IT Governance Decisions & Archetypes Week 3
IT control objectives are useful to IS auditors, as they provide the basis for understanding the:

- **A** - desired result or purpose of implementing specific control procedures.
- **B** - best IT security control practices relevant to a specific entity.
- **C** - techniques for securing information.
- **D** - security policy.
When reviewing an organization's strategic IT plan an IS auditor should expect to find:

- A - an assessment of the fit of the organization's application portfolio with business objectives.
- B - actions to reduce hardware procurement cost.
- C - a listing of approved suppliers of IT contract resources.
- D - a description of the technical architecture for the organization's network perimeter security.
Which of the following IT governance best practices improves strategic alignment?

- A - Supplier and partner risks are managed.
- B - A knowledge base on customers, products, markets and processes is in place.
- C - A structure is provided that facilitates the creation and sharing of business information.
- D - Top management mediate between the imperatives of business and technology.
Responsibility for the governance of IT should rest with the:

A - IT strategy committee.
B - chief information officer (CIO).
C - audit committee.
D - board of directors.
COBIT 5

Source: COBIT® 5, figure 2. © 2012 ISACA® All rights reserved.
Figure 10—COBIT 5 Process Reference Model

Processes 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 Organise
- AP001 Manage the IT Management Framework
- AP002 Manage Strategy
- AP003 Manage Enterprise Architecture
- AP004 Manage Innovation
- AP005 Manage Portfolio
- AP006 Manage Budget and Costs
- AP007 Manage Human Resources
- AP008 Manage Relationships
- AP009 Manage Service Agreements
- AP010 Manage Suppliers
- AP011 Manage Quality
- AP012 Manage Risk
- AP013 Manage Security

Build, Acquire and Implement
- BA001 Manage Programmes and Projects
- BA002 Manage Requirements Definition
- BA003 Manage Solutions Identification and Build
- BA004 Manage Availability and Capacity
- BA005 Manage Organisational Change Enablement
- BA006 Manage Changes
- BA007 Manage Change Acceptance and Transitioning
- BA008 Manage Knowledge
- BA009 Manage Assets
- BA010 Manage Configuration

Deliver, Service and Support
- DS001 Manage Operations
- DS002 Manage Service Requests and Incidents
- DS003 Manage Problems
- DS004 Manage Continuity
- DS005 Manage Security Services
- DS006 Manage Business Process Controls

Monitor, Evaluate and Assess
- MEA01 Monitor, Evaluate and Assess Performance and Conformance
- MEA02 Monitor, Evaluate and Assess the System of Internal Control
- MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

Processes for Management of Enterprise IT
<table>
<thead>
<tr>
<th>Management Practice</th>
<th>From</th>
<th>Description</th>
<th>Outputs</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AP001.08 Maintain compliance with policies and procedures.</strong></td>
<td>DSS01.04</td>
<td>Environmental policies</td>
<td>Non-compliance remedial actions</td>
<td>MEA01.05</td>
</tr>
<tr>
<td>Put in place procedures to maintain compliance with and performance measurement</td>
<td>MEA03.02</td>
<td>Updated policies, principles,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>of policies and other enablers of the control framework, and enforce the</td>
<td></td>
<td>procedures and standards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>consequences of non-compliance or inadequate performance. Track trends and</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>performance and consider these in the future design and improvement of the</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>control framework.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Activities**

1. Track compliance with policies and procedures.

2. Analyse non-compliance and take appropriate action (this could include changing requirements).

3. Integrate performance and compliance into individual staff members’ performance objectives.

4. Regularly assess the performance of the framework’s enablers and take appropriate action.

5. Analyse trends in performance and compliance and take appropriate action.

**AP001 Related Guidance**

<table>
<thead>
<tr>
<th>Related Standard</th>
<th>Detailed Reference</th>
</tr>
</thead>
</table>
| ISO/IEC 20000     | • 3.1 Management responsibility  
                  | • 4.4 Continual improvement |
| ITIL V3 2011     | 25. The Seven-step Improvement Process |
IT Governance Decisions & Archetypes

Team 1
Team 1

• “Six IT Decisions You IT People Shouldn’t Make”

• “IT Governance Archetypes for Allocating Decision Rights”

IT Governance
Rich Flanagan
IT Governance Decisions & Archetypes

• You won’t see Weill & Ross in an ISACA exam
• Goal is for you to understand:
  – There are certain decisions all organizations make, either implicitly or explicitly
  – Different companies make these decisions in different ways
  – Even in the same firm, different decision are apt to be made in different ways
  – Many of COBIT’s processes and controls are about how to best make these decisions
<table>
<thead>
<tr>
<th>Management Practice</th>
<th>Inputs</th>
<th>Outputs</th>
<th>To</th>
</tr>
</thead>
</table>
| **APO01.01 Define the organisational structure.** Establish an internal and extended organisational structure that reflects business needs and IT priorities. Put in place the required management structures (e.g., committees) that enable management decision making to take place in the most effective and efficient manner. | EDM01.01  
• Decision-making model  
• Enterprise governance guiding principles | Definition of organisational structure and functions | APO03.02        |
| APO03.02  
Process architecture model                                                        | Organisational operational guidelines                  | APO03.02        |
<p>|                                                    | Communication ground rules                             | All APO         |
|                                                    |                                                            | All BAI         |
|                                                    |                                                            | All DSS         |
|                                                    |                                                            | All MEA         |</p>
<table>
<thead>
<tr>
<th>APO01.01 Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Define the scope, internal and external functions, internal and external roles, and capabilities and decision rights required, including those IT activities performed by third parties.</td>
</tr>
<tr>
<td>2. Identify decisions required for the achievement of enterprise outcomes and the IT strategy, and for the management and execution of IT services.</td>
</tr>
<tr>
<td>3. Establish the involvement of stakeholders who are critical to decision making (accountable, responsible, consulted or informed).</td>
</tr>
<tr>
<td>4. Align the IT-related organisation with enterprise architecture organisational models.</td>
</tr>
<tr>
<td>5. Define the focus, roles and responsibilities of each function within the IT-related organisational structure.</td>
</tr>
<tr>
<td>6. Define the management structures and relationships to support the functions and roles of management and execution, in alignment with the governance direction set.</td>
</tr>
<tr>
<td>7. Establish an IT strategy committee (or equivalent) at the board level. This committee should ensure that governance of IT, as part of enterprise governance, is adequately addressed; advise on strategic direction; and review major investments on behalf of the full board.</td>
</tr>
<tr>
<td>8. Establish an IT steering committee (or equivalent) composed of executive, business and IT management to determine prioritisation of IT-enabled investment programmes in line with the enterprise’s business strategy and priorities; track status of projects and resolve resource conflicts; and monitor service levels and service improvements.</td>
</tr>
<tr>
<td>9. Provide guidelines for each management structure (including mandate, objectives, meeting attendees, timing, tracking, supervision and oversight) as well as required inputs for and expected outcomes of meetings.</td>
</tr>
<tr>
<td>10. Define ground rules for communication by identifying communication needs, and implementing plans based on those needs, considering top-down, bottom-up and horizontal communication.</td>
</tr>
<tr>
<td>11. Establish and maintain an optimal co-ordination, communication and liaison structure between the business and IT functions within the enterprise and with entities outside the enterprise.</td>
</tr>
<tr>
<td>12. Regularly verify the adequacy and effectiveness of the organisational structure.</td>
</tr>
</tbody>
</table>
What are the five decisions that all organization’s need to make?

1. IT Principles
2. IT Architecture
3. IT Infrastructure
4. Business Application Needs
5. IT Investment & Prioritization
# IT Governance Archetypes

## Week 3

**What are some common decision making structures?**

1. Executive committees
2. IT Leadership committees
3. Process teams
4. Business/IT relationship managers
5. IT Business councils
6. Architecture committee
7. Capital Approval Committee
IT Governance Archetypes
Week 3

What are some common alignment processes?

1. Tracking projects
2. Service level agreements
3. Tracking the business value of IT
4. Chargeback mechanisms

IT Governance
Rich Flanagan

FOX | ITACS
Master of IT Auditing & Cyber Security
What are some common communication approaches?

1. Work with unaligned managers
2. Senior management announcements
3. Office of the CIO or IT Governance group
4. IT Governance web portals
The Dentdel Case

• 30 minutes

• As teams, consider the following questions

  1. What processes were ineffective and allowed this situation to occur

  2. Suggest the steps management should take to assess the situation, and create an action plan.

  3. What kind of governance would you recommend to prevent a reoccurrence of such a project failure?

• Be prepared to discuss your ideas
Backup Slides
IT Governance Archetypes
Week 3

For which decisions is each archetype commonly used?

1. Business Monarchy
2. IT Monarchy
3. Feudal
4. Federal
5. Duopoly
6. Anarchy

What are the strengths and risks of each?