Audit Considerations for your 11i implementation

Author:	Richard Byrom
Organization:	RPC Data Ltd
Position:	Oracle Applications Consultant
Publication	OAUG Insight – Spring 2004
E-mail	richard@rpcdata.com richard@richardbyrom.com
Web Site	http://www.rpcdata.com http://www.richardbyrom.com

Introduction

In the many Enterprise Resource Planning (ERP) implementations I have been involved with, review and audit is an inevitable part of the journey. This is particularly true today with the enactment of the Sarbanes-Oxley Act of 2002 and other worldwide initiatives to enhance corporate governance. The objective of this article is to outline the audit and review features provided by Oracle Applications that can be utilized to provide an improved control environment.

From a control perspective the various Oracle products should provide a business with appropriate levels of general and application controls. **General controls** are those that relate to all information systems. They are designed to ensure that the organisations Information Technology (IT) environment is stable and well managed. Examples include segregation of duties, physical access controls, logical access controls and documentation standards. **Application controls** are those that are specific to applications with a focus on transaction processing. The primary objective of application controls is to ensure the accuracy of a specific application's inputs, files, programs, and outputs. Examples include Source data controls, Input validation routines, on-line data entry controls, output Controls, data processing and file maintenance controls.

All general and application controls can also be classified as either preventative, detective or corrective. **Preventative** controls are those are designed to discourage errors or irregularities from occurring. An example would be the application of cross validation and security rules to a Chart of Accounts to ensure that data is captured correctly. **Detective** controls are designed to find errors or irregularities after they have occurred. An example would be the production of reports to indicate whether accounting information had been correctly captured. Most of the Oracle functionality to be discussed here will relate to detective controls. **Corrective** controls are designed to fix errors or irregularities after they are detected. For example, to adjust a journal raised in error, a journal adjustment form may have to be completed, properly approved, and sent to Finance.

Having considered the types of controls that need to be in place in a business I will now highlight the functionality provided by Oracle Applications and how each of the areas mentioned will help introduce controls that mitigate the various risks that arise in an organisation.

Modular integration

Every system within an organization has three core components namely, financial, operations and Payroll/HR as indicated in Figure 1. Oracle E-Business suite can offer highly integrated solutions for each of these components of the system as they all reside on the same database and share important information. The fact that the modules are highly integrated is a preventative control in that this should ensure all transactional information ends up in the central repository of the general ledger. The key features of modular integration that assist in the audit and review process are the reconciliation reports as well as month end reports which can be found for each particular module. These reports enable reconciliation of inter modular movement to take place. The fact that the modules interface in a standard way also means that it is easy to trace the flow of transactions from one module to the other.

Where 3rd party interfaces exist or are used instead of an Oracle module, as indicated by the red arrows in figure 1, these also integrate/interface in a standard way and hence it is rather easy to trace interfaced transactions online or by printing out pertinent reports.

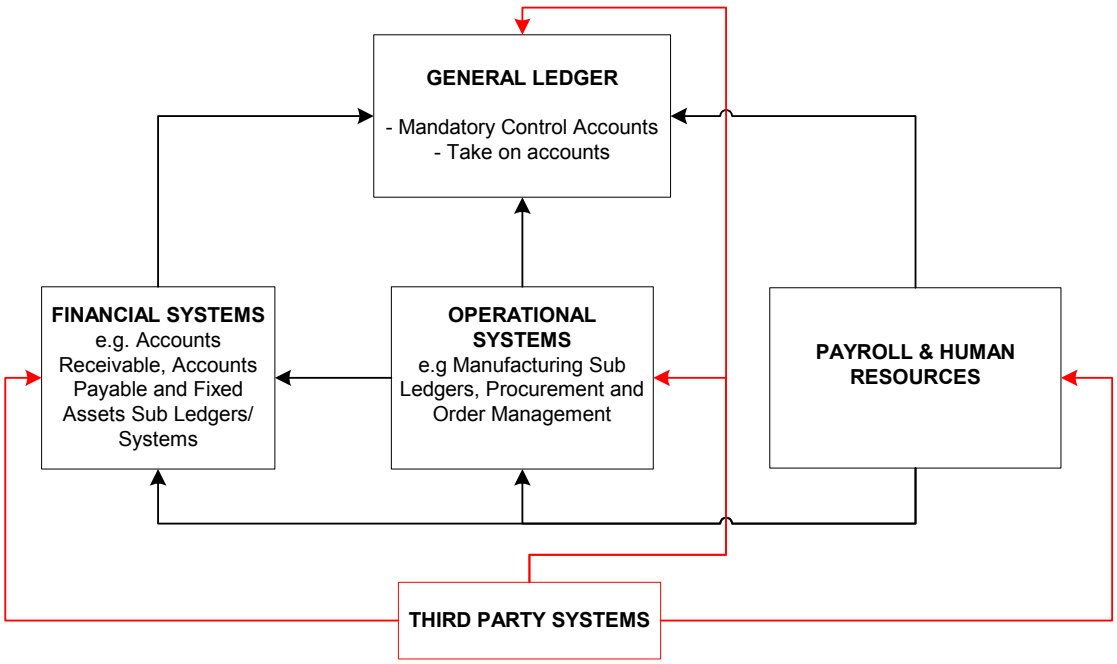


Figure 1: The three components of a system and how they interface.

Reporting Capability

On line reporting

Two way drill

Perhaps one of the most useful features in Oracle is the two-way drill facility which allows users to trace their sub-ledger accounting transactions to General Ledger (GL), or GL transactions back down to sub-ledger transaction detail. Being able to utilize the two-way drill will ensure that auditors and reviewer can easily follow up specific transactions they are investigating.

Transaction status

Each transaction generated by the system will be accorded a status. This status can be reviewed on line as well as in printed reports and will change depending what action is taken on such a transaction. Each change in document status is typically followed by appropriate accounting entries. Knowing the accounting entries that result from a change of document status is an important part of auditing and reviewing transactional data.

T-accounts and activity summaries

For the die-hard accountants Oracle can provide a graphical view of the accounting entries in the form of a T-account. Where there are many transactions flowing into a particular account for a specific transaction Oracle also provides an activity summary.

Web reports

Oracle has web functionality embedded into its product suite which enables a wide range of reports to be delivered in web format. At the click of a button users can get timely and up to date information that provides a cross functional view of the business.

Standard reports

For each particular module standard reports are available in the following categories

- Transactional Data – details of invoice, payments and receipts can be printed out in a variety of reports and formats.
- Master Data – customer, supplier and employee listings.
- Roles and Responsibilities – roles and responsibilities assigned to particular users indicate which areas of the system they have access to.
- Setup parameters at modular and system level – should be reviewed to check for errors in setup. In addition to the setup reports that can be printed by the system, auditors should ensure that all setups are documented outside of the system. Oracle provides a tool called Oracle Applications Implementation Methodology (AIM) which contains document templates that can be used to document the system set up.
- Sequentially numbered documents – the General Ledger Report "Journals – Document number" can be used to trace sequentially numbered documents for all the modules and related transactions. It is important to ensure that all documents are numbered using a predetermined sequence so that they can easily be traced and proper cut-off of transactions can be maintained.
- Security Rules and Cross Validation – indicate what rules have been created for restriction and control of data entry by particular users.

The RXi Tool also enables customization of certain standard Oracle Reports without having to hire a developer. Reports can also be exported into a text file, Excel file or HTML file format which certainly can help when trying to perform complex reconciliation's. Most of the reporting options mentioned are application controls and are detective in nature.

Scripts

A useful tool I have encountered which can perform checks on your set up for each and every module is the CRM analysis toolkit. Although the tool name suggests it is for Customer Relationships Management it runs checks on several modules including each of the Financials modules. The setup and use of this tool is documented in note 167000.1 on Metalink and the results it generates will be demonstrated in the presentation. As an example, the following types of checks can be run on the General Ledger module: Verification of Setup of Set of Books, Chart of Accounts, Flexfield Structure, Calendar and Currency. Errors encountered are clearly highlighted in red text and references to documents on Metalink that can assist in correction of errors are displayed. The address for the log in to the CRM analysis tool is http://<hostname>:<port number>/OA_HTML/jtfqalgn.htm

Network Test

Certainly it is important to test the network speed to ensure that is optimized. This can be checked by running the network test under System Administrator responsibility. Navigate to System Administrator > Application > Network Test. A network test is a general control relating to transmission of data over the network and is detective in nature.

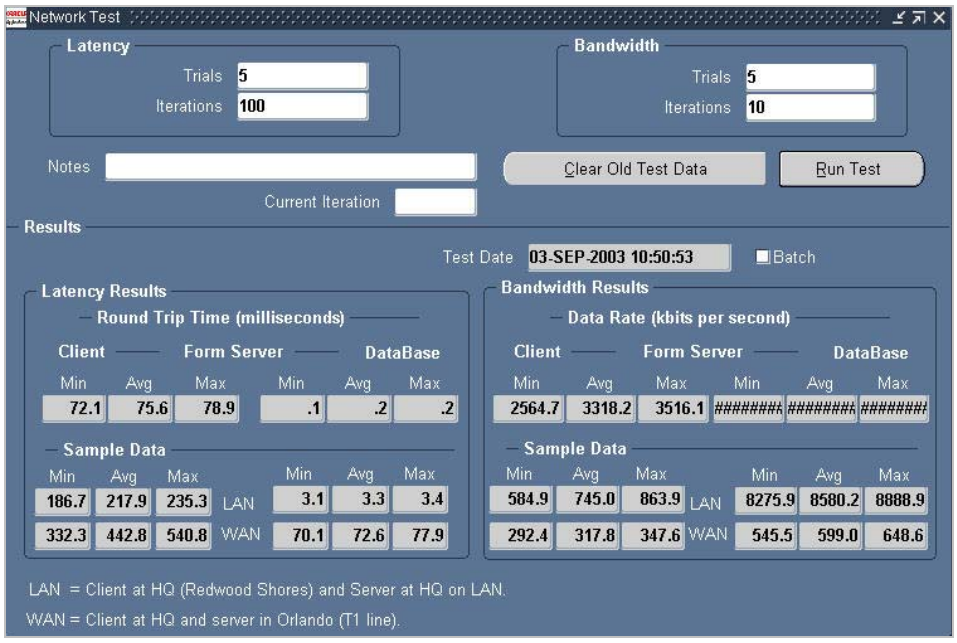


Figure 2: The results of a network test run from Oracle Applications.

Audit Trail

Report History

A history of all reports printed out by a particular user is maintained in the system. These reports can be reprinted and will show exactly the same result as was displayed when the report was originally printed. These reports can be viewed by selecting View > Requests on the menu and then searching for a specific request ID that relates to a report.

Record History

As a default, Oracle keeps a certain level of history for each transaction entered in the system. If you are reviewing a particular transaction simply choose Help > Record History on the menu and the information shown in Figure 3 below will appear. This is very useful in trying to determine who was responsible for a entering or modifying a particular transaction and can also be used to determine which table a transaction is being read from.

Figure 3: Examining the record history for a transaction

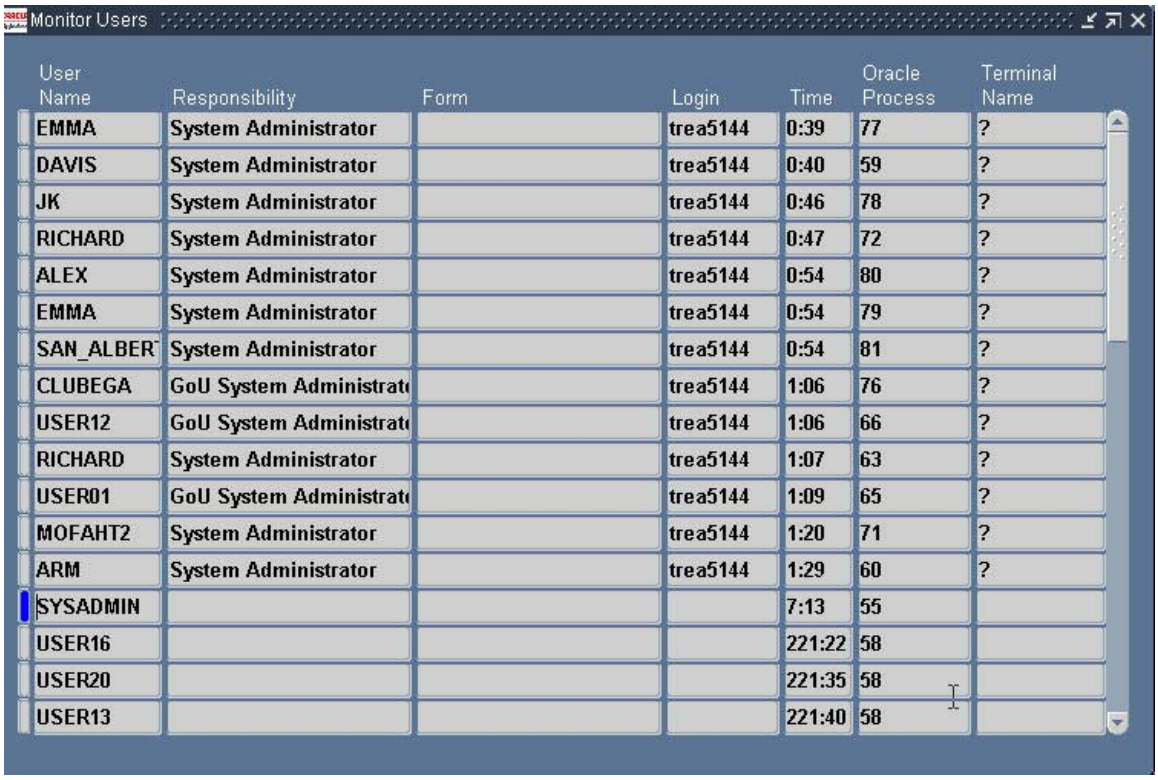
It should be noted that record history only maintains the information of the last update and does not show each and every update that was made to a particular record. For a detailed history of changes to a transaction one should use the Table Audit feature discussed next.

Table Audit

Where it is desired to monitor every amendment to a particular record, one can use the Audit trail facility available under System Administrator. This facility will allow you to monitor every INSERT, UPDATE & DELETE entry for any record that you would like to monitor. When using Audit trail the system creates a shadow table which maintains all the audit transactions. The information in this table can be extracted using SQL Plus or any other Oracle reporting tool like Oracle Discoverer. By default this option is not enabled as it would create a drain on system resources if every table were to have a detailed audit trail maintained, hence one should take care when deciding which tables to audit and what level of detail is required for your trail.

Sign on Audit.

You can audit and monitor user activity by enabling the Oracle Applications Sign-On Audit feature. This enables you to track the activity of users signed on to Oracle Applications. You can implement the Sign-on audit feature by updating the Sign-on Audit Level system profile. With Sign-On audit you can choose whom to audit and what type of user information to track. By choosing the appropriate profile option (Sign on Audit), you can audit at the following level of detail: None, User, Responsibility and Form. NONE being the lowest level of detail and FORM being the highest. Enabling the sign on audit feature will provide you with the ability to monitor users logged in as shown in figure 4.



User Name	Responsibility	Form	Login	Time	Oracle Process	Terminal Name
EMMA	System Administrator		trea5144	0:39	77	?
DAVIS	System Administrator		trea5144	0:40	59	?
JK	System Administrator		trea5144	0:46	78	?
RICHARD	System Administrator		trea5144	0:47	72	?
ALEX	System Administrator		trea5144	0:54	80	?
EMMA	System Administrator		trea5144	0:54	79	?
SAN_ALBER	System Administrator		trea5144	0:54	81	?
CLUBEGA	GoU System Administrat		trea5144	1:06	76	?
USER12	GoU System Administrat		trea5144	1:06	66	?
RICHARD	System Administrator		trea5144	1:07	63	?
USER01	GoU System Administrat		trea5144	1:09	65	?
MOFAHT2	System Administrator		trea5144	1:20	71	?
ARM	System Administrator		trea5144	1:29	60	?
SYSADMIN				7:13	55	
USER16				221:22	58	
USER20				221:35	58	
USER13				221:40	58	

Figure 4: The monitor users form

In addition to on line inquiry you will also be able to print various reports, namely: -

Sign on Audit Forms Report – who is navigating what form and when
Sign on Concurrent Requests Report – to view information about concurrent requests.
Sign on Audit Responsibilities Report – view who is selecting what responsibility and when
Sign on Audit Unsuccessful Logins Report – view who attempted unsuccessfully to log in to Oracle.
Sign on Audit Users Report – view who signs on and for how long.

The audit trail features mentioned are application controls that are largely detective in nature although sometimes just having detective controls in place can result in the control being preventative!

Conclusion

The enhanced risk posed to organizations implementing ERP systems requires a strong regime of internal controls to be implemented along side and in conjunction with such software. The increasing regulatory requirements posed by the Sarbanes-Oxley Act of 2002 and the adoption of International Accounting Standards (IAS) places organizations under further pressure to ensure that ERP systems support the requirements of the business in all respects. The risks of systems implementations as well as changing regulatory requirements also demand specialized audit and review skills at all levels of an entity. Persons responsible for audit and review should ensure that they are familiar with the ERP software in use and adopt any functionality that would help them in performing their work efficiently and effectively.

About the Author

Richard Byrom is an Oracle Applications Consultant with RPC Data, an Oracle Certified Advantage Partner located in Botswana. He has spent the last 8 years consulting with various professional firms within the Southern Africa Region. He has also presented papers at numerous national and international conferences and contributes to leading journals around the globe. Richard can be contacted at richard@richardbyrom.com or you can visit his web site to download Oracle white papers and presentations at http://www.richardbyrom.com

