Dallas IIA Chapter / ISACA N. Texas Chapter
Auditing Project Management Controls

January 7, 2010
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Management Office Overview</td>
<td>3</td>
</tr>
<tr>
<td>Aligning CobIT standards with PMBOK</td>
<td>12</td>
</tr>
<tr>
<td>Project Management Audit Recommendations</td>
<td>19</td>
</tr>
</tbody>
</table>
Manager in the Dallas Business Advisory Services practice of **Grant Thornton, LLP**. Fifteen years of technology experience, including management of several global efforts including implementations of corporate financial applications, rollout of large scale development efforts, SOX S404 I/T internal audits, and implementation of several I/T business process and controls.

Before joining Grant Thornton, David served as senior manager for an international telecom software company directly responsible for several I/T business services including program management, internal I/T 404 audit, PeopleSoft application management, development and support, desktop management, change management, business continuity, and solutions delivery.
Project Management Overview
Project management initiatives are fraught with risks as evidenced by facts* from surveys of CIO's

- 63% of projects have schedule delays
- 49% of projects exceed budget
- 45% of projects do not meet business objectives
- 23% of all projects **FAIL**

*Source: Research by the Standish Group International Inc., as reported in *Computerworld*, Feb. 17, 2005.*
What constitutes where a project is a success or a failure?

- Has the project satisfied the business requirements of the stakeholders?
- Were the deliverables produced on time and within budget?
- Do the business owners ‘perceive’ the project to be successful?
- Has the project delivered the business value promised at the beginning?

The successful project manager is one who focuses on project risks which in turn arise from uncertainty.
What is a Project Management Office (PMO)?

PMO is the department or group that defines and maintains the standards of process, related to project management, within the organization.

Additional Project Facts:
- 32% fail due to inadequate project management implementation
- 20% fail due to lack of proper communication
- 17% fail due to unfamiliarity and complexity of scope
- 69% fail due to lack and/or improper implementation of project management methodologies

PMO Value Proposition: The PMO is established to manage project management standards in order to minimize risk of project failures.
The PMO balances schedules, budgets, and performance to achieve program objectives and business requirements.

- Coordinate multiple project dependencies
- Proactive issue and risk management
- Reduced project schedule slippage
- Accurate project estimating and planning
- Timely and insightful performance metrics
- Effective resource management
- Delivery within budget
- Maximized consulting investment

Targeted communication between project teams and business units
- Repeatable standards, processes and tools
- Conduct quality assurance reviews
PMI’s PMBOK 9 Knowledge Areas and 5 Base Process Groups

Framework for successful technology initiatives.

The PMI PMBOK is a basic reference for those interested in or already working in the project management profession.
Project Management Processes to Process Groups and Knowledge Areas

1. Project Integration Mgmt
   - Planning
     • Project Plan Development
   - Executing
     • Project Plan Execution
   - Controlling
     • Integrated Change Control

2. Project Scope Mgmt
   - Initiating
     • Initiation
   - Planning
     • Scope Planning
       • Scope Definition
       • Create WBS
   - Controlling
     • Scope Verification
     • Scope Change Control

3. Project Time Mgmt
   - Planning
     • Activity Definition
     • Activity Sequencing
     • Activity Duration Estimating
     • Activity Resource Estimating
     • Schedule Development
   - Controlling
     • Schedule Control
PMBOK 9 Knowledge Areas and sub-areas

**Project Cost Mgmt**
- Planning
  - Resource Planning
  - Cost Estimating
  - Cost Budgeting
- Controlling
  - Cost Control

**Project Quality Mgmt**
- Planning
  - Quality Planning
  - Quality Assurance
- Executing
- Controlling
  - Quality Control

**Project Human Resource Mgmt**
- Planning
  - Organizational Planning
  - Staff Acquisition
  - Team Development
- Executing
PMBOK 9 Knowledge Areas and sub-areas

7. Project Communication Mgmt
   - Planning
     • Communications Planning
     • Executing
     • Information Distribution
   - Executing
     • Information Distribution
   - Controlling
     • Performance Reporting
     • Administrative Closure

8. Project Risk Mgmt
   - Planning
     • Risk Management Planning
     • Risk Identification
     • Qualitative Risk Analysis
     • Quantitative Risk Analysis
     • Risk Response Planning
   - Controlling
     • Risk Monitoring and Control

9. Project Procurement Mgmt
   - Planning
     • Procurement Planning
     • Solicitation Planning
   - Executing
     • Request Sellers Response
     • Select Sellers
     • Contract Administration
   - Closing
     • Contract Closure
Aligning PMBOK to CobIT Standards
CobIT identifies the I/T processes that should exist to ensure that I/T is aligned with and supports the business in an effective manner.

**CobIT I/T Processes within the Four Domains**

- **Monitor & Evaluate**
  - ME1 Monitor and evaluate IT performance
  - ME2 Monitor and evaluate internal control
  - ME3 Ensure regulatory compliance
  - ME4 Provide IT governance

- **Plan and Organize**
  - PO1 Define a strategic IT plan
  - PO2 Define the information architecture
  - PO3 Determine technological direction
  - PO4 Define the IT processes, organization and relationships
  - PO5 Manage the IT investment
  - PO6 Communicate mgmt aims and direction
  - PO7 Manage IT human resources
  - PO8 Manage quality
  - PO9 Assess and manage IT risks
  - PO10 Manage Projects

- **Deliver & Support**
  - DS1 Define and manage service levels
  - DS2 Manage 3rd party services
  - DS3 Manage performance and capacity
  - DS4 Ensure continuous service
  - DS5 Ensure system security
  - DS6 Identify and allocate costs
  - DS7 Educate and train users
  - DS8 Manage service desk and incidents
  - DS9 Manage the configuration
  - DS10 Manage problems
  - DS11 Manage data
  - DS12 Manage the physical environment
  - DS13 Manage operations

- **Acquire & Implement**
  - AI1 Define automated solution
  - AI2 Acquire and maintain application software
  - AI3 Acquire and maintain technology infrastructure
  - AI4 Enable operation and use
  - AI5 Procure IT resources
  - AI6 Manage changes
  - AI7 Install and accredit solutions and changes

**Information**
- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

**IT Resources**
- Application
- Information
- Infrastructure
- People
## Overlap of CobIT and PMBOK

<table>
<thead>
<tr>
<th>CobIT identifies the I/T processes that should exist to ensure that I/T is aligned with and supports the business in an effective manner. CobIT and its supporting publications identify control objectives, techniques and practices commonly required for each processes.</th>
<th>Controls Required for IT Projects</th>
<th>PMBOK identifies the best practice process for project management, together with the knowledge and techniques required for those processes to be effective.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Management Best Practices</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### CobIT

- Identifies the I/T processes
- Supports business

### PMBOK

- Best practice process
- Project management

### Controls Required for IT Projects

- Linkages between CobIT and PMBOK
- Common requirements for IT projects
Aligning CobIT to PMBOK

CobIT IT Processes

- PO1: Define a strategic IT plan
- PO2: Define the information architecture
- PO3: Determine technological direction
- PO4: Define the IT processes, organization and relationships
- PO5: Manage the IT investment
- PO6: Communicate mgmt aims and direction
- PO7: Manage IT human resources
- PO8: Manage quality
- PO9: Assess and manage IT risks
- PO10: Manage Projects

PMBOK Alignment (55 Processes)

- PO1: 1 section of PMBOK
  - Portfolio Mgmt
- PO2: No control objectives are covered by PMBOK
- PO3: No control objectives are covered by PMBOK
- PO4: 3 PMBOK processes partially mapped
  - Project Human Resource Management
- PO5: 4 PMBOK processes partially mapped
  - Project Cost Management
  - Project Procurement Management
- PO6: 2 PMBOK processes partially mapped
  - Communication Management
  - Project Risk Management
- PO7: 5 PMBOK processes partially mapped
  - Human Resource Management
  - Project Time Management
  - Project Cost Management
- PO8: 3 PMBOK processes partially mapped
  - Project Quality Management
- PO9: 7 PMBOK processes partially mapped
  - Project Risk Management
  - Communication Management
- PO10: 31 PMBOK processes are fully mapped
  - Aligned to all 9 PMBOK Knowledge Areas

Reference: IT Governance Institute: Mapping of PMBOK with CobIT 4.0
Aligning CobIT to PMBOK

CobIT IT Processes

- AI1: Define automated solution
- AI2: Acquire and maintain application software
- AI3: Acquire and maintain technology infrastructure
- AI4: Enable operation and use
- AI5: Procure IT resources
- AI6: Manage changes
- AI7: Install and accredit solutions and changes

PMBOK Alignment (28 Processes)

- AI1: 4 PMBOK processes partially mapped
  - Project Integration Management
  - Project Risk Management (Monitoring and Controls)
  - Project Quality Management
- AI2: 8 PMBOK processes partially mapped
  - Project Integration Management
  - Project Risk Management (Monitoring and Controls)
  - Project Quality Management
  - Project Scope Management
- AI3: 1 PMBOK process partially mapped
  - Project Risk Management (Monitoring and Controls)
- AI4: 1 PMBOK process partially mapped
  - Project Risk Management (Monitoring and Controls)
- AI5: 6 PMBOK processes partially mapped
  - Project Procurement Management
- AI6: 1 PMBOK process partially mapped
  - Project Integration Management (Change Control)
- AI7: 7 PMBOK processes partially mapped
  - Project Quality Management
  - Project Integration Management
  - Project Risk Management

Reference: IT Governance Institute: Mapping of PMBOK with CobIT 4.0
Aligning CobIT to PMBOK

CobIT IT Processes

DS1 Define and manage service levels
DS2 Manage 3rd party services
DS3 Manage performance and capacity
DS4 Ensure continuous service
DS5 Ensure system security
DS6 Identify and allocate costs
DS7 Educate and train users
DS8 Manage service desk and incidents
DS9 Manage the configuration
DS10 Manage problems
DS11 Manage data
DS12 Manage the physical environment
DS13 Manage operations

PMBOK Alignment (14 Processes)

DS1 - 1 PMBOK process partially mapped
Project Integration Management (service agreements)

DS2 - 4 PMBOK processes mapped
Project Procurement Management

DS3 - No control objectives are covered by PMBOK

DS4 - 1 PMBOK process partially mapped
Project Integration Management (IT Continuity)

DS5 - 1 PMBOK process partially mapped
Project Integration Management (IT Security Plan)

DS6 - 1 PMBOK process partially mapped
Project Cost Management

DS7 - 1 PMBOK process partially mapped
Project Human Resource Management (Team Development)

DS8 - No control objectives are covered by PMBOK

DS9 - 2 PMBOK process partially mapped
Project Scope Management
Project Risk Management

DS10 - 1 PMBOK process partially mapped
Project Time / Scope Management (Change Control)

DS11 - 1 PMBOK process partially mapped
Project Scope Management

DS12 - 1 PMBOK process partially mapped
Project Time / Scope Management (Change Control)

DS13 - No control objectives are covered by PMBOK

Reference: IT Governance Institute: Mapping of PMBOK with CobIT 4.0
Aligning CobIT to PMBOK

CobIT IT Processes

- ME1: Monitor and evaluate IT performance
- ME2: Monitor and evaluate internal control
- ME3: Ensure regulatory compliance
- ME4: Provide IT governance

PMBOK Alignment (8 Processes)

- ME1 - 8 PMBOK processes partially mapped
- Project Communication Management (Performance Reporting)
- Project Risk Management
- ME2 - There is no mapping between PMBOK and COBIT.
- ME3 - There is no mapping between PMBOK and COBIT.
- ME4 - There is no mapping between PMBOK and COBIT.

Reference: IT Governance Institute: Mapping of PMBOK with CobIT 4.0
Project Management Audit Recommendations
Use a structured approach when reviewing project management controls.

1. **Interviews**
   Conduct interviews with all levels to ensure the project business need, requirements and scope is properly aligned from initial concept to actual execution. Includes Executive Management, Steering Committee, Project Team, Project Manager, and End-Users.

2. **Governance Structure**
   Review the organizational and governance structure of the project. Is the project properly represented for its review and execution? Have proper roles and responsibilities been identified and communicated?

3. **Documentation Review**
   Review project documentation to ensure the initial design of project documentation and controls are actually being executed and reviewed.

4. **Risks Assessment**
   Be sure that controls are designed into the system. Focus on risks that have the highest impact and likelihood to occur.

5. **Observations**
   Captured preliminary observations related to the current state of the project. Confirm your findings prior to reporting.
Beginning with a review of the Governance process is important as it sets the foundation for how the project is managed and viewed by the organization.

**Project Governance Key Components:**

- Executive management commitment and support
- Active formal steering committee and project sponsor
- Business process leader representation on the steering committee
- Clear project charter that identifies scope and objectives
- A Program Management Office to manage the project
The Governance assessment plan should include review of the governance structure (roles & responsibilities), the program charter (requirements), business case (financials and timeline) and project plan.

<table>
<thead>
<tr>
<th>Activities</th>
<th>Reviewed Deliverables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review Governance Structure</td>
<td>Roles &amp; Responsibilities</td>
</tr>
<tr>
<td>Review Governance Charter</td>
<td>Charter / Requirements / Playbook</td>
</tr>
<tr>
<td>Review Business Case</td>
<td>Business Case with ROI</td>
</tr>
<tr>
<td>Review Project Plan</td>
<td>Master Project Plan</td>
</tr>
<tr>
<td>Review Risk Plan</td>
<td>Risk and Issue Response Plan</td>
</tr>
<tr>
<td>Attend Governance steering committee meetings</td>
<td>Meeting Notes &amp; Action Items</td>
</tr>
<tr>
<td>Monitor progress against plan</td>
<td>Periodic Team and Steering Committee Meetings</td>
</tr>
<tr>
<td>Post implementation review</td>
<td>QA Assessments and Lessons Learned</td>
</tr>
</tbody>
</table>
Clearly defined and agreed upon roles and responsibilities ensure accountability and contribute to an effective and efficient project.

<table>
<thead>
<tr>
<th>Group</th>
<th>General Roles and Responsibilities</th>
</tr>
</thead>
</table>
| Program Steering Committee    | • Holds project decision making responsibility  
                                  • Sets resources and priorities  
                                  • Handles issue resolution and barrier removal  
                                  • Participates in bi-weekly updates and key milestone meetings/takes follow up action |
| Executive Sponsor             | • Champions project importance  
                                  • Escalates Issues                                                                 |
| Risk Management               | • Monitor and manage program and project risks                                                       |
| Program Management Office     | • Builds and manages detailed project plan  
                                  • Coordinates with all stakeholders  
                                  • Facilitates resource assignment  
                                  • Develops and delivers status reports/communications                                           |
| Business Process Redesign Teams | • Detail and benchmark current business processes and related information flows  
                                  • Develop new business processes  
                                  • Report on status and/or issues                                                              |
Clearly defined and agreed upon roles and responsibilities ensure accountability and contribute to an effective and efficient project.

(continued)

<table>
<thead>
<tr>
<th>Group</th>
<th>General Roles and Responsibilities</th>
</tr>
</thead>
</table>
| Technology Implementation Teams       | • Identify network, hardware and operating system requirements  
• Install and configure hardware infrastructure, network and system  
• Develop, install and setup applications  
• Setup Development, Test and Production Environment  
• Migrate environments from Development, Test and to Production  
• Report on status and/or issues                                                                 |
| Applications Configuration and Implementation Teams | • Develop system applications (modules) based on business process and requirements  
• Install and configure application databases  
• Provide application expertise and insight/knowledge sharing  
• Migrate data from existing applications                                           |
| Systems Interfaces Team               | • Design, develop and implement interfaces                                                                                                                                             |
| Security and Controls Team            | • Identify and design business and technology controls                                                                                                                                 |
| Quality and Change Control Team       | • Reviews Quality Assessment documentation  
• Review and approve project changes  
• Work with Executive Sponsor to ensure project quality                                                                 |
Project Management Execution

- Has the team identified critical path tasks?
- Have project stakeholders completed a review of key deliverables and milestones?
- Is the project being managed from the plan?
- Is a structured development methodology been utilized?
- Is progress tracked against milestones?
- Are issues and changes being identified and tracked to resolution?
- Are estimates to complete realistic?
Assessment of the "Project Management" process should focus on the project plan, key deliverables, milestones and timeline.

Project Plan Key Components:

- A detailed project plan should be current, monitored and have critical and key milestones identified
- Requirements for each major process area should be documented, reviewed and approved by the business organization
- Take into account the “Triple Constraint” (Scope, Cost, Time)
- Plan should take into account resources day-to-day activities outside the project
- A phased roll out strategy is recommended
- A contingency plan should be included in the plan
The initial step in the system development life cycle assessment focuses on how requirements are defined and how changes are managed.

**Requirements and Change Management**

- Are business process flows and key business requirements documented, referenced, and validated during the software development cycle?
- Are the appropriate controls built into the system to meet financial statement control objectives?
- Are process flows available to document how data moves throughout the system?
- Are changes to the project being managed?
- Are controls in place to prevent scope creep?
- Are users involved in acceptance testing?
Business requirements are the foundation for all testing. The review should ensure that business functionality, conversion and interfaces have been tested rigorously and that the business organizations have signed-off before the new system is moved to production.

Testing Key Components

- Align initial requirements to the testing plan to confirm all system functionality is properly tested
- Test script development should be reviewed and approved by the business
- Test scripts should include conversion and interface testing, reconciliation and user sign-off
Be sure that application controls are designed into the system. Use a risk based approach to design and implementation controls related to application and related systems and business processes. Focus on risks that have the highest impact and likelihood to occur.

The risk approach should address the following key risk areas.

- Application Security Risks
- Financial Control Risks
- Application Control Risks
- General Computer Control Risks (Infrastructure)
- Data Conversion Risks
- Interface Risks
Be sure that Security and Controls are designed into the system. Security and Controls should focus on aligning existing controls and implementing new controls for new solution implementations.
Question ?