Auditing ERPs to continue to add value

Presented by
Johanna Terronez, Senior Manager
Grant Thornton Advisory Services
May 22, 2014

Agenda

- Triggers for ERP audits
- Types of ERP audits
- Scoping and Planning the effort
- Executing ERP audits
- Leveraging technology

Triggers for ERP Audits

- Risk assessment results
- Reporting or compliance requirements
- Prior year audit findings
- New system implementations or version upgrades

Types of ERP audits

- General security configuration **
- Business cycle/application controls **
- Segregation of duties **
- Access to sensitive data
- Database security configuration
- Data migration
- Pre- or post- implementation reviews
- Change management

**discussed in more detail in Executing

Scoping and Planning the effort

Category	Ref #	Topic/Question
Oracle e-Business Suite (EBS) Landscape	1.	Versions of the application and database(s)
	2.	Number of instances
	3.	Modules implemented and links to business cycles up for rotation
	4.	Number of production and non-production application and database servers
	5.	Sampling
	6.	Coordination with financial auditors where relying

Scoping and Planning the effort – cont'd

Category	Ref #	Question
Oracle e-Business Suite (EBS) Architecture	1.	How many nodes does the System have?
	2.	Does the DB share a server with any of the application nodes?
	3.	Is SSL enabled for the EBS System?
	4.	Is SSO enabled for the EBS system, and if yes, then what version? Is WNA enabled?
	5.	Are there any external nodes to serve certain Applications like i-Procurement, if yes, then do they exist in the DMZ?
	6.	Are there any load balancers/netscalers involved in the architecture? If yes where is the SSL terminated if it exists?

Scoping and Planning the effort – cont'd

Category	Ref #	Question
Database Access	1.	Do user accounts exist that allow for direct database access?
	2.	If so, describe the process for requesting and granting direct database access?
	3.	Is approval required to grant direct database access? If so, by who?
	4.	Are there generic DB accounts(i.e. read-only) that multiple people have access to?
	5.	Are there any firewalls in place to prevent accessing the Database?

Scoping and Planning the effort – cont'd

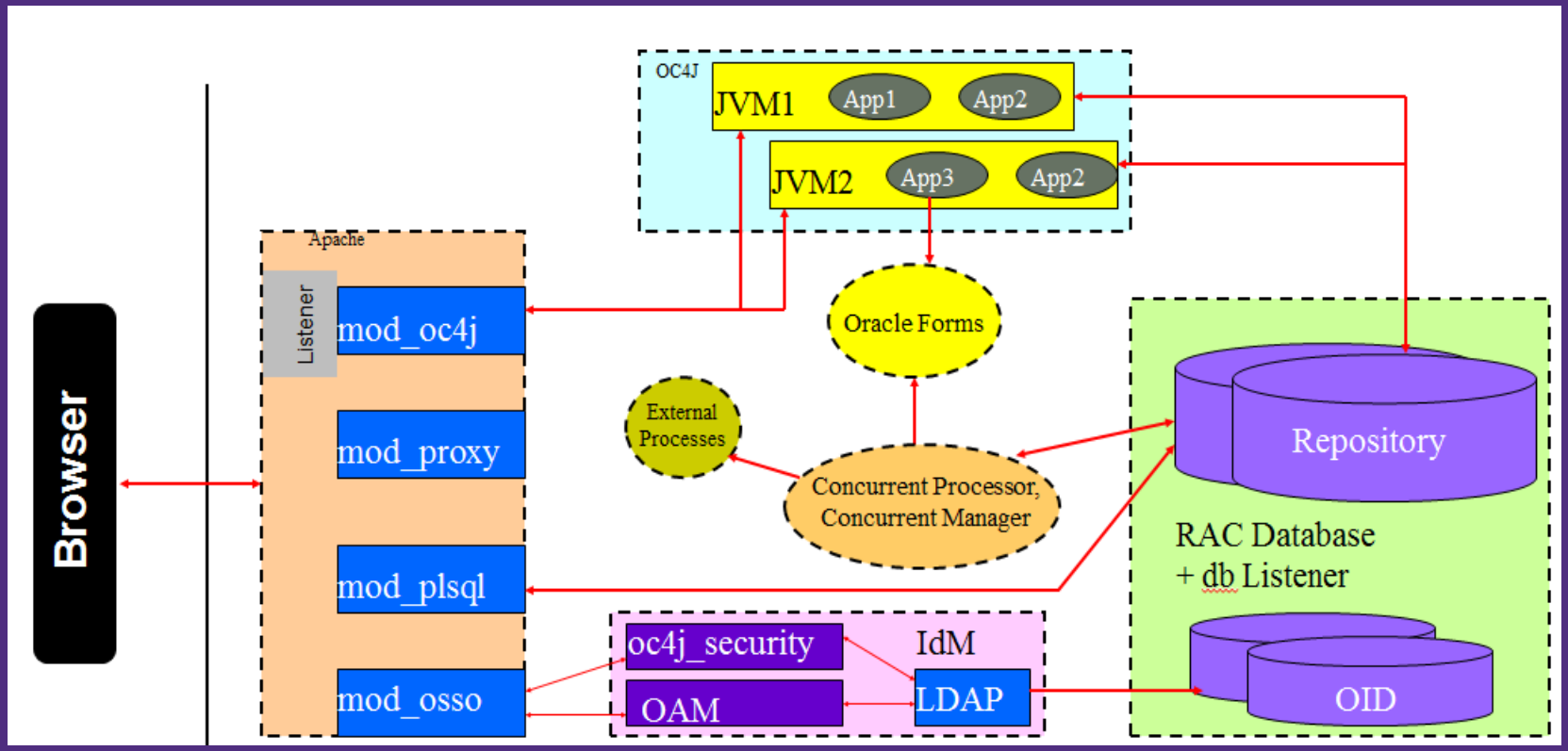
Category	Ref #	Question
Sensitive Data	1.	Do you currently store bank account data?
	2.	If yes, what measures have been taken to secure?
	3.	Do you currently store credit card data?
	4.	If yes, what measures have been taken to secure?
	5.	Do you currently store Personally Identifiable Information (PII) data?
	6.	If yes, what measures have been taken to secure?
	7.	Describe any measures taken to secure sensitive data as part of an instance refresh from production to non-production?

Executing General Security Configuration

- Yr 1, need to establish a baseline understanding of system architecture and configuration
- Gaining an understanding of the architecture, will help determine the following:
  - where to focus audit efforts
  - use of automated tools built into the customization, such as SSO, GRC module, etc.
  - application controls configured

Executing General Security Configuration – cont'd

- Typical architecture for Oracle E-Business below:



Executing General Security Configuration – cont'd

- Oracle provides recommendations for configuring the Oracle E-Business Suite
  - Many best practices have been consolidated and published in the White Paper “Secure Configuration Guide E-Business Suite Release 12” available in Oracle Support Note: 403537.1
  - Hardware and operating system parameters:
    - See Oracle E-Business Suite Installation and Upgrade Notes Release 12 (12.1.1) for Linux x86-64 (Doc ID 761566.1) or other based on your technical architecture.
  - Critical Patch Updates:

How to find the Latest, Recommended Patches for E-business Suite R12 or 11i [Article ID **1525452.1**]

Oracle E-Business Suite Recommended Performance Patches [Article ID **244040.1**]

Executing General Security Configuration – cont'd

- Additionally, Oracle provides recommendations for the following:
  - Restricting network access to critical services with the use of firewalls, for both the EBS application and database servers
    - Enabling SSL/TLS between browser and EBS webserver
  - Physical Architecture - Access to some Forms and Pages

Physical Architecture Topic	Description	Oracle Best Practice Recommendation
Users With Access to Sensitive Forms Via Responsibilities	Some forms and pages in EBS allow a user to modify the functionality of the applications by specifying values such as SQL statements, SQL fragments such as WHERE clauses, HTML strings, and operating system commands or environment variables.	Eliminate or minimize access to these screens in a production system and know exactly which users have access to these screens.
Users With Access to Sensitive Forms Via Grants		
Users With Access to Sensitive HTML Pages Via Responsibilities		
Users With Access to Sensitive HTML Pages Via Grants		

Executing General Security Configuration – cont'd

- Individual account passwords recommendations for Oracle E-Business Suite Sec. Profile Settings:

Security Profile Option	Description	Oracle Recommendation
Sign-On Password Failure Limit	The Sign-on Password Failure Limit profile option determines the maximum number of login attempts before the user's account is disabled.	5
Sign-On Password Hard to Guess	The Sign-on Password Hard to Guess profile option sets rules for choosing passwords to ensure that they will be "hard to guess." A password is considered hard-to-guess if it follows these rules: • The password contains at least one letter and at least one number. • The password does not contain the username. • The password does not contain repeating characters.	Yes
Sign-On Password Length	Sign-on Password Length sets the minimum length of an Applications sign-on password. If no value is entered the minimum length defaults to 5.	8
Sign-On Password No Reuse	This profile option specifies the number of days that a user must wait before being allowed to reuse a password.	180
Sign-On Password Case	This profile option specifies whether password case sensitivity is enabled.	Sensitive
ICX: Session Timeout	This profile option determines the length of time (in min.) of inactivity in a user's session before session is disabled. If user does not perform any operation in Oracle Apps for longer than this value, the session is disabled.	30
Sign-On: Audit Level	Profile option enables system to log user sign-ons, responsibility selection and form access	Form
Password Expiration	Number of days which the user will be required to change their password.	60

Executing General Security Configuration – cont'd

- Managing the default DB accounts and passwords:
  - Typically have privileged access to one or more schema
  - Quick check: SQL> select * from sys.dba_users_with_defpwd;
  - The following accounts may exist depending on DB version:

User Name	Default Password	Source
SYS	CHANGE_ON_INSTALL	Installation
SYSTEM	MANAGER	Installation
ANONYMOUS	ANONYMOUS	XDB
CTXSYS	CTXSYS	Oracle Text
DBSNMP	DBSNMP	Intelligent Agent
DIP	DIP	Internet Dir
DMSYS	DMSYS	Data Mining
EXFSYS	EXFSYS	Expression Filters
LBACSYS	LBACSYS	Label Security
MDDATA	MDDATA	Spatial
MDSYS	MDSYS	Spatial
MGDSYS	MGDSYS	Identity Code (RFID)
ODM	ODM	Data Mining
ODM_MTR	MTRPW	Data Mining
OLAPDBA	OLAPDBA	OLAP
OLAPSVR	OLAPSVR	OLAP
OLAPSYS	OLAPSYS	OLAP

User Name	Default Password	Source
ORACLE_OCM	ORACLE_OCM	Config Mgr
ORDPLUGINS	ORDPLUGINS	interMedia
ORDSYS	ORDSYS	interMedia
OUTLN	OUTLN	Plans
OWBSYS	OWBSYS	Warehouse Builder
RMAN	RMAN	RMAN
SCOTT	TIGER	Sample
SI_INFORMTN _SCHEMA	SI_INFORMTN_ SCHEMA	interMedia
SYSMAN	OEM_TEMP	OEM
TSMSYS	TSMSYS	Migration
WK_TEST	WK_TEST	Ultra Search
WKPROXY	CHANGE_ON_INSTALL	Ultra Search
WKSYS	CHANGE_ON_INSTALL	Ultra Search
WMSYS	WMSYS	Workspace Mgr
XDB	CHANGE_ON_INSTALL	XDB

Executing General Security Configuration – cont'd

- Managing seeded App accounts and passwords:
  - Typically have privileged access
  - Need to either manually test for the accounts or run a tool Some accounts include the following depending on version:

Account	Product / Purpose	Change	Disable
AME_INVALID_APPROVER	AME WF migration 11.5.9 to		
ANONYMOUS			
APPSMGR			
ASGADM			
ASGUEST			
AUTOINSTALL			
CONCURRENT MANAGER	FND/AOL: Concurrent Manager	Y	Y
FEEDER SYSTEM			
GUEST			
IBE_ADMIN			
IBE_GUEST			
IBEGUEST			
IEXADMIN			
INITIAL SETUP			
IRC_EMP_GUEST			
MOBILEADM	Mobile Applications Admin	Y	Y
OP_CUST_CARE_ADMIN	Customer Care Admin for Oracle Provisioning	Y	Y
OP_SYSADMIN	OP (Process Manufacturing) Admin User	Y	Y
STANDALONE BATCH PROCESS	FND/AOL	Y	Y
SYSADMIN	Application Systems Admin	Y	**N**
WIZARD	AD – Application Implementation Wizard	Y	Y
XML_USER	Gateway	Y	Y

a. Required for Mobile Sales, Service, and Mobile Core Gateway components.
b. Required for Sales Application.
c. Required for *i*Store.

Executing General Security Configuration – cont'd

- Direct Database Access should be limited
  - Often individual accounts created with read only access to all data for reporting purposes,
  - Generic accounts assigned with access to sensitive data, and/or
  - IT users have access for support purposes
- Review all users, roles and responsibilities with direct database access
- Should ensure that the Oracle hardening recommendations are implemented, including
  - password requirements to accounts, where possible
  - enabled auditing

Executing Business Cycle/App. Controls Reviews

- Risk assessment drives business cycles for the current year
- Need to identify the key application controls within each cycle
  - Consider patching or upgrades that could have effected configured controls
- Key master data and other sensitive data
- Auditing enabled
- Include review of users, roles, and responsibilities
- IT users with access to business functionality

See next couple slides for samples

Executing Business Cycle/App. Controls Reviews – cont'd – General Ledger -

- Ledger set-up for one or more legal entity:
  - chart of accounts, calendar, currency, & accounting method
- Common key controls for completeness, valuation, existence, cut-off, and presentation and disclosure:
  - Journal approvals systematically according to the approval limits pre-defined in the system.
  - Imported journals (from feeder modules) cannot be modified in GL.
  - Only allows balanced entries to be posted.
    - Automated suspense accounts.
  - Cross-validation rules have been enabled and developed to help ensure the accuracy of data entry.
  - Open/close GL periods
  - Access controls

Executing Business Cycle/App. Controls Reviews – cont'd – Fixed Assets -

- Common key controls for completeness, valuation, existence, cut-off, timeliness, and presentation and disclosure:
  - Segregation of duties and access controls.
  - Input controls for asset creation with cross-validation, as applicable.
  - Automation of activity to GL accounts.

Executing Business Cycle/App. Controls Reviews – cont'd – Payables -

- Common key controls for completeness, valuation, existence, and presentation and disclosure:
  - Invoices are authorized through a 3-way or 4-way match of PO price, invoice price and quantity received
  - System holds on the invoices cannot be released unless the error is rectified.
  - Date used for accounting date for invoices during accounting entry agrees to business process.
  - Employee expense reports are approved by managers per established approval limits.
  - Segregation of duties and access controls

Executing Business Cycle/App. Controls Reviews – cont'd – Purchasing -

- Common key controls for completeness, valuation, existence, and presentation and disclosure:
  - Edit checks help ensure valid p.o. data entry based on predefined values.
  - Automated purchase orders and requisitions approvals according to the approval limits.
  - Requisitions, P.O.s, and receipts are sequentially numbered.
  - Access controls.
  - Goods received are accurately recorded and matched to P.O.
  - Automation of accrual on receipt for expense and inventory items and feed to GL accounts.

Executing Business Cycle/App. Controls Reviews – cont'd – Receivables -

- Common key controls for completeness, valuation, existence, cut-off, and presentation and disclosure:
  - Automation for invoicing, credit memos, etc.
  - Automation for sales tax calculation
  - Automated feed to GL for revenue
  - Access controls
  - Approval limits for adjustments/write-offs

Executing Segregation of Duties (SoD) Review:

- Apply a risk-based approach to identifying conflicts
  - Consider multiple tiers of risks rather than just compliance, such as fraud, reputation, operational (i.e. costs, time, resources), etc.
  - Consider sensitive functions and sensitive data
  - Perform SoD analysis across modules and not just within one module
  - Assess IT users and business users and
- Once conflicts are identified
  - Discuss risks and magnitude associated with the exposure
  - Identify mitigating controls
  - Once residual risk is determined, determine management's willingness to accept the risk
    - Document the SoD acceptance and rationale
- As applicable, identify or implement monitoring controls

Leveraging Technology

- Use of Oracle security features and tools:
  - GRC
  - Audit Vault and Database Vault
  - Oracle Advanced Security Option (ASO)
    - Transparent Data Encryption (TDE)
    - Data redaction and data masking
- Enable auditing of high risk activity
- Other Automation tools
  - Quest Stat
  - Kintana
- Log and Event Management Tools
  - Splunk
  - HP ArcSight

Q & A

Contact Information:

- **Johanna Terronez** | Grant Thornton LLP
- Senior Manager | Advisory Services
- **T (direct)** +1 415 318 2228 | **T (mobile)** +1 773 580 2879
- One California Street, Suite 2300 | San Francisco, CA | 94111 | US
- **E** johanna.terronez@us.gt.com | **W** www.grantthornton.com