AUDITING ERP IMPLEMENTATIONS TO AVOID COMMON PITFALLS

Institute of Internal Auditors: Philadelphia Chapter
2016 Fall Conference—The Power of Partnership—75 Years Strong
November 21, 2016

The Philadelphia Chapter was established in 1943 and is the fifth affiliate chapter of The Institute of Internal Auditors (IIA). The Philadelphia Chapter, its board of governors, its officers, The IIA, and today’s presenters are not responsible or liable for any acts or omissions and specifically disclaim any and all responsibility or liability for acts or omissions.

The material contained herein or communicated is for informational purposes only and should not be construed as accounting, financial, tax or legal advice. Please seek guidance specific to your questions or concerns from qualified advisors.

All content, including graphics or art work, is protected by law and may not be duplicated in any form without the express written permission from the Philadelphia Chapter.

© 2016 Philadelphia Chapter of the IIA

IIA PHILADELPHIA CHAPTER  2016 FALL CONFERENCE

PRESENTERS

- Steve Ems
  - Principal, technology and management consulting
  - Drives strategy, vision and client service to Enterprise Resource Planning- (ERP-) related services in the Philadelphia area

- Sudhir Kondisetty
  - Principal, risk advisory services
  - Oversees IT consulting services, such as Sarbanes-Oxley (SOX) Act of 2002, Service Organization Control (SOC) and Payment Card Industry (PCI) in the Philadelphia area
DISCUSSION TOPICS

- Common issues in ERP implementations
- Suggestions to mitigate the risk imposed by the common issues—At what phases should they be done?
- Segregation of duty (SOD) best practices and tools
- What does a successful implementation look like?

MOST COMMON ERP IMPLEMENTATION RISK

After go-live:
- ERP is not working as the business designed.
- Users' security is not working. Users cannot print.
- Users do not know how to do their job.
- Some business process functions are not working.
- System performance does not meet operational demand.
- Budget for the ERP implementation was two to three times more than estimated.
- ERP project didn’t go live on the estimated date.

Sound familiar?
Root cause of these issues could be more than meets the eye...

PRE-PROJECT PREP ERP IMPLEMENTATION RISK

- Due diligence not performed during vendor selection
- Unsuccessful business process mapping prior to implementation
- Implementation vendor contract not reviewed by an outside service provider for scope, etc., prior to contract being signed by key stakeholders
- Aggressive project plan developed
- Poor resource leverage model from implementers—high percentage of offshore usage and lack of onshore strategic experts
WHAT IS CONTINUOUS ERP PROJECT IMPLEMENTATION RISK?

Business process experts leading the business side of an ERP implementation do not understand the company’s true business operations, resulting in a lack of:

- Fit-gap analysis and/or BPDs (business process design documents), process flows, not completed prior to realization or validation of system design
- Phase gate criteria not established and approved by key stakeholders
- Criteria not clearly described for use of KDDs (key decision documents), including where available system functionality will be replaced with manual steps outside the system
- Project documentation retention strategy not development
- Customized functionality added where standard functionality was available
- ERP implementers not having an understanding of how to match ERP out-of-the-box functionality to clients business needs
- User acceptance testing not well defined and not well executed
ERP IMPLEMENTATION RISK

- Aggressive project plan that is unrealistic—project plan not detailed enough to understand dependencies among work streams.
- Lack of an adequate amount of project update meetings throughout the engagement.
- Lack of clear project governance strategy or strategy not communicated to all levels of the project.
- Project methodology selected, such as AERP (accelerated ERP) or agile RDS (rapid deployment), is not understood by all project team members.
- Succession plan for key members of project leadership, process design, security or IT architecture.
- Impact of other critical projects, either in IT or the business, which could stretch resources too thin or compromise deadlines.
- ERP best practice project plan template not used, resulting in unclear understanding of dependencies and engagement between parties involved.
- Lack of 50/50 shared responsibility between business and IT for accountability of the success of the project.
- Impact of other critical projects, either in IT or the business, which could stretch resources too thin or compromise deadlines.
- ERP best practice project plan template not used, resulting in unclear understanding of dependencies and engagement between parties involved.
- Lack of 50/50 shared responsibility between business and IT for accountability of the success of the project.
- Lack of tracking of all risk/escalation/closure of all project related issues—mismatched awareness of risk escalated to key stakeholders.
- Lack of tracking of scope changes.
- Lack of a communication strategy and/or strategy roll-out throughout the project.
- Ineffective or uninvolved steering committee.
- Unclear architecture plan for the to-be state.
- Unclear disaster recovery (DR)/business continuity plan (BCP) for go-live.
- Unclear identification of all interfaces and/or third-party systems during scoping.
- System performance estimated for the to-be-environment does not align to true daily operational needs.
ERP IMPLEMENTATION RISK

Data

- Data not classified properly, including regulatory data, privacy data, sensitive data, critical data
- Data owners not identified
- Data not properly migrated or validated
- Data cleansing not properly completed
- Testing of data migration not accurate or complete—evidence of testing not retained

Regulatory Requirements/Security and Controls

- Regulatory requirements not identified upfront
- Controls work stream not integrated into the project
- Security and control design dependencies not met by the project resulting in nonideal or nonoptimal controls being identified
- HR position/titles not able to directly map to a security model
- Wrong security design model selected (enabler vs. derived)
- No ERP security vulnerability assessments prior to go-live
- Controls embedded into the responsibility of off-shore or third-party vendors not communicated or confirmed in service-level agreement (SLA) contracts
- Critical general control level configurations not enabled at go-live
- Knowledge transfer of security/control options not provided

Organizational Change Management

- Change management and communications not aligned
- Communication of changes in the to-be state not communicated to all levels of the organization
- Change management and security not aligned regarding final roles and responsibilities covering ERP tasks and clear training to the end-users.
- Inadequate training of how end users will perform their job after go-live
- Lack of quality training documentation remaining at client site after implementers leave
ERP IMPLEMENTATION RISK

- Post-go-live support does not adequately address operational needs.
- Third-party vendor SLAs are not adequate and clear enough regarding roles and responsibilities.
- Resource planning is not adequate.
  - Current daily operational needs are not met due to critical key team members involvement and focus into the ERP implementation vs. their daily job.
- For public SOX clients, key control owners shift to ERP implementation, leaving a gap of control knowledge for the current operational state resulting in SOX control failures on the current state.

SUGGESTIONS TO MITIGATE RISK

- Clearly define test scripts and user acceptance testing process.
- Document business requirements for future state (not current state).
- Implement stringent project management and communication.
- Maintain a detailed project risk register.
- Require an executive steering committee to meet monthly to review key risks.
- Limit system customization to unique business differentiators.
- Define security roles for each employee at the beginning of the implementation and use throughout testing.
- Conduct a readiness assessment for infrastructure.
SOD—BEYOND BASIC AUDIT AND COMPLIANCE

- Rationalization/pressure—Can we control/impact/monitor?
- Opportunity is what we can impact the most by implementing internal control:
  - Strong top-down ERP SOD can effectively remove (or mitigate) the opportunity component of fraud.
  - This level of ERP SOD requires rethinking your ERP risk (i.e., broader than audit, SOX or other purely compliance-based concerns).
  - This approach must involve diverse stakeholders (IA, Finance, IT, etc.) and requires regular maintenance.

AUTOMATED VS. MANUAL SECURITY CONTROLS

<table>
<thead>
<tr>
<th>Application-Based</th>
<th>Manual-Based</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detective Control</td>
<td>Detective Control</td>
</tr>
<tr>
<td>Preventive Control</td>
<td>Preventive Control</td>
</tr>
</tbody>
</table>

Desirable

FIVE COMMON ERP SECURITY/SOD MYTHS

1. We have software (ERP, Oracle, etc.) with advanced security; therefore, SOD is not a major risk.
2. We have a GRC/CCM tool; therefore, SOD is not a major risk.
3. Our ERP system is audited by both internal and external auditors each year, and we get clean audit reports. Therefore, we are not at risk.
4. We have an SOD matrix to guide access provisioning; therefore, we are not at risk.
5. We have scores of manual financial controls (e.g., reconciliations), so our ERP risk is mitigated.
DEVELOPING EFFECTIVE SOD RULES

1. Identify key business cycles
   - “Top-down” approach based on business processes
   - Links to subprocesses and specific activities
2. Identify key systems
   - All systems (ERP and otherwise) involved in process
   - Are there cross-system processes/activities?
3. Identify key risks
   - Comprehensive risk assessment
4. Identify key controls (including SOD)
   - Should include mitigating/compensating controls
   - Are key monitoring, compliance and controls performed by personnel who have transactional access?

IDENTIFICATION OF SOD

• After key business cycles have been identified and all activities documented, map to corresponding systems or manual processes.
• Document the SOD and sensitive access rules and establish periodically.
  – Rules should be driven by degree of business risk (e.g. materiality, strategy, etc.).
• Identify “toxic relationships” or opportunities for fraud.

COMMON SOD CONFlicts

• Cross-business cycle access
• Initiation vs. approval
• Transactional vs. reconcile
• Develop vs. promote
• Subsidiary vs. G/L
• Subsidiary G/L vs. consolidate
• Business access vs. IT access
• Master data vs. transactional
BUILDING THE SOD MATRIX

• Compensating controls—Lower, but do not eliminate, effects of control deficiency.
• Mitigating controls—Eliminate effect of control deficiency.

<table>
<thead>
<tr>
<th>Automated</th>
<th>Manual</th>
</tr>
</thead>
<tbody>
<tr>
<td>Built into ERP or deployed through GRC tool</td>
<td>Though manual, should still be documented in CCM/GRC tool</td>
</tr>
</tbody>
</table>

CCM/GRC TOOLS

• Continuous control monitoring (CCM)/governance, risk and compliance (GRC) tools
• Software solutions that provide ways to manage the overall IT risk compliance programs, including:
  – Internal audit controls testing documentation management
  – IT policy management
  – Dashboard reporting of control findings with remediation tracking workflows
  – Security operations management
  – Elevated security access management
  – Password change management
  – Management of changes made to ERP software
  – ERP controls monitoring

WHY CCM/GRC?

• ERPs are complex, always changing.
• Automated controls can reduce manual processes and provide value by:
  – Driving efficiency (less time to perform SOD/sensitive access analysis)
  – Reducing likelihood of false positives/negatives
• It reduces opportunity for fraud.
• It reduces costly compliance efforts.
• It automates user provisioning.
• It monitors/prevents conflicting access.
• It monitors sensitive access, facilitates review.
CCM/GRC—COMMON PITFALLS

• Implementation
  – Poor initial configuration
  – Poor (or nonexistent) risk assessment
  – Lack of ownership
  – Customizations (e.g., custom transactions) not considered
  – Manual controls not considered in rules (management override)
  – Cross-application access not accounted for

• Maintenance
  – No process to periodically update rules
  – Poor design of compensating/mitigating controls
  – Business changes not accounted for, including:
    • Acquisitions
    • New business lines
    • Technology changes
  – Risks/risk assessment never refreshed
  – False-positives/negatives

WHAT DOES A SUCCESSFUL IMPLEMENTATION LOOK LIKE?

• Go-live is a “nonevent.”
• Project is on time and on budget.
• Final system matches business requirements, with flexibility to change as needed.
• There is no system latency or access limitations.
• Executive management is able to access the key information required to make decisions.

SURVEY
HELP US IMPROVE THE CONFERENCE!

You will receive a survey via email in the next few days. Please respond to provide feedback on the speakers and the overall session.

This evaluation is how we determine the changes needed to make us better!

Thank you!!