IT Audit Process

Prof. Mike Romeu

September 23, 2015
Agenda

• Vendor Management and ‘The Cloud’
  • MIS 5202 - Governance and Management of IT
  • Cloud Main Structures
• Impact of Laws and Regulations on IT Audit Planning
• AWA Case
  • Due date extended until Saturday September 26 at 12:00 Midnight.
  • Work submitted at 12:01 or later will be considered late.
Vendor Management

• **Vendor** – A person or business entity that sells **goods** and/or **services** to another person or business entity.

<table>
<thead>
<tr>
<th><strong>Goods</strong></th>
<th><strong>Services</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Office Supplies</td>
<td>Programming and Integration</td>
</tr>
<tr>
<td>Office furnishings</td>
<td>Quality Assurance and Control</td>
</tr>
<tr>
<td>Computer hardware and software</td>
<td>Implementation</td>
</tr>
<tr>
<td>Computer peripherals</td>
<td></td>
</tr>
<tr>
<td>Network Equipment</td>
<td></td>
</tr>
<tr>
<td>Real Estate (buildings and offices)</td>
<td>Project Management</td>
</tr>
<tr>
<td></td>
<td>Cloud (IaaS, PaaS, SaaS)</td>
</tr>
</tbody>
</table>
Vendor Management

- Vendor – A person or business entity that sells **goods** and/or **services** to another person or business entity.

<table>
<thead>
<tr>
<th>Goods</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office Supplies</td>
<td>Programming and Integration</td>
</tr>
<tr>
<td>Office furnishings</td>
<td>Quality Assurance and Control</td>
</tr>
<tr>
<td>Computer hardware and software</td>
<td>Implementation</td>
</tr>
<tr>
<td>Computer peripherals</td>
<td></td>
</tr>
<tr>
<td>Network Equipment</td>
<td></td>
</tr>
<tr>
<td>Real Estate (buildings and offices)</td>
<td>Project Management</td>
</tr>
<tr>
<td></td>
<td>Cloud (IaaS, PaaS, SaaS)</td>
</tr>
</tbody>
</table>
Vendor Management

• Reasons for outsourcing IT services
  1. Focus on Core Competencies or Initiatives
     • AWA – Transportation
     • Vendor – IT Operations, infrastructure management, software development and maintenance (India)
  2. Pressure on profit margins and increasing competition
     • Profit Margin = Sales Price – Cost of Goods or Service
     • AWA is facing both: pressure on profit margin and a highly competitive industry. i.e. pressures to lower costs
  3. Organizational and Structural Flexibility
     • AWA Organizational: IT Footprint small or non-existent
     • AWA Structural: Choice of Vendors at the right price.
Infrastructure, Platform and Software as a Service (IaaS, PaaS, SaaS)

- **In-House**
  - Software
  - Data
  - Runtime
  - Middleware
  - O/S
  - Virtualization
  - Servers
  - Storage
  - Networks

- **IaaS**
  - Software
  - Data
  - Runtime
  - Middleware
  - O/S
  - Virtualization
  - Servers
  - Storage
  - Networks

- **PaaS**
  - Software
  - Data
  - Runtime
  - Middleware
  - O/S
  - Virtualization
  - Servers
  - Storage
  - Networks

- **SaaS**
  - Software
  - Data
  - Runtime
  - Middleware
  - O/S
  - Virtualization
  - Servers
  - Storage
  - Networks

- **Managed by Vendor**
  - O/S
  - Virtualization
  - Servers
  - Storage
  - Networks

- **You Manage**
  - Software
  - Data
  - Runtime
  - Middleware
  - O/S
  - Virtualization
  - Servers
  - Storage
  - Networks
Infrastructure, Platform and Software as a Service (IaaS, PaaS, SaaS)

- **In-House**
  - You Manage
  - Software
  - Data
  - Runtime
  - Middleware
  - O/S
  - Virtualization
  - Servers
  - Storage
  - Networks

- **IaaS**
  - You Manage
  - Software
  - Data
  - Runtime
  - Middleware
  - O/S
  - Virtualization
  - Servers
  - Storage
  - Networks

- **PaaS**
  - You Manage
  - Software
  - Data
  - Runtime
  - Middleware
  - O/S
  - Virtualization
  - Servers
  - Storage
  - Networks

- **SaaS**
  - Managed by Vendor
  - Software
  - Data
  - Runtime
  - Middleware
  - O/S
  - Virtualization
  - Servers
  - Storage
  - Networks

- **Managed by Vendor**
  - You Manage
  - Virtualization
  - Servers
  - Storage
  - Networks
<table>
<thead>
<tr>
<th>In-House</th>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP</td>
<td>Amazon Web Services</td>
<td>Force.com and Heroku</td>
<td>WordPress</td>
</tr>
<tr>
<td>Oracle ERP</td>
<td></td>
<td>Windows Azure</td>
<td>Google Apps</td>
</tr>
<tr>
<td>SYSPRO</td>
<td></td>
<td>IBM Smart Cloud</td>
<td>Square</td>
</tr>
<tr>
<td>AICS</td>
<td></td>
<td></td>
<td>LinkedIn</td>
</tr>
<tr>
<td>Freight Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Airfare Price Sensitivity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scheduling</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintenance</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Vendor Management – Impact on Customer Satisfaction

• Customer Satisfaction is Key!

• The right information must be available to the right customer when they need it.

• Two main areas of concern when considering outsourcing
  • Service Level Agreements (SLA)
  • Contracts
Service Level Agreements

**Definition**
- The SLA describes the services in nontechnical terms, from the viewpoint of the customer.

**Service Level Management**
- The process of defining, agreeing upon, documenting and managing levels of service that are required and cost justified.

**Aim**
- To maintain and improve customer satisfaction and to improve the service delivered to the customer.
Process for Governance of Enterprise IT
Evaluate, Direct and Monitor

- **EDM01** Ensure Governance Framework Setting and Maintenance
- **EDM02** Ensure Benefits Delivery
- **EDM03** Ensure Risk Optimisation
- **EDM04** Ensure Resource Optimisation
- **EDM05** Ensure Stakeholder Transparency

**Align, Plan and Organize**
- **AP001** Manage the IT management Framework
- **AP002** Manage Strategy
- **AP003** Manage Enterprise Architecture
- **AP004** Manage Innovation
- **AP005** Manage Innovation
- **AP006** Manage Budget and Costs
- **AP007** Manage Human Resources
- **AP008** Manage Relationships
- **AP009** Manage Service Agreements
- **AP010** Manage Suppliers
- **AP011** Manage Innovation
- **AP012** Manage Risk
- **AP013** Manage Security

**Build, Acquire and Implement**
- **BAI01** Manage Programmes and Projects
- **BAI02** Manage Requirements Definition
- **BAI03** Manage Solutions Identification and Build
- **BAI04** Manage Availability and Capacity
- **BAI05** Manage Organisational Change Enablement
- **BAI06** Manage Changes
- **BAI07** Manage Change Acceptance and Transitioning
- **BAI08** Manage Knowledge
- **BAI09** Manage Assets
- **BAI10** Manage Configurations

**Deliver, Service and Support**
- **DSS01** Manage Operations
- **DSS02** Manage Service Requests and Incidents
- **DSS03** Manage Problems
- **DSS04** Manage Continuity
- **DSS05** Manage Business Process Controls
- **DSS06** Manage Security Services
- **DSS07** Manage Change Acceptance and Transitioning

**Monitor, Evaluate and Assess**
- **MEA01** Monitor, Evaluate and Assess Performance and Conformance
- **MEA02** Monitor, Evaluate and Assess the System of Internal Controls
- **MEA03** Monitor, Evaluate and Assess Compliance With External Requirements
## Service Level Agreements

<table>
<thead>
<tr>
<th>Process Description</th>
<th>APO09 Manage Service Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Align IT-enabled services and service levels with enterprise needs and expectations, including identification, specification, design, publishing, agreement, and monitoring of IT services, service levels and performance indicators.</td>
<td></td>
</tr>
</tbody>
</table>

| Purpose Statement | Ensure that IT services and service levels meet current and future enterprise needs. |

<table>
<thead>
<tr>
<th>IT goals</th>
<th>Delivery of IT services in line with Business requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Available and useful information for decision-making</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Activities</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>* Analyse requirements for new or changed service agreements received from business relationship management to ensure that the requirements can be matched. Consider aspects such as service times, availability, performance, capacity, security, continuity, compliance and regulatory issues, usability, and demand constraints.</td>
<td></td>
</tr>
<tr>
<td>* Draft customer service agreements based on the services, service packages and service level options in the relevant service catalogues.</td>
<td></td>
</tr>
<tr>
<td>* Determine, agree on and document internal operational agreements to underpin the customer service agreements, if applicable.</td>
<td></td>
</tr>
<tr>
<td>* Liaise with supplier management to ensure that appropriate commercial contracts with external service providers underpin the customer service agreements, if applicable.</td>
<td></td>
</tr>
<tr>
<td>* Finalise customer service agreements with business relationship management.</td>
<td></td>
</tr>
</tbody>
</table>
Process for Governance of Enterprise IT
Evaluate, Direct and Monitor

Align, Plan and Organize
- AP001 Manage the IT management Framework
- AP002 Manage Strategy
- AP003 Manage Enterprise Architecture
- AP004 Manage Innovation
- AP005 Manage Innovation
- AP006 Manage Budget and Costs
- AP007 Manage Human Resources
- AP008 Manage Relationships
- AP009 Manage Service Agreements
- AP010 Manage Suppliers
- AP011 Manage Innovation
- AP012 Manage Risk
- AP013 Manage Security
- AP003 Manage Enterprise Architecture
- AP004 Manage Innovation
- AP005 Manage Innovation
- AP006 Manage Budget and Costs
- AP007 Manage Human Resources
- AP008 Manage Relationships
- AP009 Manage Service Agreements
- AP010 Manage Suppliers
- AP011 Manage Innovation
- AP012 Manage Risk
- AP013 Manage Security

Build, Acquire and Implement
- BAI01 Manage Programmes and Projects
- BAI02 Manage Requirements Definition
- BAI03 Manage Solutions Identification and Build
- BAI04 Manage Availability and Capacity
- BAI05 Manage Organisational Change Enablement
- BAI06 Manage Change Acceptance and Transitioning
- BAI07 Manage Change Acceptance and Transitioning
- BAI08 Manage Knowledge
- BAI09 Manage Assets
- BAI10 Manage Configurations

Deliver, Service and Support
- DSS01 Manage Operations
- DSS02 Manage Service Requests and Incidents
- DSS03 Manage Problems
- DSS04 Manage Continuity
- DSS05 Manage Security Services
- DSS06 Manage Business Process Controls
- DSS07 Manage Business Process Controls

Processes for Management of Enterprise IT

Monitor, Evaluate and Assess
- MEA01 Monitor, Evaluate and Assess Performance and Conformance
- MEA02 Monitor, Evaluate and Assess the System of Internal Controls
- MEA03 Monitor, Evaluate and Assess Compliance With External Requirements
Good Place For A Break!
Laws, Regulations and Audit Planning
Laws, Regulations and Audit Planning

• Laws and Regulations Placed on Audit or IS Audit Function
  • Auditing Standards
  • Laws
  • Regulations
  • Contractual Agreements
  • Data Management
  • Reporting

• Laws and Regulations Placed on Auditee
Laws, Regulations and Audit Planning

• A review of applicable laws and regulations will impact the scope of the audit.

1. Review and Document legal and regulatory requirements for:
   • Electronic data, electronic signatures, personal information, copyright, …
   • Computer system practices and controls
   • Storage and protection of computers programs and data
   • Organizational structures and activities (SOD)
   • IS Audit

2. Assess whether Management and IT have incorporated legal and regulatory requirements by reviewing policies, procedures and standard practices

3. Determine adherence to established policies, procedures and standard practices.
## Laws, Regulations and Audit Planning

<table>
<thead>
<tr>
<th>Law/Regulation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sarbanes-Oxley Act of 2002 (SOX)</strong></td>
<td>SOX enacts strong regulations regarding controls for financial risks. Because many of these controls are increasingly automated SOX requires the inspection of IT General Controls such as Program Change Management, SDLC, Business Continuity, and Security.</td>
</tr>
<tr>
<td><strong>Payment Card Industry Data Security Standard (PCI DSS)</strong></td>
<td>The Payment Card Industry Security Standard Council established a standard of controls around cardholder data to reduce credit card fraud via its exposure.</td>
</tr>
<tr>
<td><strong>Health Insurance Portability and Accountability Act (HIPAA)</strong></td>
<td>Established in 1996 the primary goal of the law is to make it easier for people to keep health insurance, protect the confidentiality and security of healthcare information and help the healthcare industry control administrative costs.</td>
</tr>
</tbody>
</table>
Laws, Regulations and Audit Planning

• You can outsource the service but not the compliance accountability
• In an outsourcing situation expectations must be clear, unambiguous and documented.
• Vendors that provide services that are affected by laws and regulations must provide assurance of compliance.
IT Assurance and COBIT® 5 - Enablers

1. Principles, Policies and Frameworks

2. Processes

3. Organizational Structures

4. Culture, Ethics and Behaviour

5. Information

6. Services, Infrastructure and Applications

7. People, Skills and Competencies

Resources