on application controls, the guide states “the nature and extent of the evidence the auditor should obtain to verify the control has not changed may vary, based on circumstances such as the strength of the organization’s program change controls. As a result, when using a benchmarking strategy for a particular control, the auditor should consider the effect of related files, tables, data, and parameters on the application control’s functionality.”

The guide makes three critical points that we will address because we have seen significant deficiencies in the processes for companies running Oracle Applications that need to be remediated immediately. First, it identifies benchmarking as a critical process in maintaining the reliance of application controls. Second, it addresses the critical nature of general computer controls (commonly referred to as GCCs or ITGCs) in support of application controls. Third, it discusses the possibility of manipulating system level controls such as tolerances and purchase approval controls during the entry of transactions.

### **Impact of Guidance on Benchmarking**

The essence of benchmarking is that for application controls, a company benchmarks the configurations related to that application control. That is, they identify the values of the related setups pertaining to the application control at the beginning of the period. When determining the operating effectiveness of the control, an auditor can rely on the control from year to year as long as the values that were “benchmarked” haven’t changed. If the values were to have changed, the auditor would want to ‘re-benchmark’ the values by evaluating the impact of the changes on the design effectiveness, perhaps by doing a walkthrough of the process after the change. So, the benchmarking process is critical for the auditor to know to what extent they can rely on the application control from year to year (note that the PCAOB guidance does suggest that the

application control be reviewed every three years even if the configuration of that control hasn't changed).

Therefore, the configurations related to each application control are critical to monitor. Absent an ability to tell if a change has been made or what change has been made to the application controls, the reliability of the application controls will be called into question by your auditors.

We will look at the journal approval workflow in the general ledger as an example. Later we will look at the matching requirements (2-way, 3-way, or 4-way) in the purchasing module when discussing

***Benchmarking the Journal Approval Workflow Process in Oracle's General Ledger Module***

First, we'd like to point out a white paper called "Internal Control Best Practices for Implementing Oracle's Journal Approval Process" which can be accessed by end users by joining the Internal Controls Repository at:

[\(http://tech.groups.yahoo.com/group/oracleappsinternalcontrols/\)](http://tech.groups.yahoo.com/group/oracleappsinternalcontrols/). In this paper we point out the internal controls issues with the implementation of this workflow. One of the key setups is the determination of which journal sources are required to be subject to the journal approval workflow. The Journal Sources screen is as follows:

Source	Description	Require Journal Approval	Freeze Journals	Import Journal References	Effective Date Rule
Receivables	Accounts Receivable System	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Roll Date
Recurring	Recurring Journal Entry	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Roll Date
Revaluation	Revaluation Journal Entry	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Roll Date
Revenue	Revenue Accounting System	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Roll Date
SM_Journal Source	SM_Journal Source	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Roll Date
SN SOURCE	SN SOURCE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Leave Alone
SS SOURCE		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Roll Date
SSA PAYABLES	SAGAR PAYABLES IMPORT	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Roll Date

In this form, you can see where the Require Journal Approval button is checked for each of the sources. You can also see where other information is maintained for each source such as Freeze Journals, Import Journal References, Description, and Effective Date Rule. The risk impact depends on how the data is stored.

Here is an example of how the data looks in the GL\_JE\_SOURCES table (not actual column names for you techies, but will illustrate the issue):

Source Name	Description	Freeze Journals	Require Journal Approval	Last Updated By	Last Updated Date
Receivables	Accounts Receivable System	Yes	Yes	HAREJ	01-Jan-06

If the challenge is to benchmark the setups related to the journal approval process, then the benchmarked values for Receivables source would be 'Yes.' However, let's look at the impact of a change made to the journal sources, but for the Freeze Journals value which could happen if the journal when imported to the GL needed to be updated. So, a call is placed during November month end (Nov-7) to a business analyst by the accounting manager to uncheck the freeze journals button so the journal entry can be updated in the GL. The values after this change would be as follows:

Source Name	Description	Freeze Journals	Require Journal Approval	Last Updated By	Last Updated Date
Receivables	Accounts Receivable System	No	Yes	HAREJ	01-Dec-07

Then, after the change is made to the journal, the Freeze Journals button is set back to Yes. This is how the values would like at the database level:

Source Name	Description	Freeze Journals	Require Journal Approval	Last Updated By	Last Updated Date
Receivables	Accounts Receivable System	Yes	Yes	HAREJ	01-Dec-07

When an auditor comes out to look at the benchmarked values of the journal approval process, they will want to know whether or not any of the values related to the setups of the journal approval process have changed. The data in the database would indicate that something has changed related to the Receivables source because the last updated date would be in the period being audited. However, you would have no way of identifying the changes or proving to the auditor that the change made was not related to the journal approval configuration.

The solution is that a detailed audit trail needs to be developed for such changes so that, in this case, the change could be identified as a change to the freeze journals configuration, not the journal approval setup. We originally discussed the need for such an audit trail in a white paper published called “Building an Audit Trail in an Oracle Applications Environment” which can be requested at [www.oubpb.com](http://www.oubpb.com). However, we will reiterate the salient points here.

There are a couple of ways to generate a detailed audit trail – through the use of logs and through the use of triggers.

### *Using Logs to Generate an Audit Trail*

Logs come in multiple forms – database logs or network logs. In laymen’s terms, database logs are internal database and record changes to the database for backup purposes, but can be effectively used for auditing or forensic analysis. Network logs are activity that runs across the network – from a person’s PC to the server(s) that host the applications and database. The pros of logs are that they are external to the application and have no direct impact on the application’s performance (ignoring the potential for shared resources that may control log activity and the application). Let me illustrate their major drawback by using an illustration. Let’s say you wanted to audit any changes to responsibilities in Oracle. Here is a screen shot of the Responsibilities form:

Responsibilities

Responsibility Name: **Receivables Manager**

Application: **Oracle Receivables**

Responsibility Key: **RECEIVABLES\_MANAGER**

Description:

Effective Dates: From **01-JAN-1951** To

Available From:
 

- Oracle Applications
- Oracle Self Service Web Applications
- Oracle Mobile Applications

Data Group:
 

- Name: **Standard**
- Application: **Oracle Receivables**

Request Group:
 

- Name: **Receivables All**
- Application: **Oracle Receivables**

Menu: **AR\_NAVIGATE\_GUI**

Web Host Name:

Web Agent Name:

Menu Exclusions | Excluded Items | Securing Attributes

Type	Name	Description
<b>Function</b>		

One of the fields that you would want to audit is the Menu field (i.e. because of the risk of changing from inquiry to an update menu). Audits in either log-based tools or trigger-based tools are enabled by identifying the tables and columns within each table that you want to audit. So, you identify that the FND\_RESPONSIBILITY table is the table which holds the data related to Responsibilities. Here is a list of columns in this table from the eTRM related to this table:

**Columns**

Name	Datatype	Length	Mandatory	Comments
APPLICATION_ID	NUMBER	(15)	Yes	Application identifier
RESPONSIBILITY_ID	NUMBER	(15)	Yes	Responsibility identifier
LAST_UPDATE_DATE	DATE		Yes	Standard Who column
LAST_UPDATED_BY	NUMBER	(15)	Yes	Standard Who column
CREATION_DATE	DATE		Yes	Standard Who column
CREATED_BY	NUMBER	(15)	Yes	Standard Who column
LAST_UPDATE_LOGIN	NUMBER	(15)		Standard Who column
DATA_GROUP_APPLICATION_ID	NUMBER	(15)	Yes	Data group application identifier
DATA_GROUP_ID	NUMBER	(15)	Yes	Data group identifier
MENU_ID	NUMBER	(15)	Yes	Menu identifier
TERM_SECURITY_ENABLED_FLAG	VARCHAR2	(1)		Flag to indicate if Security by Terminal is enabled for the responsibility
START_DATE	DATE		Yes	The date the responsibility becomes active
END_DATE	DATE			The date the responsibility expires
GROUP_APPLICATION_ID	NUMBER	(15)		Application identifier from report security group definition
REQUEST_GROUP_ID	NUMBER	(15)		Identifier of report security group assigned to the responsibility
VERSION	VARCHAR2	(1)		Version of responsibility. For example, web (W) or AOL (4)
WEB_HOST_NAME	VARCHAR2	(80)		IP address or alias of machine where the Webserver is running. Defaults to the last agent
WEB_AGENT_NAME	VARCHAR2	(80)		Name of Oracle Web Agent. Defaults to the last agent
RESPONSIBILITY_KEY	VARCHAR2	(30)	Yes	Internal developer name for responsibility

Note that what is stored related to the menu is the menu\_id. The menu\_id is a reference to the FND\_MENUS table which is the table that stores the menu name and other information related to that menu. Here is the eTRM related to that table:

Columns				
Name	Datatype	Length	Mandatory	Comments
MENU_ID	NUMBER		Yes	Menu identifier
MENU_NAME	VARCHAR2 (30)		Yes	Menu name
LAST_UPDATE_DATE	DATE		Yes	Standard Who column
LAST_UPDATED_BY	NUMBER		Yes	Standard Who column
LAST_UPDATE_LOGIN	NUMBER (15)		Yes	Standard Who column
CREATION_DATE	DATE		Yes	Standard Who column
CREATED_BY	NUMBER (15)		Yes	Standard Who column
TYPE	VARCHAR2 (30)			TYPE

There is yet another table that holds information relevant to the change – FND\_MENU\_ENTRIES. Here is the eTRM related to that table:

Columns				
Name	Datatype	Length	Mandatory	Comments
MENU_ID	NUMBER		Yes	Menu identifier
ENTRY_SEQUENCE	NUMBER		Yes	The order the menu entry will be shown in the menu
LAST_UPDATE_DATE	DATE		Yes	Standard Who column
LAST_UPDATED_BY	NUMBER (15)		Yes	Standard Who column
LAST_UPDATE_LOGIN	NUMBER (15)		Yes	Standard Who column
CREATION_DATE	DATE		Yes	Standard Who column
CREATED_BY	NUMBER (15)		Yes	Standard Who column
SUB_MENU_ID	NUMBER			Submenu attached to the entry
FUNCTION_ID	NUMBER			Function attached to the entry
GRANT_FLAG	VARCHAR2 (1)		Yes	GRANT_FLAG

So, as an auditor, when a change was made to a menu, you would want to know more than just the menu\_id before the change and the menu\_\_id after the change. Certainly, to give it any context, you would want to know the name of the menu which is stored in the FND\_MENUS table. Therefore, when the audit record is written, you would want to capture certain meta-data related to that record – in this case, the MENU\_NAME field from the FND\_MENUS table.

The problem with log-file based audit trails is there is no mechanism to add cross-references to other tables. The process of building the logs are inherent to the application and cannot be manipulated or customized. Therefore, while the data in the log files may provide a piece to the puzzle in a way that does not interfere with the performance of the application, it may not provide a discernible record that an auditor would need to verify the nature of the change against an approved change control request document. The major challenge for an auditor working with database logs is that the logs contain raw data which must be manipulated and analyzed in order to produce meaningful results.

### ***Using Triggers to Generate an Audit Trail***

Triggers, like logs, come in many forms. Triggers are executed when data is inserted, modified, or deleted and are commonly used throughout the application to initiate events based on certain data transactions. Triggers, for example, are used to fire alerts. Oracle also provides for the use of triggers in building an audit trail that is embedded in the eBusiness Suite.

Triggers can be customized to write audit records so they can be made to be more precise and allow for the writing of other data. Therefore, triggers can be written to capture data from other tables at the time the audit record is written to help enhance the usefulness of audited data.

Because conditions (i.e. 'where' clauses) can be placed on triggers, they can also be used to only write records for certain types of activities such as the monitoring of Super Users or transactions over a certain amount. Also note that triggers can also be written very poorly so as to have an impact on performance and system resources.

Triggers also determine where audit records are written. Most of the third party products on the market build their triggers to

One final comment on the types of triggers in the marketplace, Oracle has standard audit process that is trigger based and can be enabled in the eBusiness Suite through the use of the System Administrator responsibility. The drawback to using this functionality is the decentralized nature of the audit trail. For each table that is audited, a shadow table is created to store the audit records. In an environment where many tables are audited, perhaps that number in the hundreds, the decentralized nature of the audit records causes a lot of extra burden on a company. That burden includes a significant number of additional hours to build and maintain audit queries because each query has to be written individually against each particular audit table. It also includes DBA maintenance hundreds of additional tables.

In the Summer of 2007, Oracle released a technology product called Audit Vault that may take the place of the standard audit trail in the Oracle E-Business Suite. However, as of the writing of this white paper, we have not been able to verify whether it is certified to work with the E-Business Suite and is able to capture the necessary session information such as the E-Business Suite user\_id.

### ***Using Standard Table Information for Benchmarking***

I'd like to make one additional comment on the use of data that is standard in each table (created\_by, creation\_date, last\_updated\_by, last\_updated\_date) for benchmarking. Some have suggested that benchmarking can be done by using this information because the absence of a date in the period under audit would indicate to an auditor that the benchmarked configuration remains the same. However, as the example above related to the Journal Sources configuration indicates there could be a change to another setting not related to the benchmarked control in the same table that would indicate a false positive. However, due to the lack of information to

support your assertion that the benchmark hasn't been changed, the auditor would like no be able to rely on that control. This would likely cause them to re-test the application control or resort to testing that particular process in their substantive audit work. Either way, the increase in scope of their testing would likely result in audit overages. Additionally, as we will see below in the section on ITGC's, there are cases where you cannot gain comfort as to the appropriateness of changes without the use of a detailed audit trail supported by either the log or trigger-based processes described above.

### **Impact of Guidance on Testing of ITGC's**

The critical commentary in the IIA guidance on the importance of ITGC's states that "if the ITGC's that monitor program changes are not effective, then unauthorized, unapproved, an untested program changes can be introduced to the production environment, thereby compromising the overall integrity of the application controls." In other words, if your change management process is not effective, then it can compromise the reliance on application controls. Where I see this having the greatest area of risk for companies is in the completeness of their ITGC process. That is, most companies fail to take into account certain changes made through the forms as needing to go through a company's change management process. There are two types of changes that I see companies are at great risk – SQL forms and foundational setups.

Before commenting specifically on those two types of changes, let me a couple of general comments on "Change Management". Change management is typically thought of as an "IT" process. That is, the purpose of change management is to make sure that IT changes go through a review and approval process before the changes are implemented into the Production environment. The essence of the change management process is to protect the Production environment from unintended consequences or unapproved changes. What the change management process is attempting to protect is the integrity of the business process which it supports because IT is merely an enabling agent for the business process. The code being changed isn't 'the end', but merely a means to 'an end.' The 'end' is an effective (and, hopefully, efficient) business process. So, the goal of an effective change management process should be to protect the integrity of the business process (and the related data). Historically, all changes made to the business process had to be made via IT code changes. In other words, a programmer was required to manipulate the code in order to change how the business process was effected in the system. However, with the advent of ERP systems that has changed. It is no longer the case that a developer has to change the code in order for the software to act differently. An analyst or end-user can manipulate certain setups that will change the way the system interacts with the users and, therefore, change the business process. Key configurations such as tolerances and PO matching requirements can not be changed without a developer. With this perspective, let's take a look at two types of changes that are made that have yet to fully resonate with companies running Oracle Applications.

### ***SQL form changes and their impact on ITGC***

Most IT managers and guardians of their company's change management process would agree that any script to manipulate data or the structure of the database so go through a company's change management process. However, many companies have failed to take into account that Oracle has provided a mechanism to manipulate scripts or to embed a SQL statement in various

forms. Oracle has identified these forms in its “Best Practices for Securing E-Business Suite document (Metalink Note 189367.1) and recommends restricting access to a small group of users and to consider auditing the underlying tables.

We have identified at least one form that accepts SQL statements that is not documented by Oracle in this document. We have documented this form and have also provided some important cross-reference information from their list in a document in our Internal Controls Repository that is free to end users of Oracle Applications. You can join the ICR at <http://tech.groups.yahoo.com/group/oracleappsinternalcontrols/>. As such, we recommend you stay current with Oracle’s recommendations as well as track our recommendations).

We will make the recommendation more firmly than does Oracle. Absent a detailed audit trail for every change made through these forms, you cannot be certain that those with access to these forms in your production environment aren’t making unauthorized changes to your data or database structure. We recommend a very thorough audit of access to such forms and an approval by management for each person being granted access to such forms.

Further, we recommend a strict approval process for those that gain access in the future. In addition, we recommend that your change management process for changes to menus, responsibilities, forms, and functions also be strictly controlled and audited to make sure they aren’t manipulated to grant access to the SQL forms without management approval. Strict controls on updates to any of these security components through a database login need to be in place, but are outside the scope of this white paper. There is a full white paper for members of the ICR called “Accessing the Database without a Database Login” that would also be a good resource for you to reference.

Finally, we recommend all changes to these forms should be audited and be subject to your change management process. This includes the reconciling of actual changes to approved changes to identify any unapproved changes. Any level less than 100% of changes made versus approved is unacceptable.

### ***Foundational setups and their impact on ITGC***

Another area of great risk from an ITGC perspective is the failure to require changes made to foundational setups to be subject to the change management process. As discussed above, the intent of the change management process is to protect the integrity of the data and the business process. The shift to the use of ERP systems and their configurability should have caused an epic shift in how companies view change management. However, this is one area or risk that has largely gone unrecognized.

Some examples of foundational setups that should be subject to your company’s change management process include Profile Options (set at any level), Journal Sources (GL), Depreciation Methods (FA), Document Types and Line Types (PO), Transaction Types (AR and OM), and PO and Requisition Approval Limits (PO).

Therefore, we recommend companies need to take a risk-based approach to understanding which foundational setups need to be subject to their change management process. We have included

such as access in our risk assessment methodology that analyzes user access controls and suggest that companies take a similar approach in their risk assessment process.

**Impact of Guidance – the override of system level controls during the entry of transactions**

The final significant risk we have identified based on this guidance from the IIA relates to security design. Consider the possibility of manipulating system level controls such as tolerances and purchase approval controls during the entry of transactions.

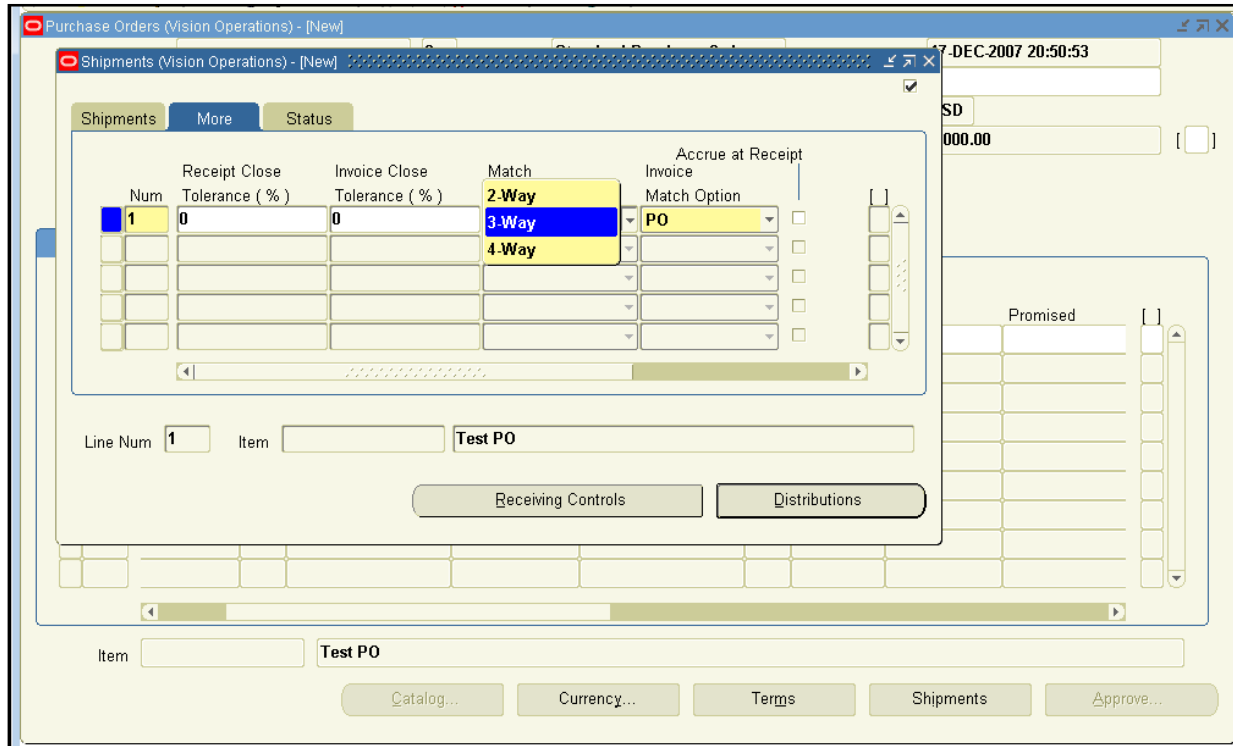
There are some instances where the system level systems can be overridden. For example, in the purchasing options form, you can indicate the desired level of matching – 2-way, 3-way or 4-way. However, this can be overridden by defaulting it at the Supplier level as shown:

The screenshot shows the 'Suppliers (Vision Operations: USD)' form. At the top, there are fields for 'Supplier Name' (JTH Test), 'Supplier Number' (65006), 'Alternate Name', 'Taxpayer ID', 'Tax Registration Number', and 'Inactive On'. Below these are several tabs: 'Accou...', 'Control', 'Payment', 'Bank...', 'EDI', 'Invoi...', 'Withh...', 'Tax R...', 'Purch...', and 'Recei...'. The 'Recei...' tab is selected, showing a list of receipt-related settings:

- Enforce Ship-To Location: Warning
- Receipt Routing: 2-Way
- Match Approval Level: 3-Way (highlighted in blue)
- Qty Received Tolerance: 4-Way
- Qty Received Exception: [dropdown]
- Days Early Receipt Allowed: 5
- Days Late Receipt Allowed: 5
- Receipt Date Exception: Warning

There are also two checkboxes: 'Allow Substitute Receipts' (checked) and 'Allow Unordered Receipts' (checked). A 'Sites' button is located at the bottom right of the form.

Or the match approval level can be overridden when a Purchase Order is created as shown:



The solution for this issue varies depending on your company's matching policy. If you have a strict policy that all PO's must use a three or four way match, then the fix is to prevent update on this form via the use of Forms Personalization (or the use of a custom trigger). If you have a policy where some vendors are allowed a two-way match, then you could put a process in place to maintain that value at the Supplier level and prevent any changes on this form via forms personalization. However, if your policy allows the buyers to choose based on conditions set in your policy, then your only choice may be manual monitoring against that policy. As the guidance mentions, there is risk to relying on the automation of the control if the proper analysis in conjunction with the necessary development, and/or monitoring to monitor the policy.

Your risk assessment process should also include the risk that certain controls such as the PO Match Level can be overridden at the transaction level. The result of such risk analysis may be forms personalization requirements and/or reporting requirements for monitoring certain types of transactions.

### ***Another risk of overriding controls***

Consider also the possibility of manipulating system level controls such as tolerances and purchase approval controls during the entry of transactions. For example, if you have a user with access to maintain PO approval limits that also has the ability to enter a PO, it would allow the user to manipulate their approval limit, issue a PO outside of policy, and then change their approval limit back to what is policy. Without an audit trail of changes made to approval limits, then there would be no discernable way to identify whether such person was circumventing the approval policy.

Therefore, we recommend companies include some transactional-type setups such as PO approval limits, journal authorization limits, and adjustment approval limits in their risk assessment process. The result of the risk assessment process should be that these key setups be subject to change management and an audit trail of these key setups to support the audit of the change management process.

### **Impact of Guidance – direct table updates**

Another important consideration when evaluating the risks discussed above is the direct updating of tables via SQL using a database login. Update scripts don't necessarily track who made changes to the data via SQL scripts unless that information is built into the script. To capture this information, the standards for such updates should require the update of the standard audit fields in the database tables (created\_by, creation\_date, last\_updated\_by, last\_updated\_date. Ideally, any solution for which you are looking to monitor the above risks would take into account changes made through the standard eBusiness Suite or to via direct database login.

### **Conclusion**

As usual, the IIA has provided some valuable guidance to their practitioners. However, the guidance provided exposes some significant deficiencies in many company's change management practices and security design. Will your company be prepared when your internal auditors audit you under this guidance? Will your company be prepared when your external audit firms incorporates such guidance into their SOX audits?

If you are relying on certain application controls in Oracle or other systems, but have not developed the proper processes or audit trail to support those controls, you may be at risk for losing your reliance on such controls or incurring additional audit costs to substantiate these controls. The cost of publicly available tools start from at little as \$25,000 USD implemented and may be a good insurance policy worthy of your consideration.

#### **About the Author**

*Jeffrey T. Hare, CPA CISA CIA*

Jeffrey is the founder of ERP Seminars ([www.erpseminars.com](http://www.erpseminars.com)) and the Oracle User Best Practices Board ([www.oubpb.com](http://www.oubpb.com)) and has written various white papers on Internal Controls and Security Best Practices in an Oracle Applications environment. He has presented white papers to various users groups throughout the country as well as at OAUG and Appsworld conferences. He is the author and presenter of the seminar "Internal Controls and Security Best Practices in an Oracle Applications Environment." His background includes Big 4 experience, over six years experience in CFO/Controller roles, and in the Oracle Applications space since 1997. Jeff can be reached at [jhare@erpseminars.com](mailto:jhare@erpseminars.com).

#### **About ERP Seminars:**

We recognize the need for companies to have continuing knowledge of industry Best Practices. We team with respected independent consultants and firms to provide quality, relevant seminars based on these Best Practices prepared and presented by well-rounded professionals with ERP expertise.

#### **About Oracle Users Best Practices Board:**

The mission of the OUBPB is the aggregation of willing writers and reviewers who will participate in a process to develop Best Practices for the Oracle community. The end result will be a repository of "best practice" white papers and other content for end users and consultants to reference in their projects and ongoing development.

*Version Control*

<u>Date</u>	<u>Author</u>	<u>Version</u>	<u>Reference</u>
15-Jan-08	Jeffrey Hare	1.0	Initial publication