

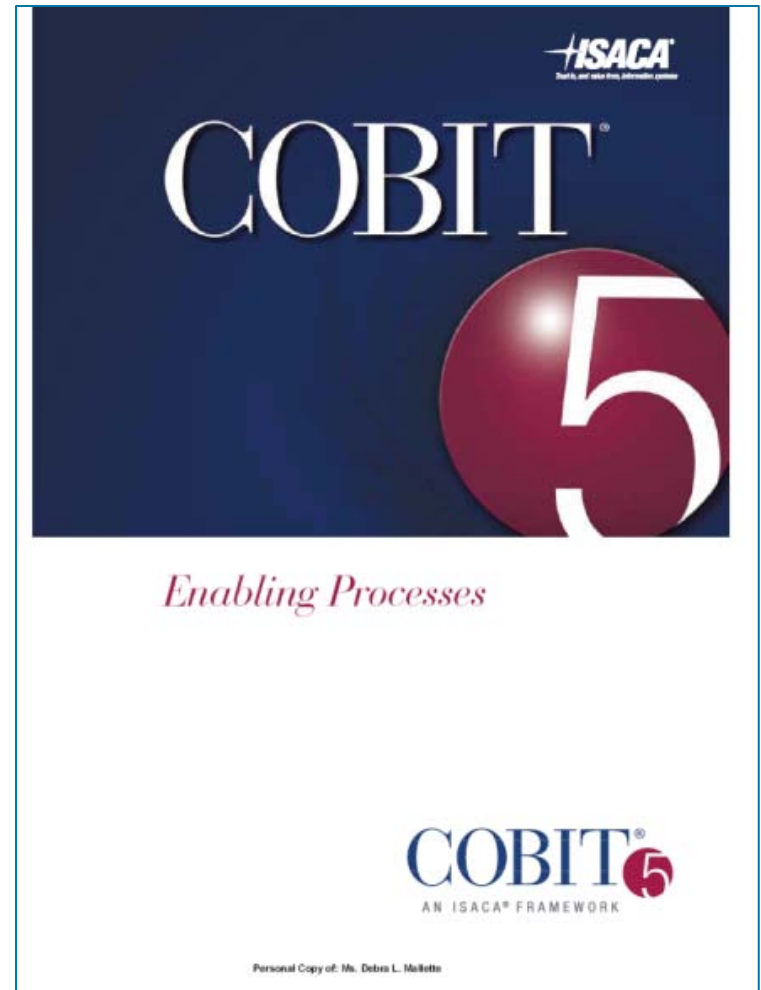
COBIT 5 Process Assessment Method (PAM)

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:

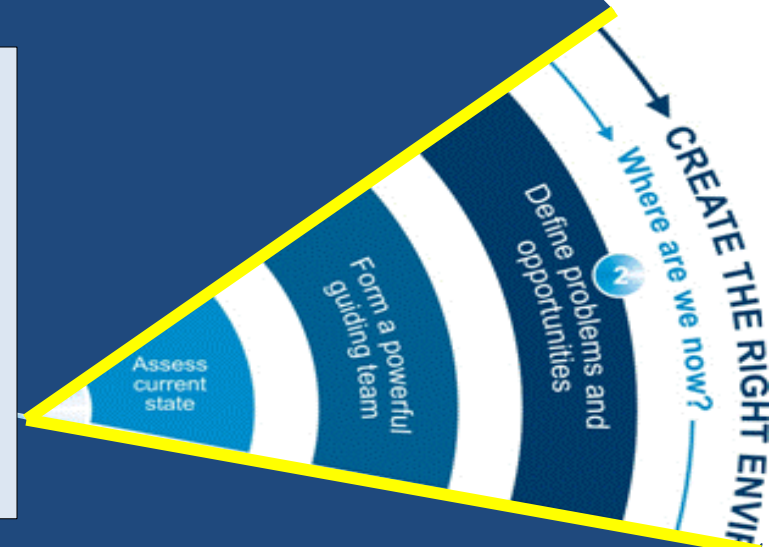
- the capability of its IT processes
- targets for improvement based on business requirements

Enables fact-based decisions of where and how to apply resources in order to mitigate risks or assure value is delivered

When?

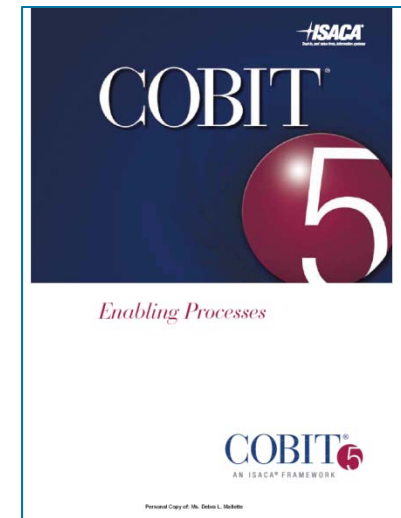
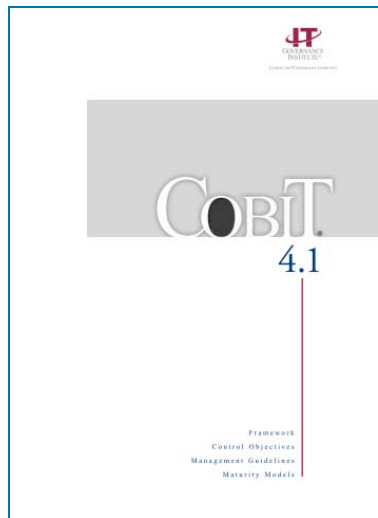
2. Where are we now?

- Define the Problems and Opportunities
- Form Powerful Guiding Team
- ***Assess the Current State***



COBIT Process Assessment Model

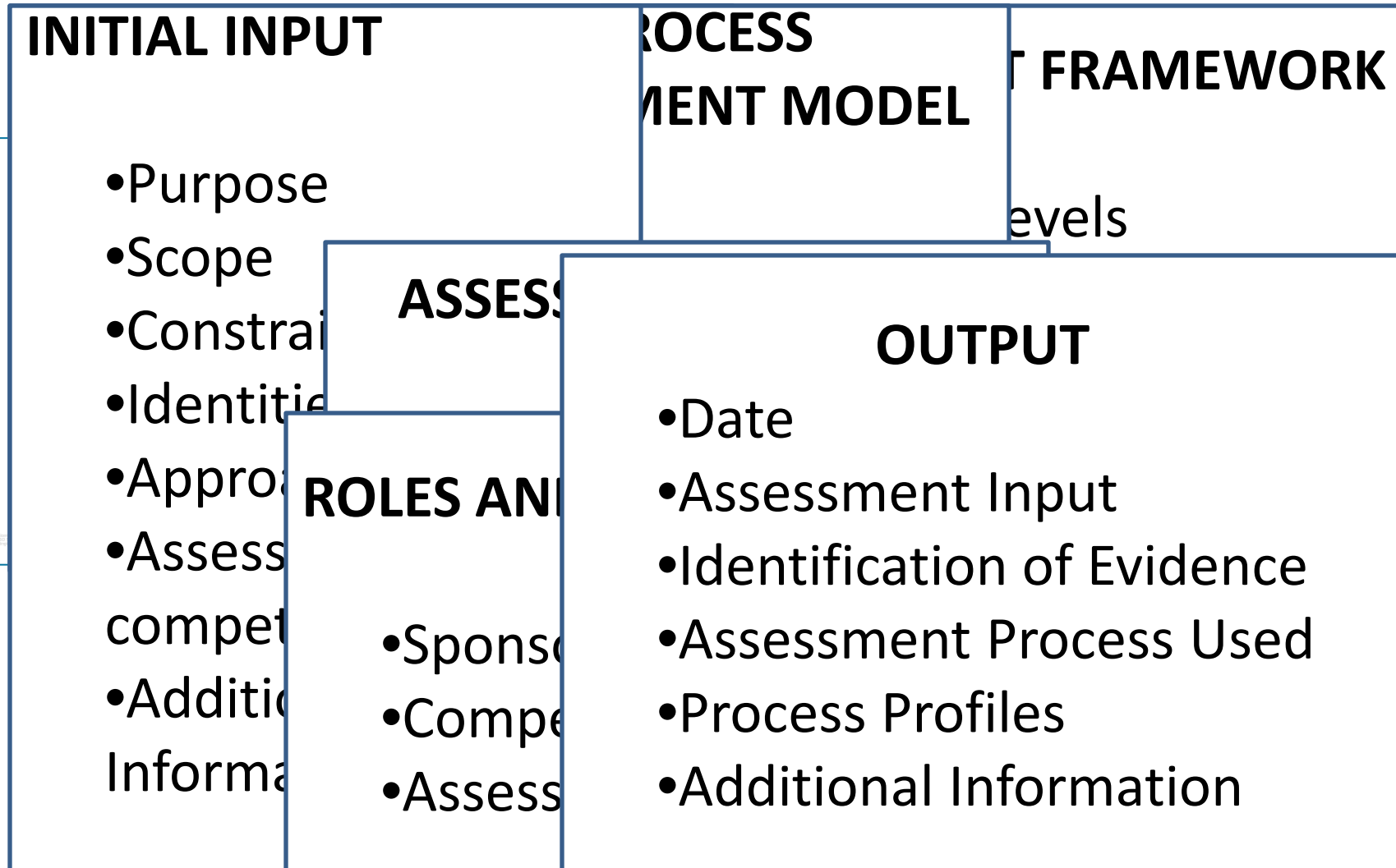
- 1st Described in *COBIT[®] Process Assessment Model (PAM): Using COBIT[®] 4.1*.
- PAM brings together ISO and ISACA.
- COBIT 4.1 was adapted into ISO 15504 compliant Process Reference Model for COBIT 4.1 PAM
- COBIT 5 Enabling Processes designed for ISO 15504 compliance



What's different?

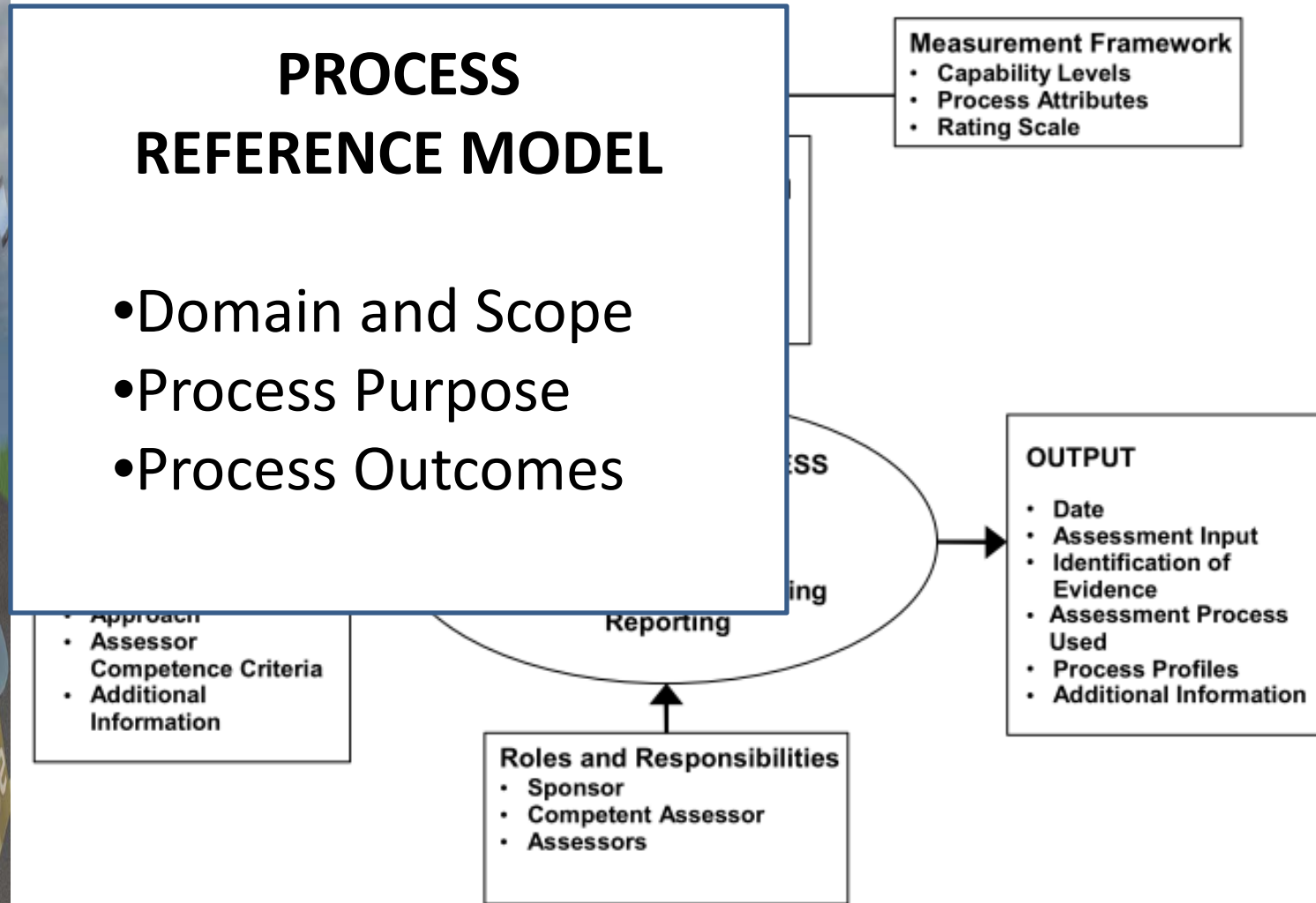
- But don't we already have **maturity models** for COBIT 4.1 processes?
- The new COBIT assessment programme is:
 - A robust assessment process based on ISO 15504
 - An alignment of COBIT's maturity model scale with the international standard
 - A *capability*-based assessment model
- More rigor results 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!)*

ISO 15504 Assessment Overview

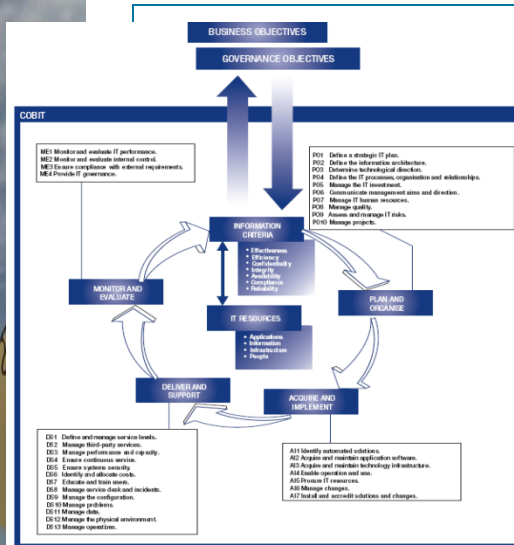


This figure is reproduced from ISO 15504-2:2003 with the permission of ISO at www.iso.org. Copyright remains with ISO.

Assessment Model: Process Reference Model



COBIT as Process Reference Model

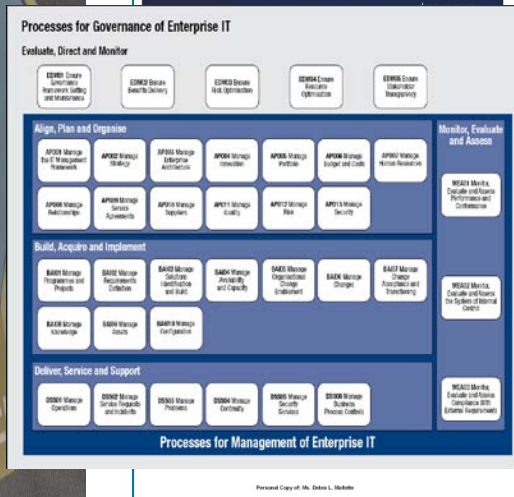


PROCESS REFERENCE MODEL

- 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)

Process ID	APO09	
Process Name	Manage Service Agreements	
Process Description	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.	
Process Purpose Statement	Ensure that IT services and service levels meet current and future enterprise needs.	
Outcomes (Os)		
Number	Description	
APO09-O1	The enterprise can effectively utilise IT services as defined in a catalogue.	
APO09-O2	Service agreements reflect enterprise needs and the capabilities of IT.	
APO09-O3	IT services perform as stipulated in service agreements.	
Base Practices (BPs)		
Number	Description	Supports
APO09-BP1	Identify and analyse IT services and service levels against current and future enterprise needs and options.	APO09-O1
APO09-BP2	Catalogue and publish IT services and service levels for enterprise groups.	APO09-O1
APO09-BP3	Define and publish IT service levels for enterprise groups.	APO09-O1/O2
APO09-BP4	Monitor and report on IT service levels to ensure they meet enterprise needs.	APO09-O3
APO09-BP5	Review and revise service agreements and service levels when needed.	APO09-O3
Work Products (WPs)		
Inputs		
Number	Description	Supports
EDM04-WP1	Guiding principles for allocation of resources and capabilities	APO09-BP2, APO09-O1
APO02-WP8	Gaps and changes required to realise target capability	
APO02-WP9	Value benefit statement for target environment	
APO06-WP4	IT budget and plan	

- Purpose
- Outcomes
- Base Practices
- Work Products

Process ID: Name	APO09 Manage Service Agreements
Process Description	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
Process Purpose Statement	Ensure that IT services and service levels meet current and future enterprise requirements.

Purpose: high-level measurable objectives of performing the process and the likely outcomes of effective implementation of the process

COBIT 5 Process Reference Model in PAM (excerpt from Draft)

Outcomes (O)

Number	Description
APO09-O1	The enterprise can effectively utilize IT services as defined in a catalogue.
APO09-O2	Service Agreements reflect enterprise needs and the capabilities of IT.
APO09-O3	IT Services perform as stipulated in service agreements.

Outcomes: observable results of a process—an artefact, a significant change of state or the meeting of specified constraints

Base Practices (BPs)

Number	Description	Supports
APO09-BP1	Identify IT services.	APO09-O1
APO09-BP2	Catalogue IT-enabled services.	APO09-O1
APO09-BP3	Define and prepare service agreements.	APO09-O1/O2
APO09-BP4	Monitor and report service levels.	APO09-O3
APO09-BP5	Review service agreements and contracts.	APO09-O3

Base Practices: activities that, when consistently performed, contribute to achieving the process purpose

Work Products (WPs)

Inputs		
Number	Description	Supports
EDMO4-WP1	Guiding principles for allocation of resources and capabilities	APO09-BP2 APO09-O1
APO02-WP8	Gaps and changes required to realize target capability	
APO02-WP9	Value Benefit statement for target environment	
APO06-WP4	IT Budget and plan	

Work Products: artefacts associated with the execution of a process—‘inputs’ and “outputs”

COBIT 5 Process Reference Model in PAM (excerpt from Draft)

Process ID	APO09		
Process Name	Manage Service Agreements		
Process Description	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.		
Process Purpose Statement	Ensure that IT services and service levels meet current and future enterprise needs.		
Outcomes (Os)			
Number	Description		
APO09-O1	The enterprise has a clear understanding of its service needs and expectations.		
APO09-O2	Service levels are defined and agreed upon.		
APO09-O3	IT services are delivered in accordance with agreed service levels.		
Base Practices (BPs)			
Number	Description	Supports	
APO09-BP1	Identify and analyse service needs and expectations, current service levels, and options for improvement.	APO09-O1	
APO09-BP2	Catalogue and publish service levels and options.	APO09-O1	
APO09-BP3	Define and prepare service agreements based on the options in the service catalogues. Include internal operational agreements.	APO09-O1/O2	
APO09-BP4	Monitor and report service levels. Monitor service levels, report on achievements and identify trends. Provide the appropriate management information to aid performance management.	APO09-O3	
APO09-BP5	Review service agreements and contracts. Conduct periodic reviews of the service agreements and revise when needed.	APO09-O3	
Work Products (WPs)			
Inputs			
Number	Description	Supports	
EDM04-WP1	Guiding principles for allocation of resources and capabilities	APO09-BP2, APO09-O1	
APO02-WP8	Gaps and changes required to realise target capability		
APO02-WP9	Value benefit statement for target environment		
APO06-WP4	IT budget and plan		

- Purpose
- Outcomes
- Base Practices
- Work Products

COBIT 5 Enabling Processes as Process Reference Model



Enabling Processes

COBIT[®] 5
AN ISACA[®] FRAMEWORK

Personal Copy of: Ms. Debra L. Mallette

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**

COBIT 5 Enabling Processes

APO09 Manage Service

- Purpose
- Outcomes
- Base Practices
- Work Products

APO09 Manage Service Agreements
Process Description Align IT-enabled services and service levels with enterprise needs and expectations, including and monitoring of IT services, service levels and performance indicators.
Process Purpose Statement Ensure that IT services and service levels meet current and future enterprise needs.

Purpose: Process Purpose Statement is the Purpose.

14 Availability of reliable and useful information for decision making	• Level of business user satisfaction with quality and timeliness (or availability) of management information • Number of business process incidents caused by non-availability of information • Ratio and extent of erroneous business decisions where erroneous or unavailable information was a key factor
Process Goals and Metrics	
Process Goal	Related Metrics
1. The enterprise can effectively utilise IT services as defined in a catalogue.	• Number of business processes with undefined service agreements
2. Service agreements reflect enterprise needs and the capabilities of IT.	• Percent of live IT services covered by service agreements • Percent of customers satisfied that service delivery meets agreed-on levels
3. IT services perform as stipulated in service agreements.	• Number and severity of service breaches • Percent of services being monitored to service levels • Percent of service targets being met

Align, Plan and Organise

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.

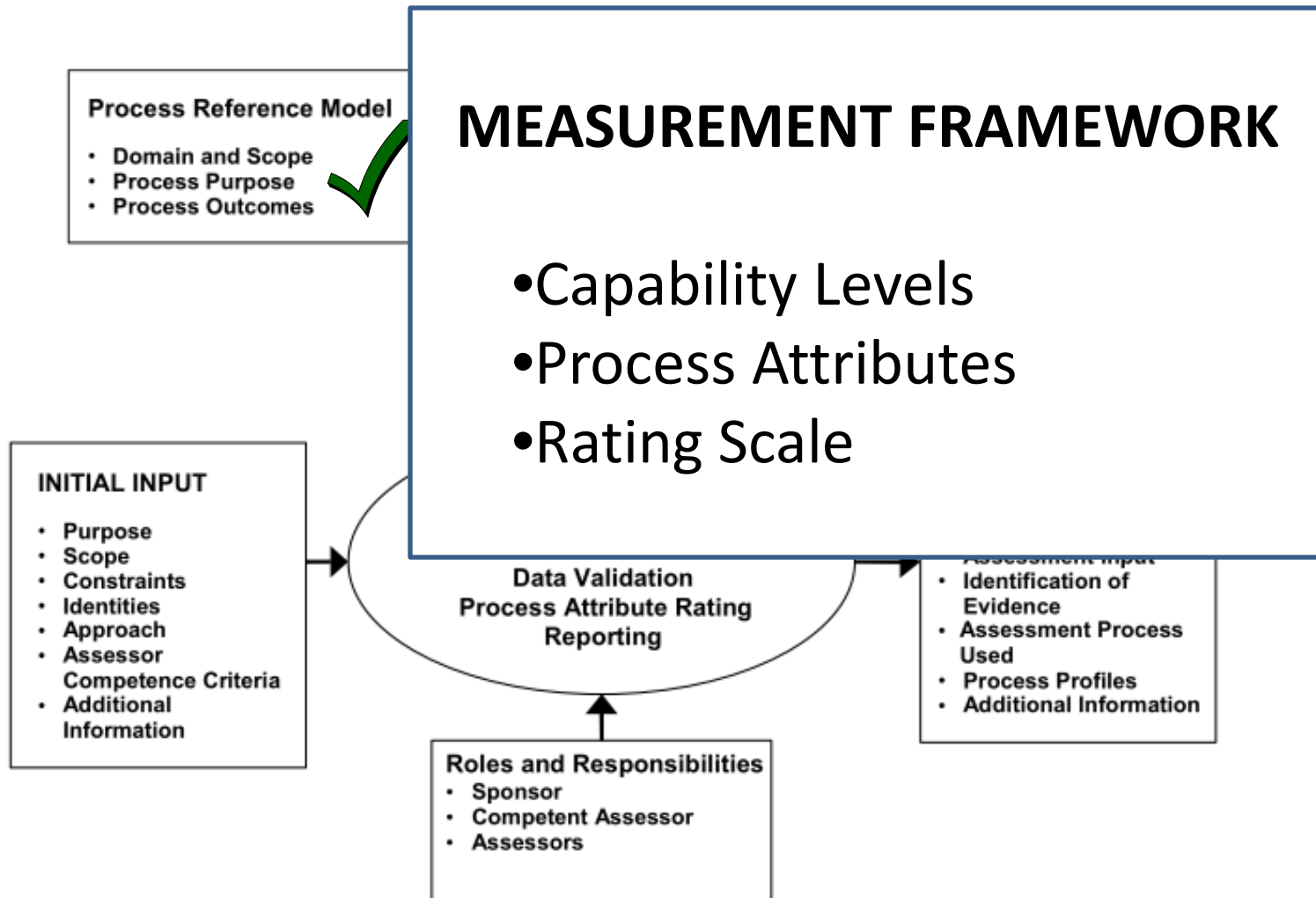
- Purpose
- Outcomes
- Base Practices
- Work Products

APO09 Process Practices, Inputs/Outputs and Activities

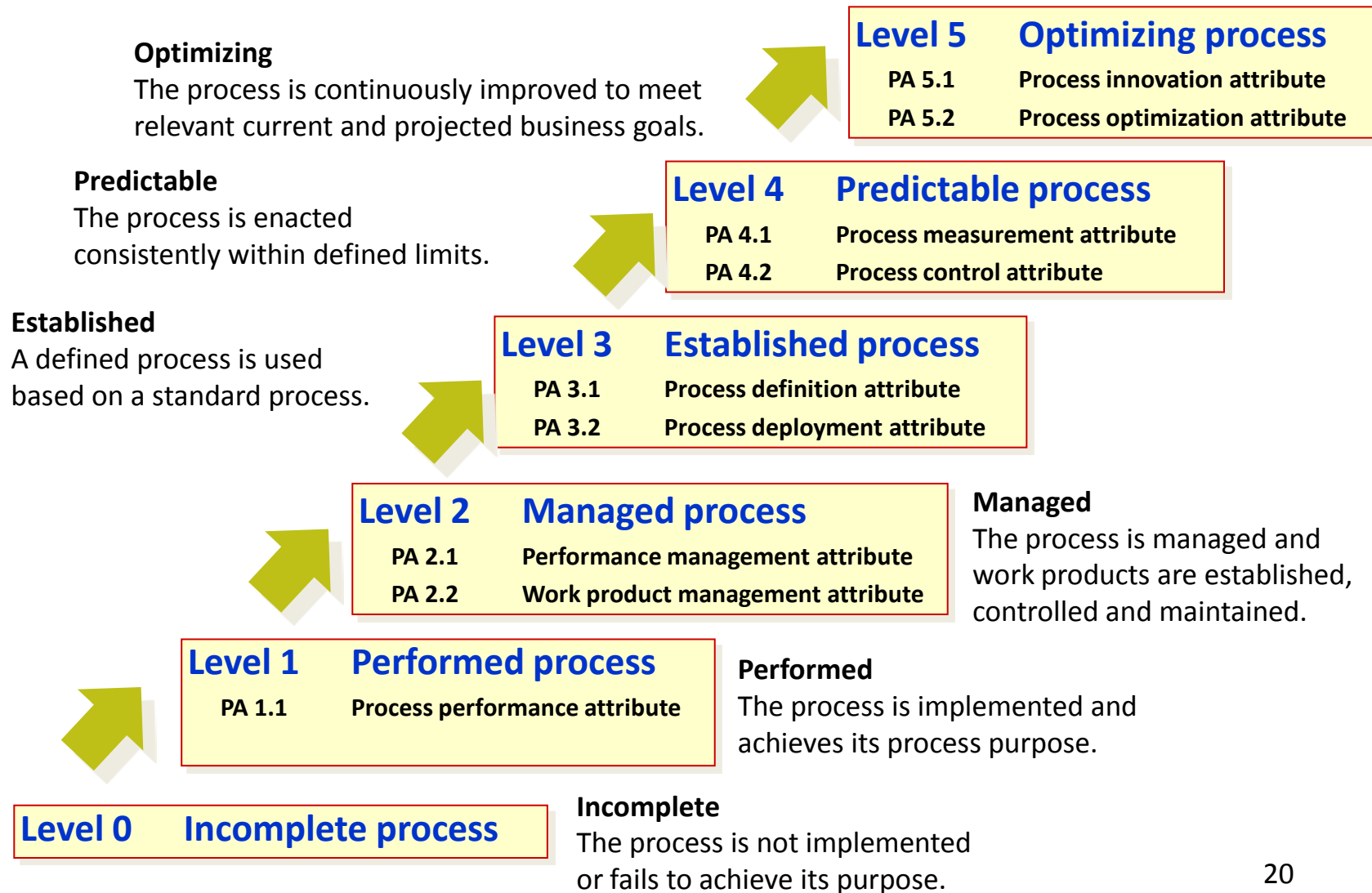
Management Practice	Inputs		Outputs	
	From	Description	Description	To
AP009.01 Identify IT services. Analyse business requirements and the way in which IT-enabled services and service levels support business processes. Discuss and agree on potential services and service levels with the business, and compare them with the current service portfolio to identify new or changed services or service level options.			Identified gaps in IT services to the business	AP002.02 AP005.03 AP008.02
			Definitions of standard services	AP005.01

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

Assessment Model: Measurement Framework



Process Capability Levels & Attributes



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 1 Performed process

**PA 1.1 Process
performance
attribute**

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 Levels & Attributes

Level 2 Managed process

PA 2.1 Performance management attribute

PA 2.2 Work product management attribute

Managed

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

Level 1 Performed process

PA 1.1 Process performance attribute

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

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 1 Performed process

PA 1.1

Process performance attribute

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 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



PA 1.1 Process performance attribute

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 Levels & Attributes

Optimizing

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

Level 5 Optimizing process

PA 5.1 Process innovation attribute

PA 5.2 Process optimization attribute



PA 1.1 Process performance attribute

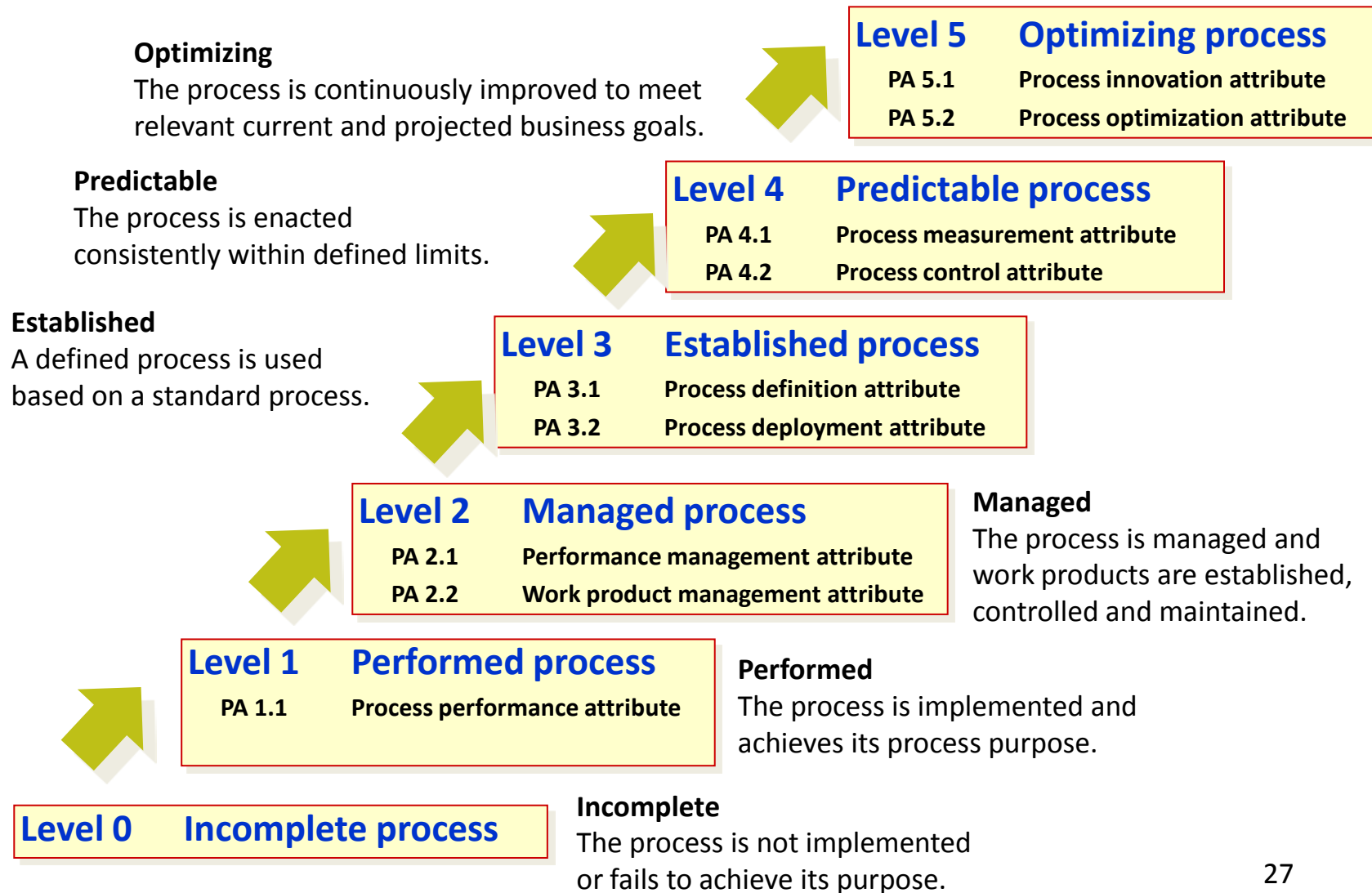
The process is implemented and achieves its process purpose.

Level 0 Incomplete process

Incomplete

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

Process Capability Levels & Attributes





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

PA1.1-Process Performance

Result of Full Achievement of the Attribute	Generic Practices (GPs)	Generic Work Products (GWPs)
The process achieves its defined outcomes.	GP1.1.1 Achieve the process outcomes. There is evidence that the intent of base practice is being performed.	Work products are produced that provide evidence of process outcomes.



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

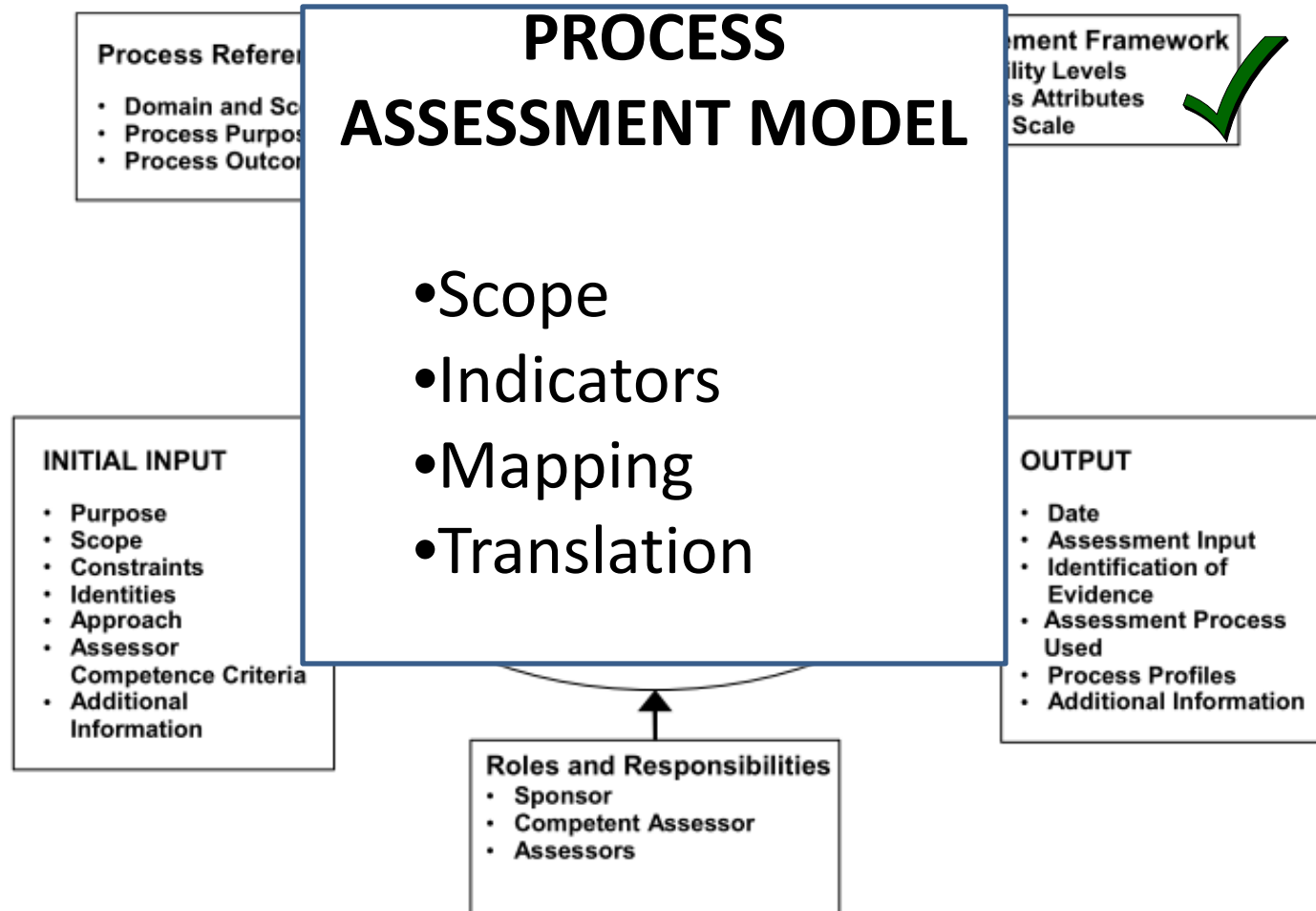
Process Attribute Achievement		
	85%-100%	Fully achieved
	50%-85%	Largely achieved
	15%-50%	Partially achieved
	0-15%	Not achieved

Capability Level & Process Attributes

Capability Level	Process Attribute	1	2	3	4	5
Level 5: Optimizing	PA5.1&5.2					L/F
Level 4: Predictable	PA4.1&4.2				L/F	F
Level 3: Established	PA3.1&3.2			L/F	F	F
Level 2: Managed	PA2.1&2.2		L/F	F	F	F
Level 1: Performed	PA1.1	L/F	F	F	F	F
Level 0: Incomplete						

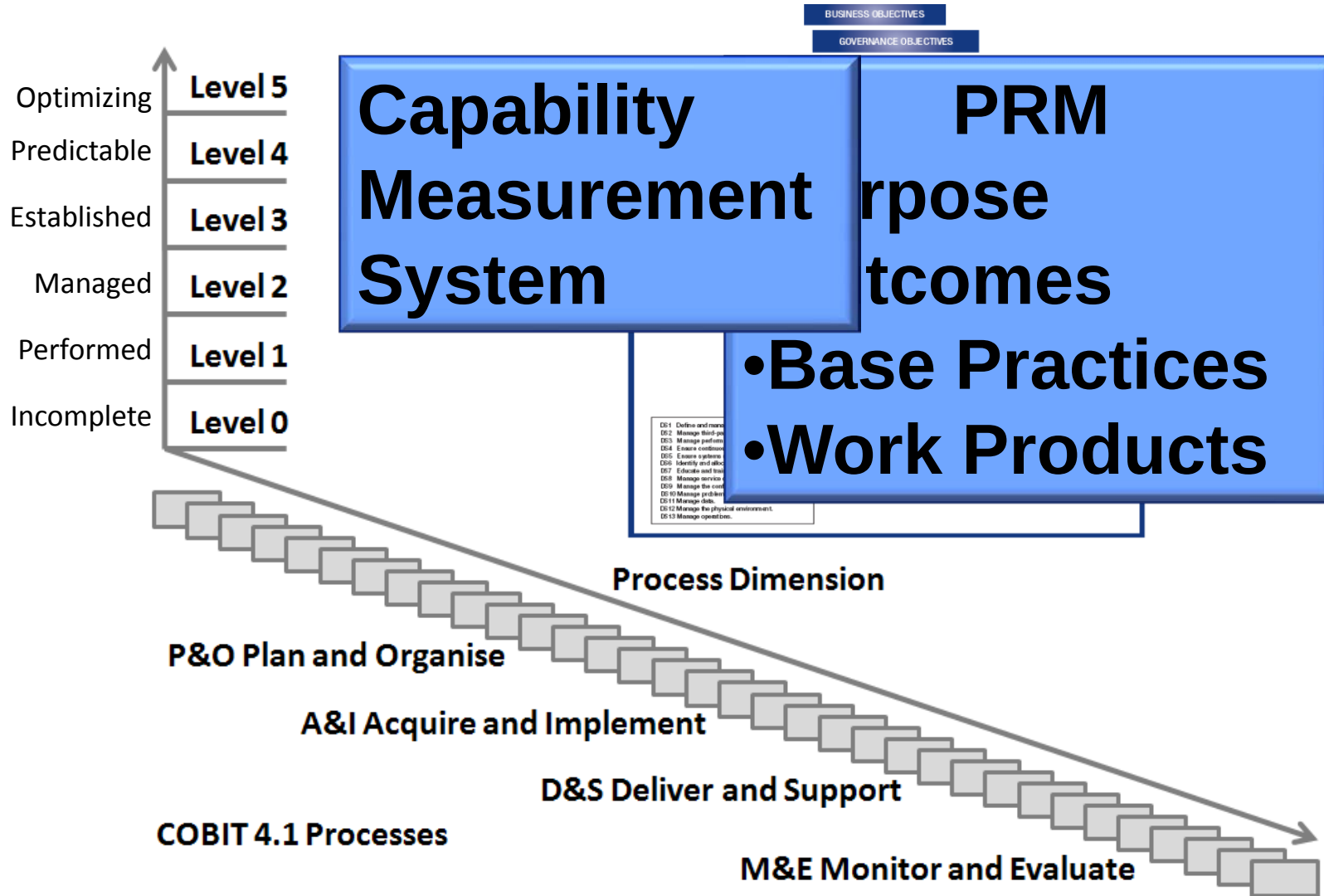
L/F = Largely or Fully Achieved F = Fully Achieved ³⁴

COBIT Assessment Model Overview



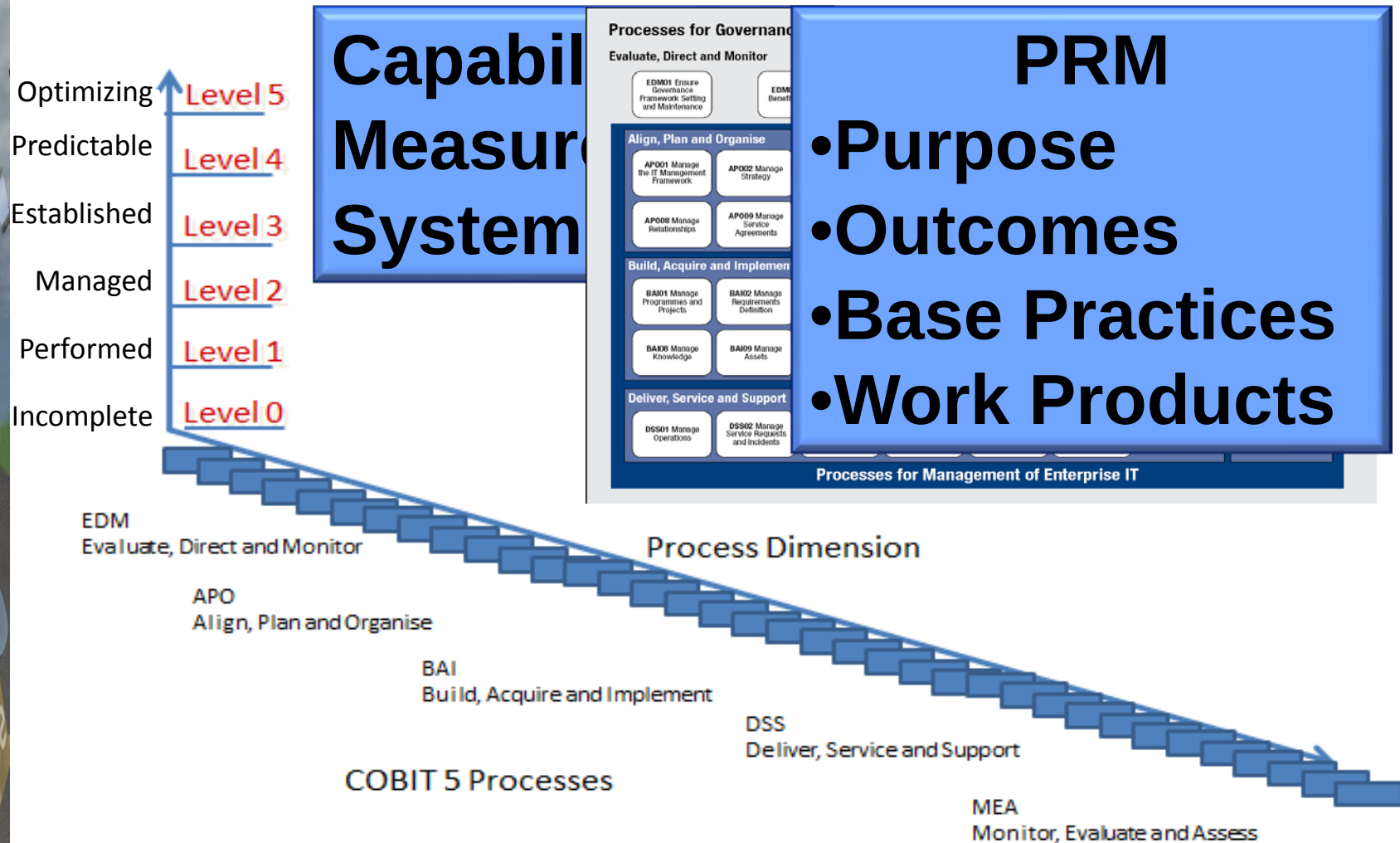
COBIT 4.1 PAM:

COBIT 4.1 Capability + Attributes & PRM



COBIT 5 PAM =>

COBIT 5 Capability + Attributes & PRM



Primary and Supporting Processes in PRM





Assess Process Capability with PAM:

COBIT 5 PAM Example: *APO09 Manage Service Agreements*

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?

Process Attribute Achievement		
	85%-100%	Fully achieved
	50%-85%	Largely achieved
	15%-50%	Partially achieved
	0-15%	Not achieved

(Draft) COBIT 5 PAM:

APO09 Manage Service Agreements

Process ID	APO09		
Process Name	Manage Service Agreements		
Process Description	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.		
Process Purpose Statement	Ensure that IT services and service levels meet current and future enterprise needs.		
Outcomes (Os)			
Number	Description		
APO09-O1	The enterprise service levels are aligned with business needs and expectations.		
APO09-O2	Service levels are monitored and reported to management.		
APO09-O3	IT service agreements are reviewed and updated as needed.		
Base Practices (BPs)			
Number	Description	Supports	
APO09-BP1	Identify and analyse service levels and current options.	APO09-O1	
APO09-BP2	Catalogue and publish service level groups.	APO09-O1	
APO09-BP3	Define and prepare service agreements based on the options in the service catalogues. Include internal operational agreements.	APO09-O1/O2	
APO09-BP4	Monitor and report service levels. Monitor service levels, report on achievements and identify trends. Provide the appropriate management information to aid performance management.	APO09-O3	
APO09-BP5	Review service agreements and contracts. Conduct periodic reviews of the service agreements and revise when needed.	APO09-O3	
Work Products (WPs)			
Inputs			
Number	Description	Supports	
EDM04-WP1	Guiding principles for allocation of resources and capabilities	APO09-BP2, APO09-O1	
APO02-WP8	Gaps and changes required to realise target capability		
APO02-WP9	Value benefit statement for target environment		
APO06-WP4	IT budget and plan		

- 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

	Capability Level 0: Incomplete	Capability Level 1: Performed	Capability Level 2: Managed	
Process Assessed	False if Capability Level $\neq$ / $>$ 1	PA 1.1	PA2.1	PA2.2
APO09 Manage Service Agreements	FALSE	45%	0%	0%

Assessment Process: Initial Input

INITIAL INPUT

- Purpose
- Scope
- Constraints
- Identities
- Approach
- Assessor competence criteria
- Additional Information

Measurement Framework

- Capability Levels
- Process Attributes
- Rating Scale



Model



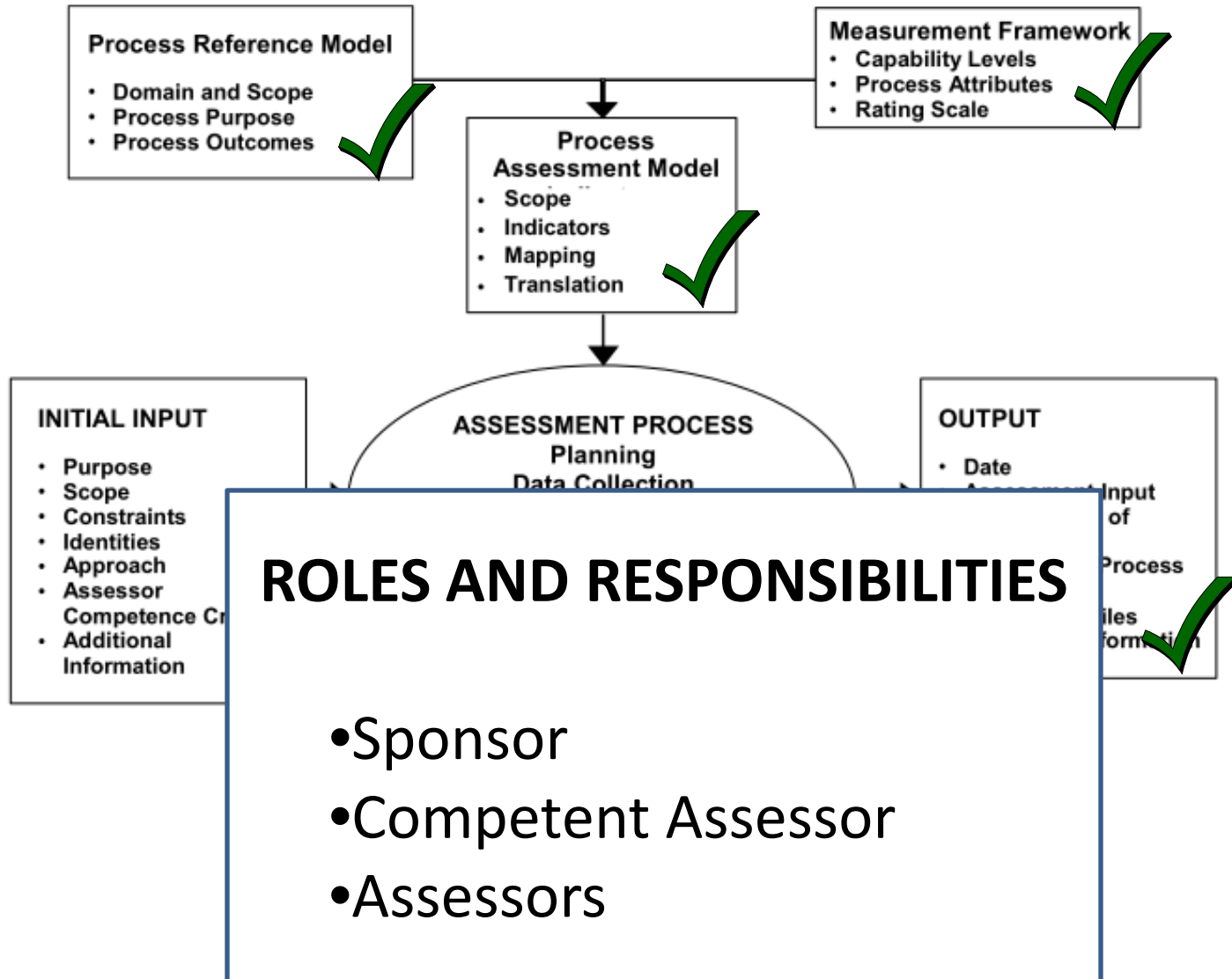
PROCESS

Responsibilities

OUTPUT

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

Assessment Process: Roles





Assessor Roles:

COBIT process assessment roles:

Lead assessor—‘competent’ assessor responsible for overseeing the assessment activities

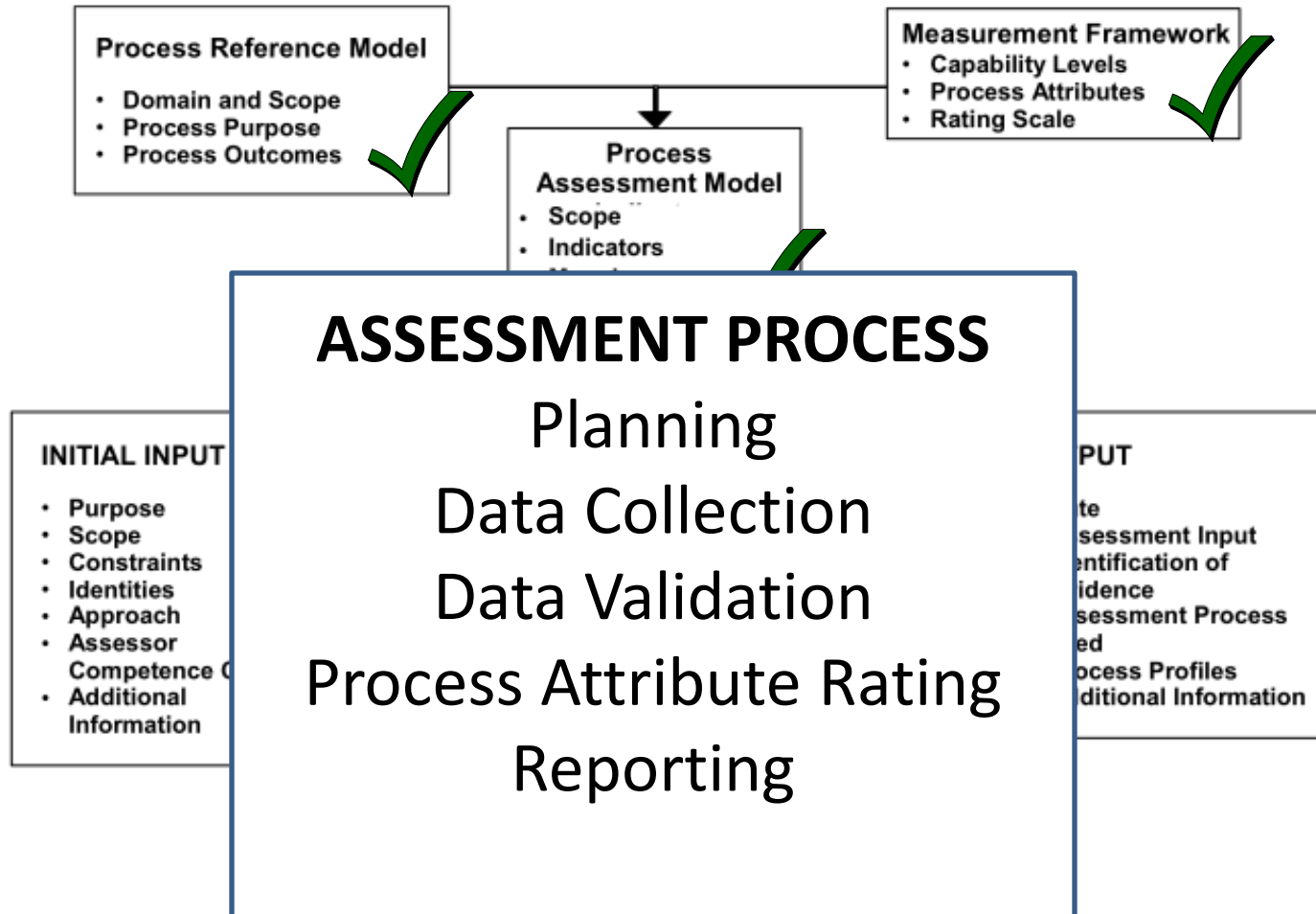
Assessor—developing assessor competencies; performs assessment activities

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

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



Assessment Process - Assessing

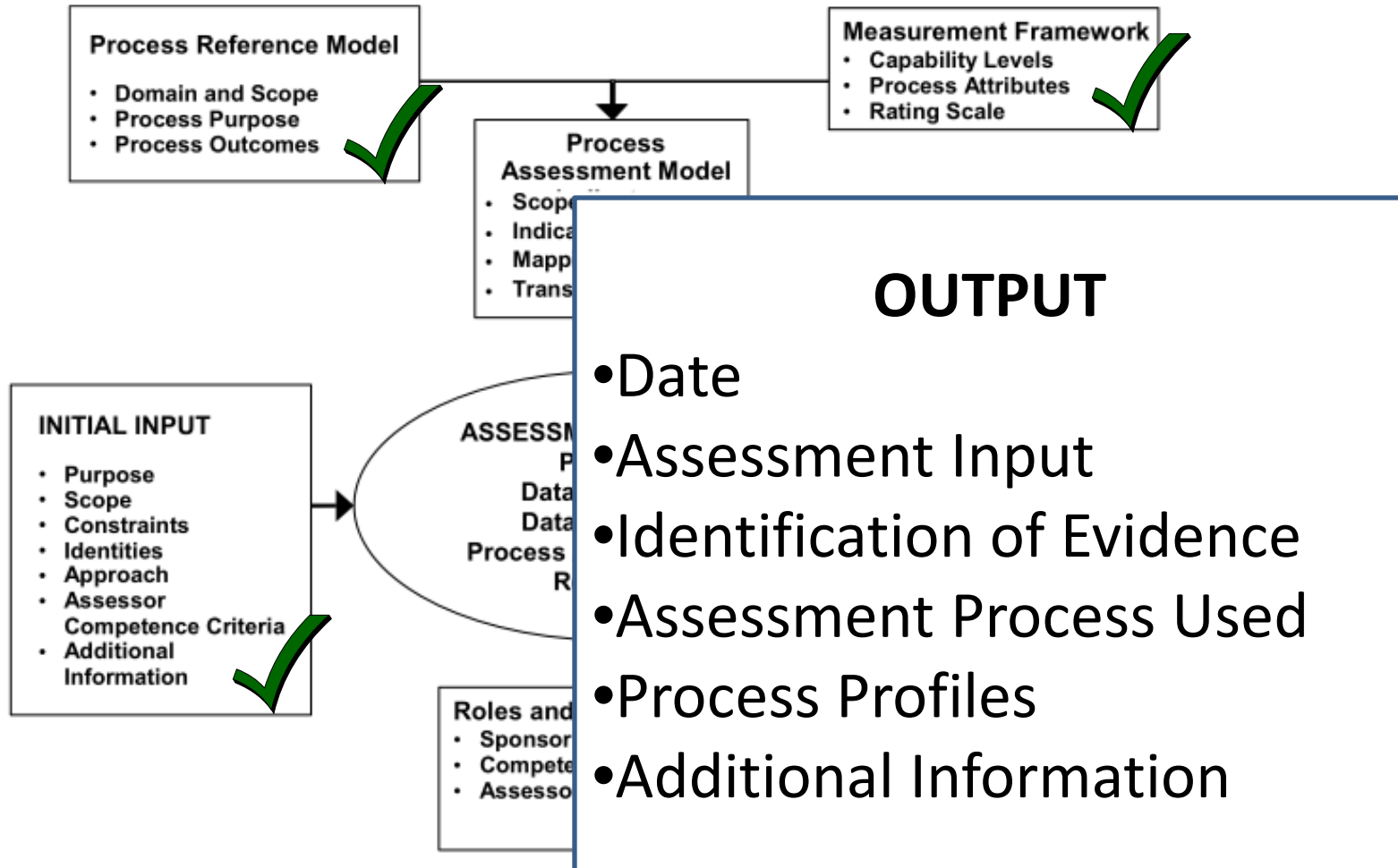
1. Initiation
2. Planning the assessment
3. Briefing
4. Data collection
5. Data validation
6. Process attributes rating
7. Reporting the results



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



A Process Capability Profile

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	
Processes Assessed	False if Process Capability is Level 1 or Better	Process Performance (PA 1.1)	Performance management (PA2.1)	Work Product Management (PA2.2)	Definition (PA3.1)	Deployment (PA3.2)	Measurement (PA4.1)	Control (PA4.2)	Innovation (PA5.1)	Optimization (PA5.2)
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

Consequence of Capability Gaps

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

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

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

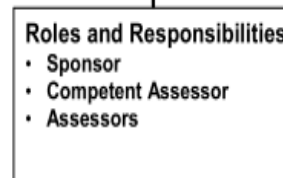
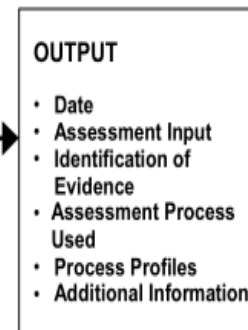
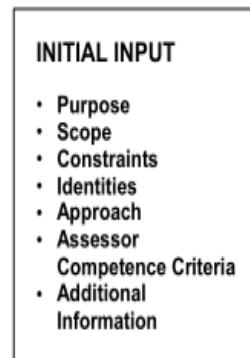
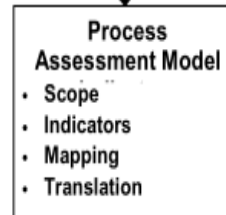
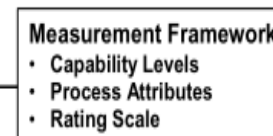
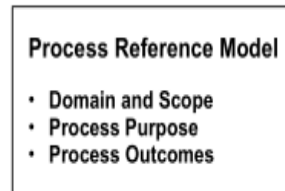
Risk from Capability Gaps

Figure A.4—Risk Associated With Each Capability Level

Consequence <i>indicated by capability level where gap occurs</i>	Probability <i>indicated by extent of capability level gap</i>		
	Slight	Significant	Substantial
5 – Optimizing process	Low Risk	Low Risk	Low Risk
4 – Predictable process	Low Risk	Low Risk	Medium Risk
3 – Established process	Low Risk	Medium Risk	Medium Risk
2 – Managed process	Medium Risk	Medium Risk	High Risk
1 – Performed process	Medium Risk	High Risk	High Risk

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

Summary



Process Capability Level (based on attributes) =>	Capability Level 1: Incomplete	Capability Level 2: Performed	Capability Level 3: Managed	Capability Level 4: Established	Capability Level 5: Predictable	Capability Level 6: Optimizing
Processes Assessed	False if Process Capability is Level 1 or Better	Process Performance management (PA1.1)	Work Product Management (PA2.1)	Definition Deployment (PA3.1)	Measurement Control (PA4.1)	Innovation Optimization (PA5.1)
CO1: Define and Manage Service Levels	FALSE	40%	20%	20%	20%	N/A
CO2: Manage Third Party Services	FALSE	30%	20%	20%	20%	N/A
CO3: Ensure Continuity Service	FALSE	10%	20%	20%	20%	N/A
CO4: Ensure Systems Security	FALSE	10%	20%	20%	20%	N/A
CO5: Manage Service Desk and Incidents	FALSE	10%	20%	20%	20%	N/A
CO6: Manage the Configuration	FALSE	10%	20%	20%	20%	N/A
CO7: Manage Data	FALSE	10%	20%	20%	20%	N/A
CO8: Monitor and Evaluate Internal Control	FALSE	10%	20%	20%	20%	N/A
CO9: Ensure Compliance with External Requirements	FALSE	10%	20%	20%	20%	N/A



Contact Information:

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

Questions?