SDLC- Key Areas to Audit in IT Projects

ISACA Geek Week 2013
8/21/2013
Introductions and Projects Overview
**Presenters**

<table>
<thead>
<tr>
<th>Charlie Miller and Andrew Gerndt</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Coca-Cola Company Principal IT Auditors</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mike Shipham</th>
</tr>
</thead>
<tbody>
<tr>
<td>PricewaterhouseCoopers LLP Project Assurance Director</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
## Agenda

<table>
<thead>
<tr>
<th>Topic</th>
<th>Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Introductions and Projects Overview</td>
<td>15 minutes</td>
</tr>
<tr>
<td>2. IT projects- the risks</td>
<td>15 minutes</td>
</tr>
<tr>
<td>3. Key areas to audit</td>
<td>20 minutes</td>
</tr>
</tbody>
</table>
Coca-Cola at a glance

280+
We support more than 280 physical activity and nutrition education programs in more than 115 countries, and we are committed to having a program in every country where we operate by 2015.

3500+
Products Worldwide

BECAME THE FIRST BRAND TO RECORD 50 MILLION “LIKES” ON FACEBOOK (SEPTEMBER 2012).

21% North America
14% Europe
29% Latin America
18% Eurasia & Africa
18% Pacific

2012 Worldwide Unit Case
Volume Geographic Mix
Project - sharing a Coke
Getting to know you

1. Are you involved in an IT project at your company?

2. How has Internal Audit been involved in this project?
   a. Mostly in planning
   b. Mostly in execution
   c. Doing a post implementation review
   d. Not at all
Getting to know you

1. What has been the greatest challenge with this project?
   a. Planning
   b. Execution
   c. Post implementation
   d. Other
Sound familiar?

How the customer explained it
How the Project Leader understood it
How the Analyst designed it
How the Programmer wrote it
How the Business Consultant described it
How the project was documented
What operations installed
How the customer was billed
How it was supported
What the customer really needed
IT Projects – the risks
Are IT projects successful?

PwC’s 2012 survey indicates that 200 global companies were **spending over $4.5 B on projects** to deliver changes required to implement their strategy.

- **20% of ERP implementation projects are not completed.** *(Gartner)*
- **51% of ERP implementation viewed as a failure** *(Robbins-Gioia Survey)*
- **71% of ERP projects do not meet the expectations of senior management** *(CSC Index/AMA Survey)*
- **84% of projects do not meet all criteria for success** *(Standish Group)*
- **2%**: Companies that had 100% of their projects on time, within budget, to scope and delivering the right business benefits. *(PwC Global Survey on State of Project Management)*
- **35%**: Number of companies where system projects deliver expected business benefits *(PwC Global Survey on State of Project Management)*
IT project risks

In your experience, what IT project risks have you seen?
Reasons for program failures

- Poor estimates/ Missed deadlines
- Lack of executive Sponsorship
- Poorly defined goals/ objectives
- Change(s) in scope mid-project
- Insufficient resources
- Poor Communication
- Lack of stakeholder involvement
- Change in environment
- Change in strategy
- Inadequate risk planning
- Lack of change management

Source: PwC's 3rd Global Survey on State of Project Management (2012)
**Key areas of project risk**

Risks are not isolated to classic project management artifacts, but extend to a broader ‘risk universe’.

**Technology**
- Infrastructure
- System architecture
- Networking
- Security
- Availability
- Performance
- Disaster recovery

**Data**
- Data Structures
- Mapping
- Cleansing Effort
- Conversion and validation
- Data governance
- Backup and recovery
- BI and reporting strategy

**Process and Solution**
- Requirements
- Business processes
- System Development Life Cycle
- Data
- Controls
- Bolt-ons
- Interfaces/integrations

**Governance**
- Strategic Alignment
- Senior Management Commitment
- Sponsorship / Champions
- Governance and Decision making
- Synergy identification and tracking

**Program Management**
- Time schedules
- Budgets
- Resources/staffing
- Vendors
- Knowledge transfer
- Issue and Risk management
- Scope management

**Organization**
- Business impacts
- Training
- Communication
- Organizational alignment
- Change management
- Compliance and controls
- Business continuity
Key areas to audit
### PM Maturation Model

<table>
<thead>
<tr>
<th>Maturity Levels</th>
<th>Characteristics</th>
</tr>
</thead>
</table>
| 5. Enterprise Standards and Program Management Culture Exists | - Strategic resource management crosses the enterprise  
- Program value management occurs through project portfolio management, prioritization and interdependency management  
- Change issues address organizational design and culture change |
| 4. Cross Business Unit Program Management Implemented  | - Measures of process quality are collected and processes are managed  
- Process performance target zones are established |
| 3. Programs Managed with a Strategic Enterprise Focus | - Management processes address multiple projects  
- A PMO is used for efficiency and risk management is proactive  
- Projects and programs assume a strategic focus with status visibility provided to a wider stakeholder audience |
| 2. Stable Project Management Processes                | - Work projects are controlled and basic PM capability established  
- Management visibility into project status at predefined checkpoints and milestones and react to problems as they occur  
- Initial use of metrics at the project performance level |
| 1. Unstable Project Performance (Ad Hoc)              | - Processes poorly defined  
- Managers have little visibility into status and processes employed  
- Success achieved through "heroics" |
**Who plays a part in managing program risk?**

Large transformation projects typically have a number of functions supporting risk and quality management. Understanding the respective roles and levels of assurance provides a holistic view of current assurance levels and helps identify the gaps that may need to be addressed.

**PMO monitoring and assurance activities**

Examples of Level 2 activities:
- **Operational risk** teams
- Compliance teams
- Organizational or independent PMO
- Targeted QA activities (from within the organization but independent of the project)
- Product vendor provided assurance

**External vendor and internal audit**

Examples of Level 3 activities:
- Internal Audit reviews (part of the annual plan)
- ‘Health checks’ and targeted specialist ‘Deep Dive’ reviews
- External Audit reviews
# How can audit add value to a project?

<table>
<thead>
<tr>
<th>1. Navigate the integration risk landscape</th>
<th>2. Understand stakeholder perspectives and provide deeper insights</th>
<th>3. Cut through the clutter</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Questions</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>How well aligned is internal audit’s plan with the critical risks facing the organization?</td>
<td>Does internal audit provide a point of view to help the business improve its responses to risk?</td>
<td>How effectively does internal audit communicate with stakeholders?</td>
</tr>
</tbody>
</table>
How can audit add value? Controls are often overlooked

Cost of controls increases as project progresses
Managing risk over the program lifecycle

Assess
- Is the ‘case for change’ robust with clear scope, business outcomes and ownership?

Design
- Will the organization & technical design deliver the benefits?

Construct
- Is the solution being built as designed and robustly tested?

Implement
- Is the business ready to go with detailed go live and support plans in place?

Operate & Review
- Are the benefits being delivered and what could be improved?

Delivering Change
- Project governance and mgmt review
- Planning and mobilization
- Business case review
- High level target operating model
- Organization change strategy
- Deployment strategy
- Business process design
- Data and reporting design
- Test and data conversion strategies
- Security & controls
- People and Org Design
- Dedicated vendor management
- Solution testing and remediation
- Training plans and execution
- Data conversion
- Security and control configuration
- Business continuity planning
- Benefits management plan
- Support model design
- Test and training results
- Go-live process
- Data conversion process
- Transition to business as usual (BAU) planning
- Stakeholder engagement
- Go-live readiness assessment
- 30-90 day support
- Business adoption
- Benefits realization
- Compliance and controls certification

Driving Change

Is the Change Management approach appropriate and delivering success?

Is the organization engaging key stakeholders (including existing vendors/partners) throughout the change?

Is the program being effectively governed against guiding principles and managed across all workstreams?

Is delivery of business benefits a key focus throughout the lifecycle?
Further reading and Appendix Slides

Internal Audit’s Role in Transformational Change


## For more information: Contact

<table>
<thead>
<tr>
<th><strong>Charlie Miller</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>The Coca-Cola Company</td>
<td>678-516-8149</td>
</tr>
<tr>
<td>Principal IT Auditor</td>
<td><a href="mailto:cmiller@coca-cola.com">cmiller@coca-cola.com</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Andrew Gerndt</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>The Coca-Cola Company</td>
<td>404-676-4897</td>
</tr>
<tr>
<td>Principal IT Auditor</td>
<td><a href="mailto:agerndt@coca-cola.com">agerndt@coca-cola.com</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Mike Shipham</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PricewaterhouseCoopers LLP</td>
<td>312-298-4188</td>
</tr>
<tr>
<td>Director</td>
<td><a href="mailto:michael.a.shipham@us.pwc.com">michael.a.shipham@us.pwc.com</a></td>
</tr>
</tbody>
</table>
Thank you
Video

2013 Creative Marketer of the Year
Appendix Slides- Examples of control considerations by project phase
**Top 10 Keys to success**

**Key events that may contribute to a successful Project Audit:**

1. Stakeholder buy-in & tone at the top, understanding & acceptance of engagement
2. Staffing, proper technical skills, qualifications and capabilities allowing the team to quickly establish credibility
3. Understanding project needs and expectations, as well as the level of comfort desired
4. Scoping appropriately, leveraging a risk based approach and delivering upon the agreed scope
5. Up-front communication regarding scope of review, extent of review, timing of review and level of details to be provided in reporting
6. Execution and completion of work within defined budget and schedule
7. Change agility, being able to change with the project needs (adjust timeline, etc.) but avoiding scope creep
8. Communication to all parties
9. Relevance, providing actionable useful and timely deliverables (reporting) – consider requirements of the audience (i.e. Audit Committee, Sponsor, Project Manager, etc.)
10. Monitoring project progress between checkpoint reviews to minimize ramp-up time required at each checkpoint
Project assurance – Control considerations

- Define
- Design
- Build & Test
- Deliver
- Imp. Support
- Maintain

ITGCs

- A clear understanding of Business Processes in Scope.
- A clear understanding of the current status of controls and the proposed change.
- A clear understanding of the control risks to be addressed:
  - Operational
  - Compliance
  - Financial Reporting
- Understanding of the efficiency improvements required
- Appropriate expertise assigned to deliver appropriate controls
- Appropriate activities included in project plan to deliver appropriate controls

Business Process

Interfaces

Data Quality
Design appropriate ITGCs based on the risks identified
Determine what the key controls are
Ensure specifications of ITGCs are produced for input into the next phase.
Ensure there is a clear understanding of current interfaces and interface controls and how these may be changing.

A high level plan has been developed to show interface development activities, priorities, and contingency plans should desired interfaces be unavailable when needed by business teams.
**Project assurance – Control considerations**

- **Define**
  - ITGCs
  - Business Process
  - Interfaces
  - Data Quality

- **Design**
  - ITGCs
  - Business Process
  - Interfaces
  - Data Quality

- **Build & Test**
  - ITGCs
  - Business Process
  - Interfaces
  - Data Quality

- **Deliver**
  - ITGCs
  - Business Process
  - Interfaces
  - Data Quality

- **Imp. Support**
  - ITGCs
  - Business Process
  - Interfaces
  - Data Quality

- **Maintain**
  - ITGCs
  - Business Process
  - Interfaces
  - Data Quality

- Ensure appropriate business process controls are developed (in line with the specifications from the previous phases)
- Make sure controls that are developed are tested appropriately
### Project assurance – Control considerations

<table>
<thead>
<tr>
<th>ITGCs</th>
<th>Business Process</th>
<th>Interfaces</th>
<th>Data Quality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define</td>
<td>Design</td>
<td>Build &amp; Test</td>
<td>Deliver</td>
</tr>
</tbody>
</table>

- Setup of integration test environment should include execution of data conversion procedures to validate completeness and accuracy of conversion procedures.
- Data conversion reconciliation specifies tests to prove that the converted data is sufficiently “clean” to be used within the new environment and data inaccuracies have not been introduced during the conversion process.
### Project assurance – Control considerations

<table>
<thead>
<tr>
<th>ITGCs</th>
<th>Design</th>
<th>Build &amp; Test</th>
<th>Deliver</th>
<th>Imp. Support</th>
<th>Maintain</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Business Process

- Define
- Design
- Build & Test
- Deliver
- Imp. Support
- Maintain

#### Interfaces

- Data Quality

- In instances where data has not been converted or migrated (i.e., only summary data is in new system), is the historical data available in a read only environment for reference purposes?