ERP Security Risks and Auditing

Irina Majstrova, Director, PwC

In-Depth Seminars – D32

ISACA®

Trust in, and value from, information systems

San Francisco Chapter

CRISC

CGEIT

CISM

CISA

2013 Fall Conference – “Sail to Success”

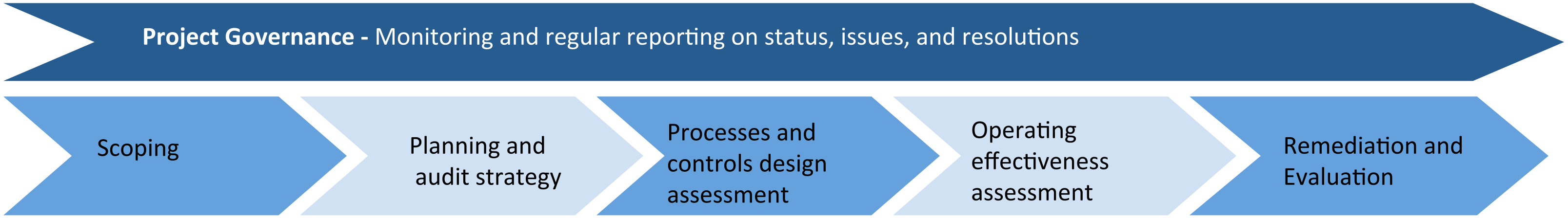
Agenda

1. Introduction
2. ERP audit scoping considerations
3. Execution of ERP audits
4. ERP implementation audits
5. Summary
6. Questions

INTRODUCTION

ERP AUDIT SCOPING CONSIDERATIONS

Typical Audit Execution Framework



Project Governance - Monitoring and regular reporting on status, issues, and resolutions

Scoping

Planning and audit strategy

Processes and controls design assessment

Operating effectiveness assessment

Remediation and Evaluation

Determine the scope of audit based on the following:
-Risk
-Materiality
-Magnitude of impact
-Specific area of focus
-Other requirements/ focus areas

Plan your audit:
-Requirements
-Timing
-Resources
-Dependencies

Plan your audit approach

Determine level of documentation and templates

Determine communication strategy

Understand processes and controls

Conduct walkthroughs to confirm understanding of processes and controls

Perform assessment of process and controls design to confirm it sufficiently covers risks

Identify design issues

Finalize areas/ controls for testing

Perform operating effectiveness testing of controls identified for testing

Identify operating effectiveness issues

Perform remediation testing on ineffective controls

Evaluate impact of identified design and operating effectiveness issues

Agree on managements’ action plan to address unremediated issues

Scoping an ERP Audit

Initial questions to start with to identify ERP related risks…

1. What ERP modules are being used and which ones support significant business processes or business processes under assessment?
2. What Ledgers/Operating units/ Organizations/ Sets of Books are significant or under assessment?
3. What is the level of automation of business processes introduced through the use of ERP?
4. Do business process owners rely on automated application controls (e.g., system configurations, customizations), or ERP-dependant manual controls to perform their duties/ controls and what those are?
5. Do business owners rely on ERP to mitigate segregation of duties (SOD) risk and segregate access and what those SOD cases are?
6. What key reports would the audit team like you to validate? And what attributes?
7. How is access to ERP provisioned?
8. How are changes to ERP promoted?
9. How are ERP batch jobs and interfaces monitored?
10. How is ERP backed up and restored?...

Typical ERP Audit Areas

Business Processes

- Scope of business processes
  - Business processes in scope
  - Subledgers/ modules
  - Organizations/ Ledgers/ Sets of books/ Operating or Business units
- Automated application controls within ERP
  - Significant configurations and customizations within each subledger/module and within each Organization/ Ledger/ Set of books/ Operating or Business unit in scope
- ERP-dependent manual controls
  - Significant transaction processing controls (i.e. complex calculations, built-in checks, etc…)
  - Reports and Interfaces
- Significant SODs and restricted access enforcement
- Master data maintenance

Typical ERP Audit Areas - Continued

IT General Controls

- Program development/ System Development Life Cycle and Program changes:
  - Code development
  - Application code changes
  - Configuration changes
  - Data changes
- Users' access (ERP security):
  - Privileged users access (application, database and OS levels)
  - Back-end access (DBA or Application developer-like access)
  - Segregation of duties (SOD)
- Computer operations:
  - Batch processing
  - Backups and restoration
  - Physical access

Establishing ERP Audit Strategy

- Timing of ERP audit:
  - Based on compliance requirements
  - Based on availability of resources to support the audit
  - Based on internal reporting requirements or milestones
- Consider dependencies that will impact ERP audit execution:
  - ERP Implementation phases
  - Business/ ERP transformations and changes in the controls
- Consider audit and documentation requirements:
  - Frequency of testing (2 times a year, quarterly, change driven, etc…)
  - Documentation (evidence retention, level of documentation, etc…)
  - Audit techniques (inquiry, observation, examination, reperformance)
- Consider resources:
  - Resources' skills, subject matter expertise in your ERP and availability to execute the audit
  - Resources availability to support the audit (participate in meetings, answer audit questions, provide evidence, etc…)

Establish ERP Audit Execution Plan

- Type of ERP is important – ensure you understand specifics of ERP such as:
  - IT solution and architecture (dependencies, security model, etc…)
  - Functionality and lack of it (business processes, reporting, configuration specifics, etc…)
  - Weak areas from security and functionality perspective
- Involve subject matter experts for ERP, Database, OS, security and functional specialists (per module and/or overall)
- Consider tools that automate audit and analysis
- Leverage technical resources, ERP design documents, business process narratives, other documentation
- Understand all ERP modules implemented and Ledgers/Operating units/ Organizations/ Sets of Books in scope for review
- Understand all processes and controls in scope for review
- Understand timing of the review and deliverables/ outcome

EXECUTION OF ERP AUDITS

Executing the ERP Audit Plan

- Start with understanding risks, business and IT processes and controls and how the ERP supports them (review design documentation, perform walkthroughs, etc…)
- Understand the areas of automation, customizations, complex calculations, workflows, SOD, reports and interfaces
- Assess whether design of processes and controls is sufficient to cover the risks and whether there is lack of control points in the process
- Perform testing of operating effectiveness of identified control points within ERP as well as SOD, reports and interfaces.
- Inherent functionality ERP controls are usually not tested unless there is a specific requirement (example: users cannot post a JE to a closed period)

Executing the ERP Audit Plan - Continued

- Perform testing of operating effectiveness of identified IT general controls supporting your ERP
- Identify issues with ERP control points
- Identify issues with excessive access and/or segregation of duties issues
- Identify issues with reports' completeness and accuracy
- Document testing with required level of evidence retained
- Discuss with control owners, IT and system administrators, process owners, data owners, etc. your findings
- Discuss remediation plans and timing
- Perform assessment of the impact:
  - Consider mitigating controls to reduce the exposure

ERP Audits – Lessons Learned

- Remember that analysis of ERP controls is point-in-time, hence IT general controls are important for continuous operation
- “False positives” in SOD typically are not false
- Consider access to powerful accounts (all layers – ERP, DB, OS) and developers access to production
- Lack of completeness or accuracy of reports or interfaces may result in significant failures of dependent controls and expose the company
- Each ERP has its own areas of weakness that should be a focus of your audit
- Collaboration with business process owners and security administrators is critical

Common ERP Risk and Audit Areas

General Ledger

- Sub-ledger to GL interfaces
- Financial statement consolidation logic
- Intercompany eliminations
- FX conversion/translation/revaluation
- Journal setups and processing

Purchasing to Payables

- PO/PR approvals / hierarchy
- Tolerances
- Matching

Fixed Assets

- Depreciation calculation

Order to Cash

- Revenue recognition
- Pricing procedures / tolerances
- Credit checking
- AR aging/bucketing
- Cash receipts

Inventory

- Costing
- Cycle counting

Segregation of Duties

Master Data setup

Interfaces

Areas of Increased Focus by PCAOB (ERP related)

- Journal Entries:
  - Initiation, authorization, approval, recording in GL
  - SOD for create, post and perform accounts reconciliation
  - Completeness of population of manual journal entries
- Income taxes
  - Understanding of the process and controls in the income tax cycle
  - Excessive reliance on “super controls”
  - Appropriateness of underlying data (i.e. reports)
- Level of ERP controls testing
  - Overreliance on inquiry and insufficient testing procedures
  - Lack of understanding of how controls are configured/ designed
- IT dependent controls (reports and interfaces) and EDI
  - Completeness and accuracy of reports, interfaces, EDI feeds

ERP IMPLEMENTATION AUDITS

Benefits of ERP Implementation Review

- Support a "**no surprises**" approach for subsequent audits via advance involvement before GO-LIVE

- Make an annual audit more efficient through **leveraging** ERP implementation review work and results performed upfront

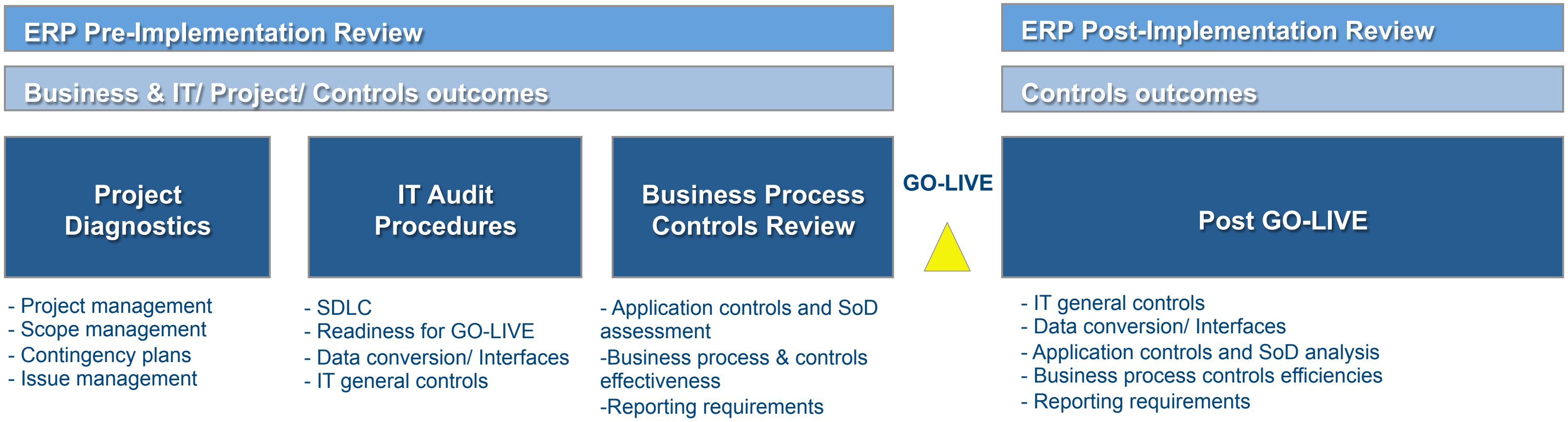
- Provide an **independent** point-of-view on how ERP helps automate business processes and setups and support a robust business process controls environment

- Provide real time and **actionable** feedback on business & IT processes and controls improvement

- Provide an **independent** view to the Executive Stakeholders on how the ERP upgrade project is meeting project objectives and progressing compared to expectations

ERP Implementation Review

- The ERP Implementation review may be performed as pre-implementation and post-implementation.
- Pre-implementation review helps identify project, business, and control risks early and address them before go-live
- Typically the pre-implementation is preferred as it occurs earlier in the process and touches on more areas: (1) Project Diagnostic, (2) Business and IT Process, and (3) Controls outcomes



ERP Pre-Implementation Review

Business & IT/ Project/ Controls outcomes

Project Diagnostics

- Project management
- Scope management
- Contingency plans
- Issue management

IT Audit Procedures

- SDLC
- Readiness for GO-LIVE
- Data conversion/ Interfaces
- IT general controls

Business Process Controls Review

- Application controls and SoD assessment
-Business process & controls effectiveness
-Reporting requirements

GO-LIVE

ERP Post-Implementation Review

Controls outcomes

Post GO-LIVE

- IT general controls
- Data conversion/ Interfaces
- Application controls and SoD analysis
- Business process controls efficiencies
- Reporting requirements

Common Areas of ERP Implementation Review

- Project diagnostics (optional)
- System development life cycle
- IT general controls and processes
- Business processes and application controls
- Segregation of duties

Typical Areas of Focus

System development life cycle (SDLC)

- Assess the design and operational effectiveness of SDLC controls based on the leading practice over the implementation with the focus on the following areas:
  - Design sign off,
  - Data Conversion/Migration,
  - Key Interfaces/ Integration with Legacy Systems,
  - UAT Testing,
  - Go-live and Cutover procedures
  - Post go-live issues tracking

IT general controls and processes

- Assess the design and operating effectiveness of IT general controls with the focus on change management, security and access areas for the application, database, and OS.

Typical Areas of Focus - Continued

Business processes and application controls review

- Assess the impact of ERP implementation on the business processes and application controls:
    - Understand business processes and controls through the review of the business process documentation, risk and controls matrices, application design documentation and meetings with business owners
    - Assess design and operating effectiveness of ERP automated controls and key reports

Segregation of duties review

- Assess segregation of duties within business process taking into consideration existing SOD policies/ rules of the company, industry good practices, ERP functionality

ERP Implementation Review Accelerators

- Tools for SOD and Access assessment
  - Oracle/ SAP GRC
  - Approva
  - Logical Apps, etc…
- Tools for ERP configuration assessment
  - Oracle/ SAP GRC
  - Custom developed scripts, etc…
- Risks and Controls Libraries per ERP
  - Proprietary libraries of audit firms

ERP Implementation Review – Typical Pitfalls

- Neglecting to scope ERP implementation review correctly
- Failing to understand the impact of new functionality
- Incorrectly evaluating security & segregation of duties
- Failing to evaluate the impact of new reports and interfaces
- Starting the review late in the process or post-go live
- Performing a key control impact assessment too late
- If the following is true, there is a heightened risk related to ERP implementation:
  - User acceptance testing designed for prior version of ERP
  - Complex data conversion/migration strategies
  - Business requirements and design documents completed untimely
  - Ineffective issues log and defect tracking
  - Inaccurate project governance & status reporting to support the go-live decision

ERP IMPLEMENTATION AUDIT – ORACLE EBS R12 IMPLEMENTATION REVIEW

Oracle R12 Implementation Audit – Company Background

- US-based private technology company with SaaS offering model
- Oracle R12 modules installed: iProcurement, Purchasing, Payables, iExpense, Order Management, Receivables, Service Contracts, Advanced Collections, Cash Management, General Ledger, Fixed Assets, System Administration
- Third party application installed for revenue recognition along with Oracle implementation – residing on the same Oracle R12 database
- Custom home-grown applications for customer portal, subscriptions, tracking of usage, etc…

Oracle R12 Implementation Review Plan

- Review Oracle R12 design
- Review Business Process and IT controls for Oracle R12 and Revenue system
- Assess SDLC and Oracle R12 implementation project execution
- Provide recommendations

Oracle R12 Implementation Review Execution

- Reviewed Oracle R12 design documentation along with the "to-be" business process narratives and flowcharts
- Interviewed business process owners to understand the future process state
- Assessed design of business processes and controls along with Oracle R12 configurations from design documentation for all Orace R12 modules and revenue system
- Identified risks and areas of insufficient controls and configurations for business processes as well as SOD
- Provided recommendations for improvement of ERP control points, missing controls and associated configurations
- Provided recommendations for SOD controls
- Assessed design of IT controls over Oracle environment and provided recommendations for IT controls

Oracle R12 Implementation Review Execution - Continued

- Assessed Oracle R12 implementation project execution and SDLC focusing on the following:
  - Project structure, roles and communication
  - Design sign off
  - Data conversion
  - CRP and UAT testing
  - Production approval and cut-over to production
  - Issues tracking and resolution
- Provided recommendations for improvement (mostly around stake holder involvement, timely sign offs on design and testing, issues tracking)

Oracle R12 Implementation Review - Findings

- Business process & policies were not clearly defined for a number of areas and hence not configured in Oracle R12:
  - Process/policy for use of customer discounts, requisition, purchasing, invoice and JE approval limits were not defined
  - Business requirements for revenue recognition were not defined (i.e. revenue treatments for product offerings, revenue triggers, stratification criteria for BESP/ VSOE, etc…)
  - Process for handling invoices on hold was not clearly defined

- Roles and responsibilities were not defined for a number of processes (customer management, credit and collections, etc…) and the client planned to use seeded responsibilities that would create a large number of SOD conflicts

Oracle R12 Implementation Review - Findings

- Design was signed off with significant areas missing:
  - GL structure such as # of legal entities, primary ledgers, secondary ledgers, reporting currencies were not defined or agreed upon in the design
  - Financial reporting and consolidation requirements have not been defined
- Lack of key stakeholders oversight of the ERP implementation execution
- CRP and UAT testing did not test for end to end scenarios and did not have detailed test scripts with expected results or input data to conduct testing
- User training was limited and combined with UAT
- Disorganized UAT process and issues resolution slowed down the testing and pushed out the go-live date by 1 month
- Lack of streamlined issues resolution process required the company to extend the post-go live support period

Example of Findings and Recommendations

Module: Purchasing

Definitions: **Design Gap** - Areas where there is an absence or insufficiency of controls or their design.

Control Point - Potential operational or financial control.

Observation - These are activities we noted from our design assessments that could be modified to help improve efficiency.

Categories: Requisitions, Purchase Orders, Blanket Agreements, Receipts/ Accruals, Reports, Workflow/Notifications/Alerts, Data Migration, Controls & Compliance, Purchasing Business Process

Category	Design Gap/ Control Point/ Observation	Ref #	Description	Impact/ Control	Rationale/ Comments
Purchasing Orders Payables Invoices	Control Point	POYY, POZZ APXX, APVV	Recommend to define a control addressing 3-way and 2-way match. Invoices should be matched to purchase orders (2-way matching) and receipts (3-way matching) and systematically validated. For Purchasing options global setting to be 3-way consider the following: - The "Match Approval Level" configuration is set to 3-way. - The "Received Flag" should be enabled. For Supplier level: - The "Invoice Match Option" configuration is set to "Receipt". - The "Hold Unmatched Invoice" configuration is Enabled. "Match Approval Level" (2-way, 3-way or 4-way) can be overridden at the following levels: Purchasing options (global setting)>Supplier level>PO line shipment level>Item master. Consider a monitoring control over changes from 3 to 2 way match on the above levels.	Financial	Supplier may over-bill and invalid or inaccurate invoices may be paid that could increase the risk of unauthorized transactions and misstatement of accounts. This control should be configured together with a control around matching tolerances and other controls in place that mitigate the risk of changing the matching on different levels.

Remediation Efforts

- The company agreed with all findings after discussion
- Identified issues were prioritized and high priority ones (business policy and recommended ERP configurations) were addressed before go-live
- A number of issues related to controls implementation in business processes were partially addressed after go-live
- There is still a number of recommendations that the company considers to implement in wave 2 of business process optimization initiative
- In response to access and SOD issues, the company decided to implementation Oracle GRC

SUMMARY

Recap

- Technical and ERP subject matter expertise knowledge is critical to a successful ERP audit
- Use of tools and accelerators significantly speeds up the audit process and analysis
- Proper scoping of the audit is critical to the success of the project
- Stakeholders' support of ERP audit is key to make an impact and contribute to improvement of ERP environment
- Early involvement to perform ERP implementation review will save company funds remediating control issues post go-live

Questions?