UNITED KINGDOM

Oracle Applications: The benefits of using automated audit tools

Will Drew and Anirvan Banerjee describe the use of Deloitte's OASIS software to audit Oracle Security.

Auditing Oracle Applications

Oracle has a significant presence in the UK public sector. Over 1,500 public sector organisations use Oracle software globally. Within the UK, 11 of the 13 major government departments use Oracle applications[1]. The products are widely used, within both central and local government, to support financial, procurement and human resource processes.

Enterprise Resource Planning (ERP) systems, including SAP and Oracle, support integrated and automated business processes. These applications often contain the General Ledger and a number of integrated sub-ledgers, including Fixed Assets, Accounts Payable, Accounts Receivable, Cash Management and Payroll. Uniquely, the application holds the account balances and also supports the processing of underlying transactions. The application automatically generates the financial accounting entries for each transaction, sometimes in real time.

Financial auditors need to consider the impact of the accounting system during audit planning. Since information is available electronically and not necessarily in hardcopy, the traditional methods used to gather and evaluate information may not be sufficient. Financial auditors often require more technical skills, or specialist input from IT auditors. This is required to understand general computer controls and the potential impact of IT controls on the audit approach. A paradigm shift is occurring for all audit bodies, regardless of size and industry, to approach the audit from a financial, business process and information technology perspective.

Importance of Security and Controls

In our experience, an area often overlooked in financial audits is Oracle security. The integrity of information within Oracle applications is critical. The financial reports produced by the system are relied upon by the organisation, their auditors and wider stakeholders, including other government bodies and ultimately the general public.

The accuracy and completeness of information held in Oracle applications depends on robust security and controls. However, many organisations struggle to get this right.

The National Audit Office (NAO) in the UK issued a 'disclaimer of opinion' in the audit report for the Home Office in 2004-05[2]. The audit report referred to 'fundamental problems' in the accounting systems and 'significant control weaknesses' within key IT applications following a troubled implementation project.

In addition to financial accounting risks, weaknesses in Oracle security and controls can introduce 'operational risks', such as expenses fraud, unauthorised 'data leakage' and late payments to suppliers. This can be damaging to the organisation's reputation.

1 www.oracle.com
2 http://www.nao.org.uk/publications/0506/home_office_account_2004-05.aspx

Common Security Weaknesses

In our experience, many organisations struggle to implement robust security and controls. UK Oracle User Group's magazine 'Oracle Scene' recently published an article written by Deloitte discussing the most common security weaknesses in Oracle applications[3]. A summary of the main issues raised in the article is provided below:

- Support team access is often excessive with many organisations using access profiles that breach traditional segregation of duties principles;
- Most organisations do not have defined segregation of duties policies. Where segregation of duties principles have been defined, many organisations have no preventative or detective controls to enforce these principles;
- Oracle does not provide standard reports to identify actual segregation of duties conflicts[4]. Few organisations have defined their own bespoke reports to address this issue;
- Few organisations configure auditing to capture changes to high risk information, such as supplier bank account details; and
- Many organisations have not defined exception reports to monitor security exceptions or incidents.

In addition to weaknesses at the application level, database security is another critical area which is often overlooked. All information in Oracle applications is held in an underlying Oracle database. If the database is not adequately secured, information can be accessed and modified directly at the database level, by-passing all application level controls.

Typical database security issues include the use of generic user accounts, inadequate password controls and no auditing to monitor the activity of database administrators.

3 'In Control? Top 5 Common Control Issues', Oracle Scene – Spring 2009.

4 Segregation of duties reports are available through Oracle's Governance Risk and Control technology. However, these products are licensed separately.

Challenges Auditing Oracle Security

Many audit bodies, including the NAO, are moving towards an integrated audit approach where specialist IT audit work is performed to support financial audits. Due to the size and complexity of Oracle systems, even qualified IT auditors can find it difficult to perform effective reviews of security and controls.

Auditors often adopt a manual approach to auditing Oracle, usually conducting limited tests around general computer control areas, such as the enforcement of basic password controls. More advanced tests are difficult to perform due to the limitations in 'out-of-the-box' reports provided by Oracle and the technical complexity of the application. Ironically, these same challenges often mean organisations that run Oracle also have a limited understanding of the status of their Oracle controls.

Where auditors do require a greater level of assurance over Oracle security and controls it is often resource intensive and requires significant involvement of the client IT staff. For example, it may take several days merging the results of several different reports to obtain a list of the users with access to enter journals.

Benefits of Automated Assessment Tools

In recent years, a number of assessment tools have been developed to help auditors review Oracle environments. These tools overcome the issues of testing Oracle security manually. The common benefits of using these tools are:

- the tools are quick to run and require less contact time with client staff;
- the tools provide more detailed information than could be obtained manually; and
- the reports are written in non-technical language, so specialist Oracle IT Auditors do not need to be involved.

Ultimately, the use of automated tools can reduce audit costs whilst increasing the audit coverage and quality of value-added recommendations.

Deloitte's OASIS Tool

OASIS (Oracle Application Security Integrity Suite) is the Deloitte UK proprietary tool for Oracle security analysis. OASIS has been used to assess Oracle security and controls at over 100 different organisations. The OASIS tool generates three separate reports. The contents of the reports are listed in the inset boxes. The purpose of the reports is described below:

Oracle Application Security Report

This report provides information about application security, including the user account management, auditing and security configuration. The report is written in non-technical language and includes sections discussing the observation, risk and recommendation for each section. Figure 1 shows the 'Generic User Names' section of a sample report.

The findings in the report enable auditors to hold follow up discussions with the Oracle support team to investigate issues and identify the root cause of problems. For example, the presence of generic user accounts may indicate poor user administration processes, inadequate system monitoring or inappropriate use of the 'live' system for testing and training.

Application Security Report Contents:

- Generic User Accounts
- Last Login Dates
- Inactive User Accounts
- Password Controls
- Exceptions to Password Controls
- Users with Powerful Access
- Users with Default Access
- Application Auditing
- Other Security Configuration

Figure 1: Generic User Names

2.4 Generic user names

Observation

The following table shows the user accounts where the user name or its description has been highlighted as potentially being generic accounts. This list contains accounts that have 'TEMP', 'TEST', 'GUEST', 'USER' or 'ADMIN' in their user name or the user description.

- 15 of 82 users (18%) have not been end-dated and have generic user names or descriptions.

USER_NAME	DESCRIPTION	USER_ID	END_DATE
APPSMGR	User for routine maintenance activities scheduled as concurrent requests. Should be used for pre scheduled requests and for requests submitted at the time of patching applications.	3	
ASGADM	asg developer user	2053	
GEMINI	External Consultant – Oracle Testing (read only)	1301	
GUEST	guest	5	
IBE_ADMIN	iStore Administrator	2078	
IBEGUEST	Guest User for iStore	1985	
IRC_EMP_GUEST	iRec Employee Guest Login	2005	
IRC_EXT_GUEST	iRecruitment External Guest Login	2004	
LLADMIN	System Administrator User	1762	
MOBILEADN	asg mobile admin user	1965	
RWALKER	Contractor User	1004	
SYSADMIN	System Administrator	0	
TEST_USER	Test Account	2034	
TRAININGUSER	Used For Training	1682	
WIZARD	USER for Application Implementation Wizard	6	

This list should be reviewed in conjunction with the Generic User Names and their Responsibilities section, which shows the high privileged responsibilities that have been assigned to these users.

Risk

Generic accounts that are not assigned to a specific individual remove accountability which increases the risk of fraud.

Recommendation

The list of account names should be reviewed and where these cannot be identified to individuals they should be investigated and disabled where appropriate.

Procedures should be implemented to control the creation of temporary accounts or system accounts to ensure that they are set up with a unique ID and end-dated as appropriate.

Management should perform periodic reviews to ensure that the process is followed.

Oracle Database Security Report

The database security report provides information about default passwords, database administrator's (DBA) accounts and database auditing. The format is the same as the application security report. Figure 2 shows the 'Database Accounts with Default Passwords' section of a sample report.

The presence of default database accounts may have a significant impact on security. The Oracle default database passwords are easy to guess as the user name and passwords are the same. This information is widely available on the internet. Accessing the 'GL' account would provide full read and write access to the database tables that hold all the information in the General Ledger. This could be used to modify accounting entries or create journals whilst by-passing application controls. Typically, there is no reason why any default database accounts should have the default password but this is an extremely common finding.

Database Security Report:

- Users with Default Passwords
- Password Controls
- DBA Accounts
- Database Auditing
- Other Security Configuration

Access Control and Segregation of Duties Matrix

This report, provided in a spreadsheet format, provides details of user access to Oracle data entry screens, such as who can access the screens to 'Enter Journals' or 'Create GL Accounts'. This report can be used to investigate user access and determine whether appropriate segregation of duties have been enforced. This is particularly powerful, as Oracle does not provide standard reports that contain this information.

Figure 2: Database Accounts with Default Passwords

2.2 Database accounts with default passwords

Observation

The following table shows default Oracle database accounts with default passwords still active on the system. A successful attempt was made to login onto each of these accounts with their default passwords. The 'Key Account' column indicates some of the key accounts – these are typically highly privileged Database Administrator level accounts. The 'Database Owned' column shows the accounts that are used by the Database Management System rather than by the application system.

ACCOUNTNAME	SUCCESS	KEYACCOUNT	DATABASEOWNED
ABM	Yes		
AP	Yes		
AR	Yes		
GL	Yes		
MDSYS	Yes		Yes
POWER6_ALIUK	Yes		
POWER6_ALIUK_DUK	Yes		
SYS	Yes	Yes	Yes
SYSTEM	Yes	Yes	Yes

Risk

All accounts with default passwords represent a risk – at the very least they will probably have sufficient privileges to allow an intruder to perform a denial of service attack through filling the available database space. At worst, if an intruder uses a highly privileged account, it may additionally allow users to change application data directly and avoid all application-level auditing and privileges. This would lead to poor decision-making and may lead to inconsistencies in the financial information.

All users that have Oracle have SQL*Plus installed by default. This tool alone would allow any legitimate applications user to attempt to guess database account and password combinations, as would Microsoft Access. Users do not have to be Database Administrators to have these tools available to them.

Recommendation

Each database account should have its password changed from the default. For application-owned accounts this needs to be in two stages – the first is to change the password through the Oracle Applications system administrator function, the second is to change the database password at the database level. If one of these stages is not performed, an inconsistency will occur and problems will arise.

Management should implement a policy such that all passwords are changed at least twice a year, with the passwords for key accounts changed at least every 90 days. Documentation should be maintained in order to confirm compliance with this procedure.

In the sample report (Figure 3), we can see that the user ABANERJEE has access to enter and post journals. This would be considered a segregation of duties conflict in many organisations.

The matrix can also be used to identify multi-dimensional segregation of duties conflicts. For example, some organisations may find it acceptable for a user to enter and post journals provided they can not also create GL accounts. In this situation, the access provided to JMANN is appropriate, whereas ABANERJEE and NYEOMANS breach this segregation of duties principle. The ability to perform flexible and customised segregation of duties analysis makes the OASIS tool extremely powerful.

The sample report only shows access to the General Ledger data entry screens. The report includes access within all major business processes including procurement, payables, receivables, fixed assets, inventory, human resources and payroll.

Figure 3: User access to Oracle data

USER_NAME	Number of privileged functions assigned to the user account	General Ledger													
		Enter Journals	Import Journals	Post Journals	Reverse Journals	Journal Authorization Limits	Journal Categories	Currencies	Create GL Accounts	Interfund Accounts	Define Suspense Accounts	Summary Accounts	Archive and Purge	Open and Close Periods	Enter Intercompany Transactions
Numbers of users with access to the functions		45	5	45	45	5	5	6	6	6	6	5	6	6	5
ABANERJEE	8	Y		Y	Y			Y	Y		Y			Y	Y
WDREW	2								Y					Y	
NYEOMANS	3	Y		Y					Y						
JMANN	2	Y		Y											

Will Drew and Anirvan Banerjee
Will Drew and Anirvan Banerjee work in Deloitte's Oracle Controls team which specialises in assessing, implementing and optimising Oracle EBS controls. This includes working as part of Oracle implementations to facilitate the inclusion of good practice security and controls. This experience is also used in performing Oracle control assessments and assisting organisations in improving and optimising their controls. They both regularly present at Oracle User Group conferences and SIGs. They can be contacted at wdrew@deloitte.co.uk and anirbanerjee@deloitte.co.uk.