COBIT 5 Process Assessment Method (PAM)

Debra Mallette, CGEIT, CISA, CSSBB
Governance Risk and Compliance -G22
Session Objectives

• Why Assess Process Capability
• COBIT 5 Process Assessment Model
• Relationship to ISO/IEC 15504
• An assessment walk through of: Define and manage service levels
Why Assess Process Capability?

Informs executive management, board of directors and management stakeholders of:

• the capability of its IT processes
• targets for improvement based on business requirements

Enables fact-based decisions of where and how to apply resources in order to mitigate risks or assure value is delivered
2. Where are we now?
   • Define the Problems and Opportunities
   • Form Powerful Guiding Team
   • **Assess the Current State**
COBIT Process Assessment Model

- PAM brings together ISO and ISACA.
- COBIT 4.1 was adapted into ISO 15504 compliant Process Reference Model for COBIT 4.1 PAM
- COBIT 5 Enabling Processes designed for ISO 15504 compliance
What’s different?

• But don’t we already have maturity models for COBIT 4.1 processes?
• The new COBIT assessment programme is:
  – A robust assessment process based on ISO 15504
  – An alignment of COBIT’s maturity model scale with the international standard
  – A capability-based assessment model
• More rigor results in a more robust, objective and repeatable assessment
• Caution: Assessment results will likely vary from existing COBIT maturity models (or any other capability and/or maturity model!)
Assessment Model: Process Reference Model

- Domain and Scope
- Process Purpose
- Process Outcomes
COBIT as Process Reference Model

**PROCESS REFERENCE MODEL**
- Domain and Scope
- Process Purpose
- Process Outcomes

**4.1 or 5.0?**
- Purpose
- Outcomes
- Base Practices
- Work Products
### COBIT 5 Process Reference Model in PAM (excerpt from Draft)

<table>
<thead>
<tr>
<th>Process ID</th>
<th>Process Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APO09</td>
<td>Manage Service Agreements</td>
<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>
</tr>
<tr>
<td></td>
<td></td>
<td>Ensure that IT services and service levels meet current and future enterprise needs.</td>
</tr>
</tbody>
</table>

#### Outcomes (Os)

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APO09-O1</td>
<td>The enterprise can effectively utilise IT services as defined in a catalogue.</td>
</tr>
<tr>
<td>APO09-O2</td>
<td>Service agreements reflect enterprise needs and the capabilities of IT.</td>
</tr>
<tr>
<td>APO09-O3</td>
<td>IT services perform as stipulated in service agreements.</td>
</tr>
</tbody>
</table>

#### Base Practices (BPs)

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APO09-BP1</td>
<td>Identify and analyse business service needs and service level expectations.</td>
</tr>
<tr>
<td>APO09-BP2</td>
<td>Catalogue and publish service level agreements.</td>
</tr>
<tr>
<td>APO09-BP3</td>
<td>Define appropriate service level agreements.</td>
</tr>
<tr>
<td>APO09-BP4</td>
<td>Monitor and review service performance.</td>
</tr>
<tr>
<td>APO09-BP5</td>
<td>Conduct periodic reviews of the service agreements and revise when needed.</td>
</tr>
</tbody>
</table>

#### Work Products (WPs)

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
<th>Supports</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDM04-WP1</td>
<td>Guiding principles for allocation of resources and capabilities</td>
<td>APO09-BP2, APO09-O1</td>
</tr>
<tr>
<td>APO02-WP8</td>
<td>Gaps and changes required to realise target capability</td>
<td>APO09-O1</td>
</tr>
<tr>
<td>APO02-WP9</td>
<td>Value benefit statement for target environment</td>
<td>APO09-O1</td>
</tr>
<tr>
<td>APO06-WP4</td>
<td>IT budget and plan</td>
<td>APO09-BP2, APO09-O1</td>
</tr>
</tbody>
</table>

- **Purpose**
- **Outcomes**
- **Base Practices**
- **Work Products**
<table>
<thead>
<tr>
<th>Process ID: Name</th>
<th>APO09 Manage Service Agreements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Process Description</strong></td>
<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>
</tr>
<tr>
<td><strong>Process Purpose Statement</strong></td>
<td>Ensure that IT services and service levels meet current and future enterprise requirements.</td>
</tr>
</tbody>
</table>

**Purpose:** high-level measurable objectives of performing the process and the likely outcomes of effective implementation of the process.
Outcomes (O)

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APO09-O1</td>
<td>The enterprise can effectively utilize IT services as defined in a catalogue.</td>
</tr>
<tr>
<td>APO09-O2</td>
<td>Service Agreements reflect enterprise needs and the capabilities of IT.</td>
</tr>
<tr>
<td>APO09-O3</td>
<td>IT Services perform as stipulated in service agreements.</td>
</tr>
</tbody>
</table>

Outcomes: observable results of a process—an artefact, a significant change of state or the meeting of specified constraints
### Base Practices (BPs)

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
<th>Supports</th>
</tr>
</thead>
<tbody>
<tr>
<td>APO09-BP1</td>
<td>Identify IT services.</td>
<td>APO09-O1</td>
</tr>
<tr>
<td>APO09-BP2</td>
<td>Catalogue IT-enabled services.</td>
<td>APO09-O1</td>
</tr>
<tr>
<td>APO09-BP3</td>
<td>Define and prepare service agreements.</td>
<td>APO09-O1/O2</td>
</tr>
<tr>
<td>APO09-BP4</td>
<td>Monitor and report service levels.</td>
<td>APO09-O3</td>
</tr>
<tr>
<td>APO09-BP5</td>
<td>Review service agreements and contracts.</td>
<td>APO09-O3</td>
</tr>
</tbody>
</table>

**Base Practices:** activities that, when consistently performed, contribute to achieving the process purpose.
<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
<th>Supports</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDMO4-WP1</td>
<td>Guiding principles for allocation of resources and</td>
<td>APO09-BP2</td>
</tr>
<tr>
<td></td>
<td>capabilities</td>
<td>APO09-O1</td>
</tr>
<tr>
<td>APO02-WP8</td>
<td>Gaps and changes required to realize target</td>
<td></td>
</tr>
<tr>
<td></td>
<td>capability</td>
<td></td>
</tr>
<tr>
<td>APO02-WP9</td>
<td>Value Benefit statement for target environment</td>
<td></td>
</tr>
<tr>
<td>APO06-WP4</td>
<td>IT Budget and plan</td>
<td></td>
</tr>
</tbody>
</table>
COBIT 5 Process Reference Model in PAM (excerpt from Draft)

- Purpose
- Outcomes
- Base Practices
- Work Products
You don’t need the COBIT 5 PAM to get started. COBIT 5 Enabling Processes already documented as a ISO 15504 PRM

- Purpose
- Outcomes
- Base Practices
- Work Products
Purpose: Process Purpose Statement is the Purpose.

Outcomes: Under Process Goals and Metrics, the Process Goals are the observable outcomes.
COBIT 5 Enabling Processes
APO09 Manage Service Agreements

**Base Practices:** The Management Practices are the Base Practices.

**Work Products:** The Inputs and Outputs are the Work Products and/or Evidence.

**Purpose**

**Outcomes**

**Base Practices**

**Work Products**
Assessment Model: Measurement Framework

MEASUREMENT FRAMEWORK

- Capability Levels
- Process Attributes
- Rating Scale
Process Capability Levels & Attributes

**Level 0** Incomplete process
- Incomplete: The process is not implemented or fails to achieve its purpose.

**Level 1** Performed process
- Performed: The process is implemented and achieves its process purpose.
- PA 1.1: Process performance attribute

**Level 2** Managed process
- Managed: The process is managed and work products are established, controlled, and maintained.
- PA 2.1: Performance management attribute
- PA 2.2: Work product management attribute

**Level 3** Established process
- Established: A defined process is used based on a standard process.
- PA 3.1: Process definition attribute
- PA 3.2: Process deployment attribute

**Level 4** Predictable process
- Predictable: The process is enacted consistently within defined limits.
- PA 4.1: Process measurement attribute
- PA 4.2: Process control attribute

**Level 5** Optimizing process
- Optimizing: The process is continuously improved to meet relevant current and projected business goals.
- PA 5.1: Process innovation attribute
- PA 5.2: Process optimization attribute

**Optimizing**
The process is continuously improved to meet relevant current and projected business goals.

**Predictable**
The process is enacted consistently within defined limits.

**Established**
A defined process is used based on a standard process.

**Managed**
The process is managed and work products are established, controlled, and maintained.

**Performed**
The process is implemented and achieves its process purpose.

**Incomplete**
The process is not implemented or fails to achieve its purpose.
Process Capability Levels & Attributes

**Level 0**

**Incomplete process**

**Incomplete**
The process is not implemented or fails to achieve its purpose.
Process Capability Levels & Attributes

Level 0  Incomplete process
The process is not implemented or fails to achieve its purpose.

Level 1  Performed process
PA 1.1 Process performance attribute
Performed
The process is implemented and achieves its process purpose.
Process Capability Levels & Attributes

**Level 2 Managed process**

- **Performance management attribute**
  - PA 2.1

- **Work product management attribute**
  - PA 2.2

**Managed**
The process is managed and work products are established, controlled and maintained.

**Level 1 Performed process**

- **Process performance attribute**
  - PA 1.1

**Performed**
The process is implemented and achieves its process purpose.

**Level 0 Incomplete process**

**Incomplete**
The process is not implemented or fails to achieve its purpose.
Process Capability Level & Attributes

**Established**
A defined process is used based on a standard process.

**Level 3 Established process**
- PA 3.1 Process definition attribute
- PA 3.2 Process deployment attribute

**Level 1 Performed process**
- PA 1.1 Process performance attribute
  
**Level 0 Incomplete process**
- PA 2.1 Performance management attribute
- PA 2.2 Work product management attribute

**Performed**
The process is implemented and achieves its process purpose.

**Incomplete**
The process is not implemented or fails to achieve its purpose.
Process Capability Levels & Attributes

**Predictable**
The process is enacted consistently within defined limits.

**Level 4**
Predictable process
- PA 4.1 Process measurement attribute
- PA 4.2 Process control attribute

The process is enacted consistently within defined limits.

**Incomplete**
The process is not implemented or fails to achieve its purpose.
Process Capability Levels & Attributes

Optimizing
The process is continuously improved to meet relevant current and projected business goals.

Level 0  Incomplete process
The process is not implemented or fails to achieve its purpose.

Level 1  Performed process
PA 1.1 Process performance attribute
The process is implemented and achieves its process purpose.

Level 2  Managed process
PA 2.1 Performance management attribute
PA 2.2 Work product management attribute
The process is managed and work products are established, controlled and maintained.

Level 3  Established process
PA 3.1 Process definition attribute
PA 3.2 Process deployment attribute
A defined process is used based on a standard process.

Level 4  Predictable process
PA 4.1 Process measurement attribute
PA 4.2 Process control attribute
The process is enacted consistently within defined limits.

Level 5  Optimizing process
PA 5.1 Process innovation attribute
PA 5.2 Process optimization attribute
The process is continuously improved to meet relevant current and projected business goals.
Process Capability Levels & Attributes

**Incomplete process**
The process is not implemented or fails to achieve its purpose.

**Performed process**
The process is implemented and achieves its process purpose.

**Managed process**
The process is managed and work products are established, controlled and maintained.

**Established process**
A defined process is used based on a standard process.

**Predictable process**
The process is enacted consistently within defined limits.

**Optimizing process**
The process is continuously improved to meet relevant current and projected business goals.

**Level 0**
Incomplete process

**Level 1**
Performed process
- PA 1.1 Process performance attribute

**Level 2**
Managed process
- PA 2.1 Performance management attribute
- PA 2.2 Work product management attribute

**Level 3**
Established process
- PA 3.1 Process definition attribute
- PA 3.2 Process deployment attribute

**Level 4**
Predictable process
- PA 4.1 Process measurement attribute
- PA 4.2 Process control attribute

**Level 5**
Optimizing process
- PA 5.1 Process innovation attribute
- PA 5.2 Process optimization attribute
Process Attributes

• Each of the 9 Process Attributes are specified as:
  – Result of Full Achievement of Attribute
  – Generic Practices (GPs)
  – Generic Work Products (GWPs)
### Capability Level 1: Performed

**PA1.1 Process Performance**

<table>
<thead>
<tr>
<th>Result of Full Achievement of the Attribute</th>
<th>Generic Practices (GPs)</th>
<th>Generic Work Products (GWPs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The process achieves its defined outcomes.</td>
<td>GP1.1.1 Achieve the process outcomes. There is evidence that the intent of base practice is being performed.</td>
<td>Work products are produced that provide evidence of process outcomes.</td>
</tr>
</tbody>
</table>
Capability Level 1: Performed
PA1.1 Process Performance

• Capability Level 1 Performed?
• PA1.1 Process Performance?
  • Does the process achieve its defined outcomes?
    – As evidenced by:
      – Production of an object
      – A significant change of state
      – Meeting of specified constraints
        – e.g., requirements, goals
Process Attribute Rating Scale

- COBIT assessment process measures the extent to which a given process achieves the process attributes as:
  - Result of Full Achievement of Attribute
  - Generic Practices (GPs)
  - Generic Work Products (GWPs)
Process Attribute Rating Scale

N  Not achieved—> 0 to 15% achievement
  • Little or no evidence of achievement
P  Partially achieved—> 15% to 50% achievement
  • Some evidence of approach
  • Some achievement with aspects unpredictable
L  Largely achieved—> 50% to 85% achievement
  • Evidence of systematic approach
  • Significant achievement with some weakness
F  Fully achieved—> 85% to 100% achievement
  • Evidence of a complete & systematic approach
  • Full achievement, no significant weaknesses
## Process Attribute Rating Heat Map

<table>
<thead>
<tr>
<th>Process Attribute Achievement</th>
<th>85%-100%</th>
<th>Fully achieved</th>
</tr>
</thead>
<tbody>
<tr>
<td>50%-85%</td>
<td></td>
<td>Largely achieved</td>
</tr>
<tr>
<td>15%-50%</td>
<td></td>
<td>Partially achieved</td>
</tr>
<tr>
<td>0-15%</td>
<td></td>
<td>Not achieved</td>
</tr>
</tbody>
</table>
# Capability Level & Process Attributes

<table>
<thead>
<tr>
<th>Capability Level</th>
<th>Process Attribute</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 5: Optimizing</td>
<td>PA5.1&amp;5.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>F/L</td>
</tr>
<tr>
<td>Level 4: Predictable</td>
<td>PA4.1&amp;4.2</td>
<td></td>
<td></td>
<td></td>
<td>F/L</td>
<td>F</td>
</tr>
<tr>
<td>Level 3: Established</td>
<td>PA3.1&amp;3.2</td>
<td></td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>Level 2: Managed</td>
<td>PA2.1&amp;2.2</td>
<td>L/F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>Level 1: Performed</td>
<td>PA1.1</td>
<td>L/F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

Level 0: Incomplete

L/F = Largely or Fully Achieved  F = Fully Achieved
COBIT Assessment Model Overview

**PROCESS ASSESSMENT MODEL**

- Scope
- Indicators
- Mapping
- Translation
COBIT 5 PAM =>
COBIT 5 Capability + Attributes & PRM

Optimizing
Predictable
Established
Managed
Performed
Incomplete

Level 5
Level 4
Level 3
Level 2
Level 1
Level 0

Capability Measurement System

PRM
• Purpose
• Outcomes
• Base Practices
• Work Products

Processes for Governance:
Evaluate, Direct and Monitor

Processes for Management of Enterprise IT:
Evaluate, Direct and Monitor

COBIT 5 Processes

Measurable
Primary and Supporting Processes in PRM
Assess Process Capability with PAM:

COBIT 5 PAM Example: APO09 *Manage Service Agreements*
• Capability Level 1 Performed?
• PA1.1 Process Performance?
  • Does the process achieve its defined outcomes?
    – As evidenced by:
      – Production of an object
      – A significant change of state
      – Meeting of specified constraints
      – e.g., requirements, goals
APO09 Manage Service Agreements

- Capability Level 1 Performed?
- PA1.1 Process Performance?

<table>
<thead>
<tr>
<th>Process Attribute Achievement</th>
<th>85%-100%</th>
<th>Fully achieved</th>
</tr>
</thead>
<tbody>
<tr>
<td>50%-85%</td>
<td>Largely achieved</td>
<td></td>
</tr>
<tr>
<td>15%-50%</td>
<td>Partially achieved</td>
<td></td>
</tr>
<tr>
<td>0-15%</td>
<td>Not achieved</td>
<td></td>
</tr>
</tbody>
</table>
(Draft) COBIT 5 PAM: APO09 Manage Service Agreements

<table>
<thead>
<tr>
<th>Process ID</th>
<th>Process Name</th>
<th>APO09 Manage Service Agreements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Description</td>
<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>
<tr>
<td>Process Purpose Statement</td>
<td>Ensure that IT services and service levels meet current and future enterprise needs.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APO09-O1</td>
<td>The entire service environment should be consistent with the service catalogues.</td>
</tr>
<tr>
<td>APO09-O2</td>
<td>Service levels should be determined, with different levels specified for different service types.</td>
</tr>
<tr>
<td>APO09-O3</td>
<td>IT service agreements should be formal documents that manage the service delivery relationship.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Base Practices (BPs)</th>
<th>Supports</th>
</tr>
</thead>
<tbody>
<tr>
<td>APO09-BP1</td>
<td>Identify, analyse and rationalise service type and service level requirements.</td>
</tr>
<tr>
<td>APO09-BP2</td>
<td>Identify, analyse and rationalise service type and service level requirements.</td>
</tr>
<tr>
<td>APO09-BP3</td>
<td>Identify, analyse and rationalise service type and service level requirements.</td>
</tr>
<tr>
<td>APO09-BP4</td>
<td>Monitor and report service levels.</td>
</tr>
<tr>
<td>APO09-BP5</td>
<td>Review service agreements and contracts.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Products (WPs)</th>
<th>Supports</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDM04-WP1</td>
<td>Guiding principles for allocation of resources and capabilities</td>
</tr>
<tr>
<td>APO02-WP8</td>
<td>Gaps and changes required to realise target capability</td>
</tr>
<tr>
<td>APO02-WP9</td>
<td>Value benefit statement for target environment</td>
</tr>
<tr>
<td>APO06-WP4</td>
<td>IT budget and plan</td>
</tr>
</tbody>
</table>

- Purpose
- Outcomes
- Base Practices
- Work Products
Capability Level 2 Managed
PA 2.1 Performance Management

a. Objectives for process performance identified?
b. Performance of process planned and monitored?
c. Performance of process adjusted to meet plans?
d. Responsibilities and authorities for performing the process defined, assigned and communicated?
e. Resources and information necessary for performing the process identified, made available, allocated and used?
f. Interfaces between involved parties managed to ensure effective communication and clear assignment of responsibility?
Capability Level 2: Managed PA2.2 Work Product Management

a. Have requirements for the work products of the process been defined?

b. Have requirements for documentation and control of the work products been defined?

c. Are work products appropriately identified, documented and controlled?

d. Are work products reviewed in accordance with planned arrangements and adjusted as necessary to meet requirements?
### Assessed Process Capability Level

<table>
<thead>
<tr>
<th>Process Assessed</th>
<th>Capability Level 0: Incomplete</th>
<th>Capability Level 1: Performed</th>
<th>Capability Level 2: Managed</th>
</tr>
</thead>
<tbody>
<tr>
<td>APO09 Manage Service Agreements</td>
<td>False if Capability Level ( \geq 1 )</td>
<td>PA 1.1</td>
<td>PA2.1</td>
</tr>
<tr>
<td></td>
<td>FALSE</td>
<td>45%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0%</td>
</tr>
</tbody>
</table>
Assessment Process: Initial Input

INITIAL INPUT

- Purpose
- Scope
- Constraints
- Identities
- Approach
- Assessor
- Competence criteria
- Additional Information
Assessment Process: Roles

ROLES AND RESPONSIBILITIES

- Sponsor
- Competent Assessor
- Assessors
Assessor Roles:

COBIT process assessment roles:

Lead assessor—‘competent’ assessor responsible for overseeing the assessment activities
Assessor—developing assessor competencies; performs assessment activities

Competencies—Knowledge, skills and experience:
• PRM, PAM, Methods & Tools, Rating Processes
• Processes/Domains being assessed
• Personal attributes for effective performance

ISACA’s COBIT Assessor training and certification scheme under development
Assessment Process

ASSESSMENT PROCESS
Planning
Data Collection
Data Validation
Process Attribute Rating
Reporting
## Assessment Process - Planning

1. Initiation  
2. Planning the assessment  
3. Briefing  
4. Data collection  
5. Data validation  
6. Process attributes rating  
7. Reporting the results
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assessment Process - Assessing</strong></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>Initiation</td>
</tr>
<tr>
<td>2.</td>
<td>Planning the assessment</td>
</tr>
<tr>
<td>3.</td>
<td>Briefing</td>
</tr>
<tr>
<td>4.</td>
<td>Data collection</td>
</tr>
<tr>
<td>5.</td>
<td>Data validation</td>
</tr>
<tr>
<td>6.</td>
<td>Process attributes rating</td>
</tr>
<tr>
<td>7.</td>
<td>Reporting the results</td>
</tr>
</tbody>
</table>
Assessment Process - Reporting

1. Initiation
2. Planning the assessment
3. Briefing
4. Data collection
5. Data validation
6. Process attributes rating
7. Reporting the results
Assessment Process: Output

- Date
- Assessment Input
- Identification of Evidence
- Assessment Process Used
- Process Profiles
- Additional Information
## A Process Capability Profile

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>False if Process Capability is Level 1 or Better</td>
<td>Process Performance (PA 1.1)</td>
<td>Performance Management (PA2.1)</td>
<td>Work Product Management (PA2.2)</td>
<td>Definition (PA3.1)</td>
<td>Deployment (PA3.2)</td>
</tr>
<tr>
<td>DS1: Define and Manage Service Levels</td>
<td>FALSE</td>
<td>45%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>DS2: Manage Third Party Services</td>
<td>FALSE</td>
<td>30%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>DS4: Ensure Continuous Service</td>
<td>FALSE</td>
<td>35%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>DS6: Ensure Systems Security</td>
<td>FALSE</td>
<td>90%</td>
<td>60%</td>
<td>75%</td>
<td>10%</td>
<td>0%</td>
</tr>
<tr>
<td>DS8: Manage Service Desk and Incidents</td>
<td>FALSE</td>
<td>90%</td>
<td>75%</td>
<td>45%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>DS9: Manage the Configuration</td>
<td>FALSE</td>
<td>60%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>DS11: Manage Data</td>
<td>FALSE</td>
<td>75%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>ME2: Monitor and Evaluate Internal Control</td>
<td>FALSE</td>
<td>90%</td>
<td>25%</td>
<td>20%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>ME3: Ensure Compliance with External Requirements</td>
<td>FALSE</td>
<td>90%</td>
<td>60%</td>
<td>70%</td>
<td>45%</td>
<td>0%</td>
</tr>
</tbody>
</table>
## Consequence of Capability Gaps

Figure A.3—Consequence of Gaps at Various Capability Levels

<table>
<thead>
<tr>
<th>Capability level where gap occurs</th>
<th>Nature of consequence</th>
<th>Seriousness of Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 – Optimizing process</td>
<td>inability to achieve or evaluate process improvements</td>
<td></td>
</tr>
<tr>
<td>4 – Predictable process</td>
<td>inability to quantify performance or detect problems early</td>
<td></td>
</tr>
<tr>
<td>3 – Established process</td>
<td>inconsistent process performance across organization</td>
<td></td>
</tr>
<tr>
<td>2 – Managed process</td>
<td>cost or time overruns; unpredictable product quality</td>
<td></td>
</tr>
<tr>
<td>1 – Performed process</td>
<td>missing work products; process outcomes Not achieved</td>
<td></td>
</tr>
</tbody>
</table>

This figure is reproduced from ISO 15504-4 2006 with the permission of ISO at www.iso.org. Copyright remains with ISO.
Risk from Capability Gaps

Figure A.4—Risk Associated With Each Capability Level

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Slight</th>
<th>Significant</th>
<th>Substantial</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 – Optimizing process</td>
<td>Low Risk</td>
<td>Low Risk</td>
<td>Low Risk</td>
</tr>
<tr>
<td>4 – Predictable process</td>
<td>Low Risk</td>
<td>Low Risk</td>
<td>Medium Risk</td>
</tr>
<tr>
<td>3 – Established process</td>
<td>Low Risk</td>
<td>Medium Risk</td>
<td>Medium Risk</td>
</tr>
<tr>
<td>2 – Managed process</td>
<td>Medium Risk</td>
<td>Medium Risk</td>
<td>High Risk</td>
</tr>
<tr>
<td>1 – Performed process</td>
<td>Medium Risk</td>
<td>High Risk</td>
<td>High Risk</td>
</tr>
</tbody>
</table>

This figure is reproduced from ISO 15504-4 2006 with the permission of ISO at www.iso.org. Copyright remains with ISO.
Summary

Process Reference Model
- Domain and Scope
- Process Purpose
- Process Outcomes

Process Assessment Model
- Scope
- Indicators
- Mapping
- Translation

ASSESSMENT PROCESS
- Planning
- Data Collection
- Data Validation
- Process Attribute Rating
- Reporting

Roles and Responsibilities
- Sponsor
- Competent Assessor
- Assessors

INITIAL INPUT
- Purpose
- Scope
- Constraints
- Identities
- Approach
- Assessor
- Competence Criteria
- Additional Information

OUTPUT
- Date
- Assessment Input
- Identification of Evidence
- Assessment Process Used
- Process Profiles
- Additional Information

Measurement Framework
- Capability Levels
- Process Attributes
- Rating Scale

Process Capability Level (based on attributes)
- Capability Level 0: Incomplete
- Capability Level 1: Performed
- Capability Level 2: Managed
- Capability Level 3: Established
- Capability Level 4: Predictable
- Capability Level 5: Optimizing

DS1: Define and Manage Service Levels FALSE
45% 0% 0% 0% 0% N/A N/A N/A N/A

DS2: Manage Third Party Services FALSE
30% 0% 0% 0% 0% N/A N/A N/A N/A

DS4: Ensure Continuous Service FALSE
35% 0% 0% 0% 0% N/A N/A N/A N/A

DS6: Ensure Systems Security FALSE
90% 60% 75% 10% 0% N/A N/A N/A N/A

DS8: Manage Service Desk and Incidents FALSE
90% 75% 45% 0% 0% N/A N/A N/A N/A

DS9: Manage the Configuration FALSE
60% 0% 0% 0% 0% N/A N/A N/A N/A

DS11: Manage Data FALSE
75% 0% 0% 0% 0% N/A N/A N/A N/A

ME2: Monitor and Evaluate Internal Control FALSE
90% 25% 20% 0 0% N/A N/A N/A N/A

ME3: Ensure Compliance with External Requirements FALSE
90% 60% 70% 45% 0% N/A N/A N/A N/A
Contact Information:

- Debra Mallette, CGEIT, CISA, CSSBB
- PastPresident@sfasica.org