Project Risk and Pre/Post Implementation Reviews

Material Changes to the System of Internal Control

VGFOA Conference (Virginia Beach, VA)
May 20, 2015
Agenda/Objectives

- Understand why system implementations fail
- Identify key system implementation risk areas
- Define types of implementation reviews
- Describe key implementation practices
- Describe the Auditor’s role and audit considerations
- Identify audit resources and tools available
Many organizations are deploying a number of strategic, high profile, capital intensive information technology (IT) or business projects.

Unfortunately, many projects fail:

- Delivered late
- Expanded budgets
- Don’t meet stakeholder expectations

39% of all projects are successful
43% are delayed
59% experience cost overruns

Source: The Standish Group (2013)
McKinsey 2012 Study revealed that for IT projects budgeted at $15 million or higher:
- 40% of these projects failed
- 17% threatened the company’s existence

The Standish Group examined 3,555 IT projects over nine years that had labor costs of $10 million or more
- Only 6.4% were successful
- 52% were either over budget, behind schedule or didn’t meet user expectations
Why Implementations Fail

- **Implementation or Hardware Errors**
  - Lack of software fit between the system and the organization.

- **Unrealistic implementation expectations**
  - Scope of implementation not clearly defined allowing vendor scope creep and project slippage.

- **Poor Development Practices**
  - Lack of controls around the change management process

- **Poor integration with Entity User and Management**
  - Lack of management buy-in, involvement, and user training

- **Budget Constraints**
  - Limited IT Budgets leading to cutting corners.
Northrop Grumman takes blame for Va. IT services outage

- Northrop Grumman today apologized for an outage that began last Wednesday and caused 26 Virginia state agencies to lose their Web services, some for more than a week.
- The Virginia Information Technologies Agency (VITA) outsources the management of its data centers to Northrop Grumman through a 10-year, $2.4 billion contract that it signed in 2005.
- The outage affected 13% of the Commonwealth's file servers.
- VITA's contract with Northrop Grumman has been criticized in the past for a number of project delays, cost overruns and performance problems that included other service outages.
- After an audit by Virginia's Joint Legislative Audit and Review Commission last year, VITA's contract with Northrop Grumman was modified, resulting in more stringent performance requirements and greater accountability. The contract, however, also boosted payments to Northrop Grumman by $105 million over nine years.
- In its apology, Northrop Grumman admitted that its technology partnership with the Commonwealth of Virginia's government has "experienced its share of obstacles," but went on to say that problems of this sort are not unusual with large technology transformation programs.
Implementation Opportunities

The planned changes and implementation of a major IT System are intended to improve the Organization’s enterprise risk management including:

- **Improving** the Organization’s ability to meet its operational, financial reporting and compliance objectives.

- **Creating efficiencies** (including cost savings) in managing Organization’s business.

- **Effectively safeguarding** shareholder/taxpayer assets and demonstrate sound financial stewardship.
Risk and Requirements

- **Change in Enterprise Business Systems** – the implementation of a major system covers most, if not all, significant business cycles and represents a *material change* to the Organization’s system of internal control.

- **Risk** – Change in systems also increases the Organization’s exposure to unintended consequences affecting many enterprise risk areas e.g., inefficiency, error and fraud until the control environment matures on the new system.

- **Audit Requirements** – Auditing standards require External Auditors to consider changes to a client’s system of internal control. Therefore, the auditor should validate the effectiveness of key IT general controls (ITGCs) to obtain comfort over the information technology systems that house, transport, store, and transform data for reliable financial reporting.
Options and Requirements

Three Options:

1. Pre & Post Implementation Review
   - Performed under Consulting Standards

2. Post Implementation Review Only (Extended Audit Procedures) – Required for AUC315
   - Performed under Audit Standards

3. Segregation of Duties (SoD) and Logical Access Review
   - Performed under Consulting Standards
   - Can be done in conjunction with Option 1 or 2
Implementations Reviews

  - Planning
  - Requirement Analysis
  - System Design
  - System acquisition/development
  - System Implementation

- Post-Implementation – Subsequent Review of the Process after Implementation
  - System Design
  - System acquisition/development
  - System Implementation
### Common Risks

<table>
<thead>
<tr>
<th>AREAS</th>
<th>Project Management</th>
<th>Business Process</th>
<th>Application Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>KEY RISKS</strong></td>
<td>• Project Scope is not clearly defined or managed. A good plan or just a plan</td>
<td>• Lack of alignment of System with business processes</td>
<td>• Key controls not configured, considered or available in new system</td>
</tr>
<tr>
<td></td>
<td>• Part time project management</td>
<td>• Decentralized decision making</td>
<td>• Programmed application controls incorrectly coded</td>
</tr>
<tr>
<td></td>
<td>• Insufficient testing approach</td>
<td>• User resistance and customization</td>
<td>• Continued reliance on manual procedures</td>
</tr>
<tr>
<td></td>
<td>• Insufficient stress testing and/or capacity planning</td>
<td>• Regulatory and other requirements overlooked</td>
<td>• Implementer does not provide adequate focus on controls, only functionality and</td>
</tr>
<tr>
<td></td>
<td>• Quality control system for project management is not adequately considered or</td>
<td>• Lack of user procedures / training</td>
<td>efficiency</td>
</tr>
<tr>
<td></td>
<td>established</td>
<td>• Ineffective operating effectiveness of controls.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Missing/overlooked controls</td>
<td></td>
</tr>
</tbody>
</table>
**Common Risk (cont.)**

<table>
<thead>
<tr>
<th>AREAS</th>
<th>Logical Access - Security</th>
<th>Change Management</th>
<th>Data Conversion</th>
</tr>
</thead>
</table>
| KEY RISKS | • Logical access is an after thought  
• Error and fraud occurs until the control environment matures on the new system  
• Inappropriate access granted to functional users and implementers  
• Provisioning process is not clearly defined  
• Segregation of duties is not adequate designed or considered | • Change management process for pre and post implementation are not well defined and/or followed  
• Unauthorized changes to systems  
• Failure to make necessary changes  
• Issue/resolution management process not clearly defined  
• Changes not analyzed/tested for across business impact | • Control total reconciliations and exception reports are poorly designed  
• Time to convert has been poorly estimated resulting in significant manual intervention and time delays  
• Lack of data cleansing results in misstatement of information or data integrity problems  
• Incorrect data mapping resulting in processing data error or misclassifications |
**Implementation Requirements**

**Functional**
Business processes that users expect to be fully, or at least partially, automated by the new system. These would include such things as three-way match, reasonableness tests for salary increases, automated purchase order management and automated budgetary performance monitoring.

**Technical**
Capability of the system to conform to and complement protocols inherent in the technology infrastructure. Examples would include compatibility of access control methodology with Windows Active Directory and functionality supporting seamless transition to disaster recovery mode. Also, consideration for cloud computing.

**Operational**
Capability to support day-to-day functions of business unit users, including certain automated workflow, user-friendly query capabilities, comprehensive audit trail of user activities and flexible reporting capabilities.
How To Define Requirements

- Form a task force with representatives from all stakeholder groups – this is not just an IT project
  - Define Requirements at a granular level
  - This is a bottom-up process
- Make sure the Requirements reflect the real world
- Make sure that the Requirements look to, and accommodate for, future growth, expansion and change
Auditor’s Role

Auditor’s role is to help organizations determine whether software initiatives follow established development methodologies and procedures, meet organizational needs, and include adequate security and management controls. Key areas to consider are planning, methodology assessments, reports of project results, and post-implementation reviews. This includes review of:

- Project Management
- Application Controls
- Application Security
- Change Management
- Data Conversion
Auditor Value

- Value that can be added by Auditor involvement during the implementation process includes: d control environments
  - Independent third party perspective,
  - Subject Matter Knowledge over systems
  - Knowledge of current state business processes
  - Knowledge of key Application Controls
  - Previous experience testing Logical access and Change Management controls
  - Experience in review Data Conversion
Procedures (High Level)

Review and test the following:

- Project Plan and Milestones against COBIT 4.1 SDLC
- Project Risk assessment and evaluation criteria affecting “go” or “no go” decisions
- Future state internal control design
- Conference Room Pilots (CRP)
- Training
- Systems Acceptance Testing (SAT)
- Systems Integration Testing (SIT)
- User Acceptance Testing (UAT) and training
- Interface Testing
- Data Conversion Testing, Data Migration & System Cutover
- Key report testing
- Defects, issues, errors and remediation
- Business cycle transaction walk-throughs and expected results
- Mock financial close testing (Month and Year End)
**Project Management - Planning**

- Evaluation of project objectives, structure, phases, and timeline, as well as assess the impact of the project on the control environment.
  - Includes Project Charter, Executive Summaries, Steering Committee Presentations, Stakeholders

- Evaluation of project the project plan
  - Business Requirements definition,
  - Resource roles and responsibilities and assignments
  - Evaluation of software requirements
  - Scheduled communications and method
  - Testing requirements (System and User Acceptance testing)
  - Detailed implementation requirements
  - Infrastructure configuration (i.e. backup and recovery)
  - Data Conversion requirements
  - Disaster Recovery preparation
  - Deliverable milestones and signoff requirements
  - Business readiness and cutover requirements
  - Post implementation plan and user support
Project Management - SDLC

- Project management for System Development Life Cycle
  - Clear definition of the scope for the project
  - An approved project request
  - Clear and concise process for scope change and approval
  - Scope Change Management
  - Formal Assessment or Quality Assurance process
  - Formal issues tracking and reporting process
  - Establishment and communications through executive reporting and user status reporting, Steering Committee
  - Involvement of key users
  - Monitoring controls to ensure on-time delivery and project milestones are being met (Measurement of progress, Budget to actual)
  - Documentation repository
  - Project plan development and maintenance assigned
  - Controls are mapped from current state to future state
Project Management - Cutover

- Evaluate that the business has developed and documented an acceptance plan and criteria for Go-Live. Evaluate the acceptance criteria for the following elements:
  - Critical business processes are ready to an acceptable level
  - Critical users are ready and at an acceptable training level to reduce impact
  - Infrastructure is ready and critical processing are operating as intended
  - Issues identified are resolved to an acceptable level
  - Any existing bugs and defects are appropriately communicated to affected parties prior to Go-Live
  - Critical operations and logistics are ready
GO or NO GO Decision Criteria

- Training (% complete)
- Testing (% complete)
- Issues/Defects Log – P1, P2, P3 etc.
- Issues/Defects Log (% complete)
- Data conversion
- Change Order Management
  - System requirements
  - Human capital
- Communication Plans
  - Staff, customers, vendors, business partners etc.
Application Controls

- Evaluate transaction specific controls to determine that business process documentation includes business controls mapping, account mapping, and updated process narratives for current and future state to determine required application. Test key application controls for effectiveness.
Logical Access

- Test the process in place for safeguarding IT systems and resources against unauthorized use, modification, disclosure, or loss
  - Authentication
  - Privilege Access
  - User provisioning
  - Role design
  - Segregation of Duties
Segregation of Duties

- Segregation of Duties (SOD) and system based logical access controls
- Review and inspect evidence of project team’s self-assessment procedures to determine future state internal control design requirements.
- Review internal control design for planned pre “go-live” user provisioning, periodic access review, configuration change management for authorization levels and workflow routing such as, purchase requisitioning.
Change Management

- Change management is the process that provides for the analysis, implementation, and follow-up of all changes requested and made to the existing infrastructure
  - Authorization of changes
  - System and UAT Testing
  - Access to promote changes
Data Conversion

- Evaluate data conversion results to determine results are signed off by management and are adequately documented to provide an audit trail, including steps performed, balances and/or controls totals reconciled and test success or failure with appropriate follow-up if necessary.
  - Reconcile totals/balances and ensure they are within documented tolerance levels.
  - Evaluation corrective action for any errors identified
Tips and Recommendations

- Ensure “Test” environment reflects expected production environment.
  - Use of cloned production data vs. dummy data
  - Just because it worked in “Test”….
  - Performance is slow….
- Risks/Rewards with “train the trainer” approach…
- Procurement cycle internal controls (highest risk)
- Key report testing…
- Mock financial close training and testing…
- “We have a workaround for that…” = CUSTOMIZATION
- Post go live production support plan (60 days starting when?)
- Anticipating project team and internal employees turnover…
Resources

Control Frameworks/Approaches to implement systems

- COBIT Framework for ITGCs including SDLC
- ISO/IEC 12207 Software Life cycle processes
- IEEE (Standard setter)
- NIST 800-64
- PMBOK (Standards issued by Project Management Institute)
Summary

- Review reasons why system fail
- Describe system development approaches and key Risk areas of interest
- Define pre- and post-implementation
- Describe the Auditor’s role and audit considerations
- Identify audit resources and tools available
Questions

Contact:
Chloe Haidet | Senior Manager – Risk Advisory Services
chaidet@cbh.com | 404.733.3322

Cherry Bekaert LLP
cbh.com
Appendix A

Example Assessment Criteria
Assessment Criteria

COBIT 4.1 Control Objectives (abbreviated)

- **7.1 Training** - Train the staff of the affected user departments and the operations group of the IT function in accordance with the defined training and implementation plan and associated materials, as part of every information systems development, implementation or modification project.

- **7.2 Test Plan** - Establish a test plan and obtain approval from relevant parties.

- **7.3 Implementation Plan** - Establish an implementation plan and obtain approval from relevant parties.

- **7.4 Test Environment** - Establish a separate test environment for testing. This environment should reflect the future operations environment.

- **7.5 System and Data Conversion** - Ensure that the organization’s development methods provide for all development, implementation or modification projects.

- **7.6 Test of Changes** - Ensure that changes are tested in accordance with the defined acceptance plan and based on an impact and resource assessment that includes performance sizing in a separate test environment.

- **7.7 Final Acceptance Test** - Ensure that procedures provide for, as part of the final acceptance or quality assurance testing of new or modified information systems, a formal evaluation and approval of the test results by management of the affected user department(s) and the IT function.

- **7.8 Promotion to Production** - Implement formal procedures to control the handover of the system from development to testing to operations in line with the implementation plan.
7.1 – Training Plan

Train the staff of the affected user departments and the operations group of the IT function in accordance with the defined training and implementation plan and associated materials, as part of every information systems development, implementation or modification project.

- The training plan clearly identifies learning objectives, resources, key milestones, dependencies and critical path tasks impacting the delivery of the training plan. The plan considers alternative training strategies depending on business needs, risk level and regulatory and compliance requirements.

- The Training plan identifies and addresses all impacted groups, including business end users, IT operations, support and IT application development training, and service providers.

- There is a process to ensure that the training plan is executed satisfactorily. Complete the documentation detailing compliance with the training plan.

  - Training is monitored to obtain feedback that could lead to potential improvements in either the training or the system.

- All planned changes are monitored so that training requirements have been considered and suitable plans created.
7.2 – Test Plan

Establish a test plan and obtain approval from relevant parties. The test plan is based on organization-wide standards and defines roles, responsibilities and success criteria. The plan considers test preparation (including site preparation), training requirements, installation or update of a defined test environment, planning/performing/documenting/retaining test cases, error handling and correction, and formal approval. Based on assessment of the risk of system failure and faults on implementation, the plan should include requirements for performance, stress, usability, pilot and security testing.

- A documented test plan exists, which aligns to the project quality plan and relevant organizational standards.

- The test plan reflects an assessment of risk and all functional and technical requirements are tested.

- The test plan addresses need for internal or external accreditation of outcomes of the test process (e.g., financial regulatory requirements).

- The test plan identifies necessary resources to execute testing and evaluate the results. Includes construction of test environments and staff for the test group.

- The test plan identifies testing phases appropriate to the operational requirements and environment. The test plan considers:
  - site preparation
  - training requirements,
  - documenting, retaining test cases,
  - error and problem handling, correction and escalation, and
  - formal approval.

- Test plan establishes clear criteria for measuring the success for each testing phase.
- Determine plan establishes remediation procedures when the success criteria are not met.
Establish an implementation plan and obtain approval from relevant parties. The plan defines release design, building of release packages, rollout procedures/installation, incident handling, distribution controls (including tools), storage of software, and review of the release and documentation of changes. The plan should also include fallback/backout arrangements.

- Define a policy for numbering and frequency of releases.
- Confirm that all implementation plans are approved by stakeholders, including technical and business.
- Create an implementation plan reflecting the outcomes of a formal review of technical and business risks.
- Obtain commitment from third parties to their involvement in each step of the implementation.
- Identify and document the fallback and recovery process.
7.4 – Test Environment

Establish a separate test environment for testing. This environment should reflect the future operations environment (e.g., similar security, internal controls and workloads) to enable sound testing. Procedures should be in place to ensure that the data used in the test environment are representative of the data (sanitized where needed) that will eventually be used in the production environment. Adequate measures should be provided to prevent disclosure of sensitive test data. The documented results of testing should be retained.

- The test environment is representative of the future operating landscape, including likely workload stress, operating systems, etc.
- The test environment is secure and not capable of interacting with production systems.
- Create a database of test data that are representative of the production environment.

- Protect sensitive test data and results against disclosure, including access, retention, storage and destruction.
- Put in place a process to enable proper retention or disposal of test results, media and other associated documentation to enable adequate review and subsequent analysis as required by the test plan.
7.5 – System and Data Conversion

Ensure that the organization's development methods provide for all development, implementation or modification projects and that all necessary elements, such as hardware, software, transaction data, master files, backups and archives, interfaces with other systems, procedures, and system documentation, be converted from the old system to the new according to a pre-established plan. An audit trail of pre- and post-conversion results should be developed and maintained. A detailed verification of the initial processing of the new system should be performed by the system owners to confirm a successful transition.

- Define a data conversion and infrastructure migration plan. Consider, for example, hardware, networks, operating systems, etc.
- The data conversion plan incorporates methods for collecting, converting and verifying data to be converted and identifying and resolving any errors found during conversion.
- The data conversion plan does not require changes in data values unless absolutely necessary for business reasons.
- Consider real-time disaster recovery, business continuity planning, and reversion in the data conversion and infrastructure migration plan where risk management, business needs, or regulatory/compliance requirements demand.
- Co-ordinate and verify the timing and completeness of the conversion cutover so there is a smooth, continuous transition with no loss of transactions.
- There is a backup of all systems and data taken at the point prior to conversion, audit trails are maintained to enable the conversion to be retraced, and there is a fallback and recovery plan in case the conversion fails.
7.6 – Testing of Changes

Ensure that changes are tested in accordance with the defined acceptance plan and based on an impact and resource assessment that includes performance sizing in a separate test environment by an independent (from builders) test group before use in the regular operational environment begins. Parallel or pilot testing should be considered as part of the plan. The security controls should be tested and evaluated prior to deployment, so the effectiveness of security can be certified. Fallback/backout plans should also be developed and tested prior to promotion of the change to production.

- Testing of changes is undertaken in accordance with the testing plan. The testing is designed and conducted by a test group independent from the development team.

- The tests and anticipated outcomes are in accordance with the defined success criteria set out in the testing plan.

- Consider using clearly defined test instructions (scripts) to implement the tests.

- Undertake tests of security in accordance with the test plan. Measure the extent of security weaknesses or loopholes.

- Undertake tests of system and application performance in accordance with the test plan. Consider a range of performance metrics.

- When undertaking testing, the fallback and rollback elements of the test plan have been addressed.

- Identify, log and classify errors during testing. Ensure that an audit trail of test results is available.
7.7 – Final Acceptance Test

Ensure that procedures provide for, as part of the final acceptance or quality assurance testing of new or modified information systems, a formal evaluation and approval of the test results by management of the affected user department(s) and the IT function. The tests should cover all components of the information system (e.g., application software, facilities, and technology and user procedures) and ensure that the information security requirements are met by all components. The test data should be saved for audit trail purposes and future testing.

- The scope of final acceptance evaluation activities covers all components of the information system.
- The categorized log of errors found in the testing process has been addressed by the development team.
- The final acceptance evaluation is measured against the success criteria set out in the testing plan. The review and evaluation process is appropriately documented.
- Document and interpret the final acceptance testing results, and present them in a form that is understandable to business process owners.
- Business process owners, third parties (as appropriate) and IT stakeholders formally sign off on the outcome of the testing process as set out in the testing plan.
7.8 – Promotion to Production

Implement formal procedures to control the handover of the system from development to testing to operations in line with the implementation plan. Management should require that system owner authorization be obtained before a new system is moved into production and that the new system has successfully operated through all daily, monthly, quarterly and year-end production cycles before the old system is discontinued.

- A formal cutover plan should be established.
- Formal sign-off of the readiness of the entity to move to production in the new environment should be formally documented from key stakeholders and project management.