Internal Audit’s Role in the Vendor and System Selection Process

October 5, 2015
With you today

Brett Luis, Practice Leader
IT Audit and Advisory
CNM LLP
About CNM

• Founded in 2003, CNM is recognized as one of the premier technical accounting and internal controls consulting firms in Southern California.

• Our team has deep information technology (IT), accounting and internal control skills given our experience assisting clients address technical matters and in implementing the provisions of Sarbanes Oxley Section 404 and COSO 2013.

• Approximately 85% of our clients are acquired through direct referrals from the Big 4. We work closely with EY, PwC and DT on multiple engagements.

• We only hire experienced professionals that meet our demanding hiring criteria.
Hypothesis

Whether in an assurance or consultative role internal audit has a vital role to play in the system selection and implementation process

- Large scale system selection and implementation projects are too infrequent, complex and varied to enable the development of a robust in-house competency
- Internal auditors possess a broad perspective
- Internal auditors commitment to continuous learning, integrity and structured communications are just some of the skills that align well with the selection process
- Knowledge of compliance requirements is limited to a few key departments and resources
1120 – Individual Objectivity Internal auditors must have an impartial, unbiased attitude and avoid any conflict of interest.

1130.A1 – Internal auditors must refrain from assessing specific operations for which they were previously responsible. Objectivity is presumed to be impaired if an internal auditor provides assurance services for an activity for which the internal auditor had responsibility within the previous year.

1210.C1 – The chief audit executive must decline the consulting engagement or obtain competent advice and assistance if the internal auditors lack the knowledge, skills, or other competencies needed to perform all or part of the engagement.

2210.C1 – Consulting engagement objectives must address governance, risk management, and control processes to the extent agreed upon with the client.

2210.C2 – Consulting engagement objectives must be consistent with the organization's values, strategies, and objectives.

2010.C1 – The chief audit executive should consider accepting proposed consulting engagements based on the engagement’s potential to improve management of risks, add value, and improve the organization’s operations. Accepted engagements must be included in the plan.

2440.C2 – During consulting engagements, governance, risk management, and control issues may be identified. Whenever these issues are significant to the organization, they must be communicated to senior management and the board.
Information Technology Trends
3rd Platform for IT — and Business — Innovation and Growth

Source: IDC, 2014
CIO Agenda

The predictions from the International Data Corporation (IDC) Future Scape for the CIO Agenda:

• By 2017, 80% of the CIO’s time will be focused on analytics, cybersecurity and creating new revenue streams through digital services.

• By 2016, 65% of global competitive strategies will require real-time 3rdPlatform IT-as-a–Service (ITaaS).

• By 2016, security will be a top 3 business priority for 70% of CEOs of global enterprises.

• By 2015, 60% of CIOs will use DevOps as their primary tool to address the speed and sprawl of mobile, cloud, and open source applications.

• By 2016, 80% of CIOs will deliver a new architectural framework that enables innovation and improved business decision-making.
CIO Agenda, continued

• By 2020, 60% of CIOs in global organizations will be supplanted by the Chief Digital Officer (CDO) for the delivery of IT-enabled products and digital services.

• By 2016, 80% of CIOs will accelerate 3rd Platform migration to counter premature obsolescence of current IT assets.

• By 2018, 30% of CIOs of global organizations will have rolled out a pan-enterprise data and analytics strategy.

• By 2017, 35% of vendor sourcing relationships around 3rd Platform technologies will fail, causing CIOs to roll out new sourcing processes.

• By 2018, 50% of CIOs will relinquish IT's traditional mode of technology control in favor of an open standards-based framework.
## Cloud Computing Landscape

<table>
<thead>
<tr>
<th>Applications</th>
<th>Blackline Systems</th>
<th>Netsuite</th>
<th>Zoho</th>
<th>Soxhub</th>
<th>Google Docs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computing</td>
<td>Amazon Web Services</td>
<td>Rackspace</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Development platform</td>
<td>Windows Azure</td>
<td>Salesforce</td>
<td>Force.com</td>
<td>Google</td>
<td>GitHub</td>
</tr>
</tbody>
</table>
Cloud and Agile Era

• According to Forrester Research, the public cloud market is estimated to reach $191 billion by 2020, a significant increase from 2013’s $58 billion

• Gartner, Inc. named cloud as one of the top 10 strategic technology trends for 2015

• Gartner also named Software-Defined Applications and Infrastructure and Web-Scale IT in their top 10 strategic technology trends for 2015

• IT organizations are experiencing significant changes in the nature of the services and solutions they procure

• Many startup organization are operating with little or no internal IT
Cloud and Agile Era

• IT purchasing decision are being made outside of IT
• Compliance requirements have increased significantly and are often overlooked during the requirements gathering and selection process
• Proliferation of cloud based almost point solutions (“there’s an app for that”)
• Interoperability, connectivity and confidentiality concerns have taken the place of flexibility, scalability and availability concerns
The Tipping Point for Change

• Most organizations do not have a structured process for determining when to upgrade or change their IT systems

• Organizations too often have a “make do with” mentality when it comes to large scale IT systems

• Total Cost of Ownership and lack of information to support sound decision making criteria delay new technology adoption

• IT is often not viewed as a strategic enabler or is poorly tied into the organizations overall strategy
Drivers for Changing Systems

Internal Audit may play an active role in identifying key drivers for system change, key drivers include:

- Strategic Alignment
- Confidentiality
- Integrity
- Availability
- Performance
- Manual Workarounds
- Compliance
- Information
- Integration
- Mobility
- Scalability
- Cost
PIECES Framework

PIECES framework can be used for assessing or determining the ongoing feasibility of a system:

- **Performance**, does the system provide adequate throughput and response time?
- **Information**, does the system provide end-user and managers with timely, pertinent, accurate, and useful formatted information?
- **Economy**, does the system offer adequate service level and capacity to reduce/manage cost?
- **Control**, does the system offer adequate controls to protect against fraud and embezzlement and to guarantee the accuracy and security of data and information?
- **Efficiency**, does the system make maximum use of available resources including people, time, flow of forms, minimum processing delays, and the like?
- **Services**, does the system provide desirable and reliable service to those who need it? Is the system flexible and expandable?
Selection Process
Traditional Systems Life Cycle Overview

Continuous Improvement
- Synchronize evolving business needs with application functionality
- Change management
- Vendor management

Implementation
- Convert legacy data
- Build/Configure functionality
- Develop interfaces
- Develop test plans
- Develop implementation strategy
- Develop archival strategy
- Go-Live

Vendor/Solution Selection
- Create vendor selection criteria
- Create vendor long/short list
- Create & distribute RFI/RFP
- Create vendor evaluation framework
- Select vendor

Approach
- Project planning
- Identify drivers
- Identify constraints
- Develop business case

Preparation
- Document current state
- Develop future state requirements
- Perform gap analysis

CNM
All Rights Reserved
Selection Process

CNM’s Selection Assistance Approach

Project Initiation
- Gain consensus on strategy, objectives and vision
- Current state assessment:
  - People
  - Process
  - Technology
- High level business needs
- Business Case (Total Value/TCO/ROI)

Requirements/Vision Definition
- Define system requirements
  - Functional
  - Technical
  - Compliance
- Identify “must have” vs. “nice to have” requirements
- RFI if needed
- Define vendor evaluation framework/seletion criteria
- Develop long list

Solution Evaluation
- Identify potential solutions (short list) and any additional requirements
- RFP if needed
- Conduct scripted vendor demos (using your data and scenarios)
- Evaluate technical requirements and deployment strategy alternatives
- Negotiate and contract
- Ongoing Vendor Management/Governance

Selection and Contracting
- Evaluate solutions/vendors for best fit against key criteria
- Evaluate technical requirements and deployment strategy alternatives
- Negotiate and contract
- Ongoing Vendor Management/Governance
Business Case

• IT organization’s are typically not well equipped to estimate IT costs and benefits

• A business case author should be:
  • Thorough - (research possible impacts, cost/benefits),
  • Structured and precise - (outline the clear cause and effect leading to each cost/benefit)
  • Objective - (unbiased)
  • Systematic - (summarize data and rely on sound financial models)
Business Case

Approach the business case by focusing on the following questions:

1. Why do we need to change?
   - Market changes
   - Industry reaction
   - Regulatory compliance

2. Where are we today? (AS-IS)

3. Where do we need to be? (TO-BE)

4. What are the challenges?

5. How do we get to where we need to be?
   - Business drivers
   - How does the solution enable us to get there
   - How do leaders realize the benefits

Potential Benefits

What are the potential benefits?
Sample Business Case Outline

- Introduction and Overview
  - Title
  - Purpose/Introduction
  - Disclaimer
  - Executive Summary

- Assumptions and Methods
  - Financial Metrics
  - Assumptions
  - Scope/Boundaries
  - Scenario Analysis
  - Cost Model

- Business Impacts
  - Financial Model and Assumptions
  - Analysis of financial and non financial results

- Sensitivity, Risks, Contingency and Dependency Analysis

- Conclusions and Recommendations
Example Selection Categories

Solution evaluation based on four categories:

- **Functionality**: How well do the packages meet the company’s requirements?
- **Vendor Viability**: How likely is it that the vendor will be there when we need them?
- **Technology**: How current is the technical design of the software?
- **Cost/Benefit**: What are the comparative initial and ongoing costs/benefits?
Example Selection Criteria

Use structured decomposition techniques to help ensure that the decision takes into account critical criteria in each of the defined categories.

- **Functionality**
  - Plan Production
  - Buy Materials
  - Produce Product
  - Move and Warehouse Materials
  - Fulfill Orders
  - Administer Business/Financials

- **Vendor Viability**
  - Market Position
  - Financials Stability
  - Service & Support
  - Vision

- **Technology**
  - Platforms
  - Client/Server
  - Tools
  - Ease of Interface

- **Cost**
  - Software License
  - Implementation Services
  - Hardware
  - On-going maintenance costs
# Example Selection Criteria

<table>
<thead>
<tr>
<th>Software Evaluation Criteria</th>
<th>Description</th>
<th>Weight (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Functional and Technical Assessment Factors</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Functionality</td>
<td>Robustness of vanilla solution in comparison to best of creed solutions; Degree of customization needs that can be met; Availability of workarounds that can be used to meet business needs</td>
<td>30%</td>
</tr>
<tr>
<td>Usability</td>
<td>Ease of use, intuitiveness, number of clicks, user interface appeal, portal</td>
<td>15%</td>
</tr>
<tr>
<td>Technical Alignment</td>
<td>Architectural openness and extensibility, performance, scalability, reliability, availability, security and compliance</td>
<td>20%</td>
</tr>
<tr>
<td>Vendor Background</td>
<td>Company history, strategic direction, stability, support, risk impact</td>
<td>5%</td>
</tr>
<tr>
<td>Total Cost of Ownership</td>
<td>Hardware costs, software license, implementation costs, and on-going support costs</td>
<td>30%</td>
</tr>
</tbody>
</table>
Selection Principles

• All RFP information must be provided to all respondents, including responses to all questions
• Selection criteria must be clearly identified and communicated to the respondents
• Weighting of selection criteria must be identified and can be communicated to all respondents
• Selection criteria and weighting must be strictly followed by the Selection Committee
• Transparency and fairness must be maintained throughout the process
Example RFP Outline

• Introduction
  • Purpose
  • RFP Organization
  • Background

• Current State
  • Current IT-system(s)
  • Current Processes and Modules
  • Project Objectives
  • Business Drivers

• Scope of work
  • Functional Requirements
  • Non-Functional Requirements
Example RFP Functional Requirements

• Processes
  • Process model
  • Process specification

• Data model
  • Data model
  • Data specification

• Use Cases
  • Use Case model
  • Use Case specification
Example RFP Non Functional Requirements

- System
- Data Migration and Conversion
- System Interface/Integration
- Technical Architecture
- Hardware
- Development, Test and Staging Environment
- Security
- Monitoring & Management Requirements

- Performance and Scalability Requirements
- Implementation Requirements
- Maintenance and Support Requirements
- Change Enablement and Training Requirements
- Operations Requirements
- Quality Assurance and Acceptance Requirements
- Assurance/Audit Requirements
Assurance
Project Assurance

- Selection Process
- IT Application and Information Controls (Reports etc.)
- IT General Controls
- Data Integrity and Interfaces
- Functional, Technical and Organizational Preparedness
- Project management and Governance
SOX Implications/Recommendations

1. Follow a structured implementation approach
2. Ensure process level risks and controls are defined and incorporated as key requirements and tested
3. Ensure interface controls, role based access control and security configurations are defined and tested
4. Ensure you can evidence reconciliation of source system to target system data
5. Ensure management reviews key configuration and master data setups
6. Document and test IT general controls incl. program development
7. Baseline application controls and reports
8. Establish ongoing vendor oversight controls
Q&A
www.cnmllp.com

Brett Luis
21051 Warner Center Lane, Suite 140
Woodland Hills, CA 91367
Tel. 858.401.2526
bluis@cnmllp.com

Building RELATIONSHIPS that last.