BCNET

Shared IT Services for Higher Education & Research

Conference 2018

Using COBIT 5 Framework for Cybersecurity Assessment

Hugh Burley, Trevor Hurst, and Ivor MacKay

Speakers

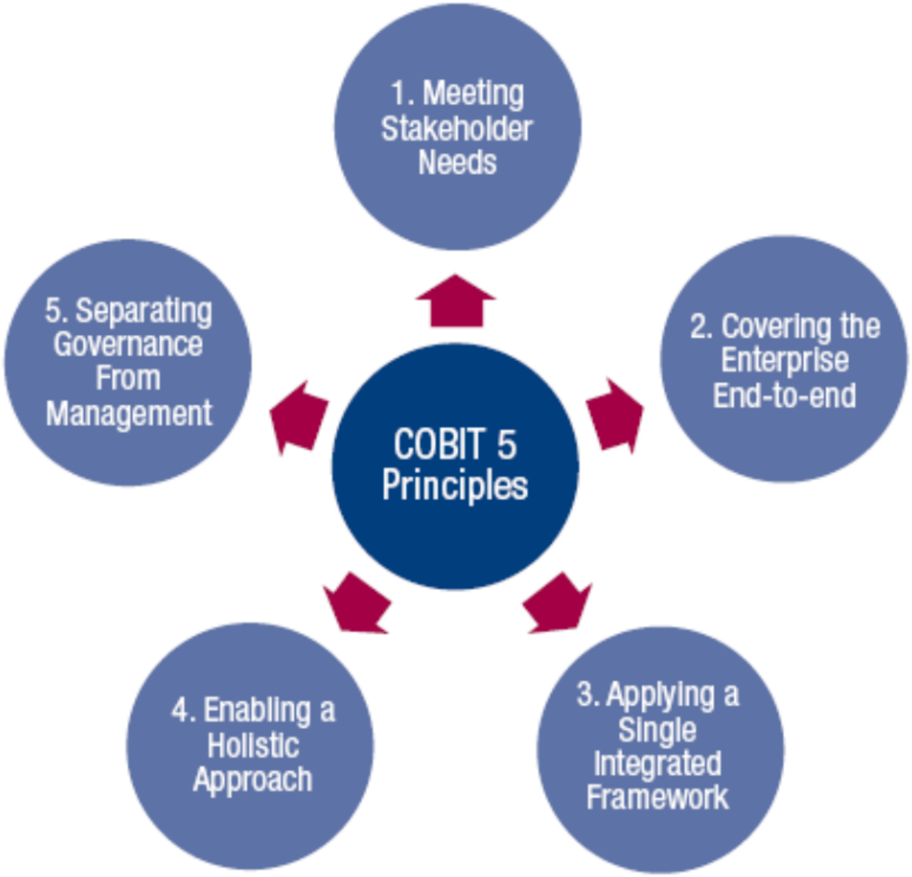
Trevor Hurst,	Chief Information Officer Ministry of Advanced Education, Skills & Training
Hugh Burley,	Manager of Information Security/Information Security Officer Thompson Rivers University/BCNET
Ivor MacKay,	Manager, Information Technology BCNET

Agenda

1. COBIT 5 Refresher
2. Why COBIT 5
3. Assessments
4. Q & A

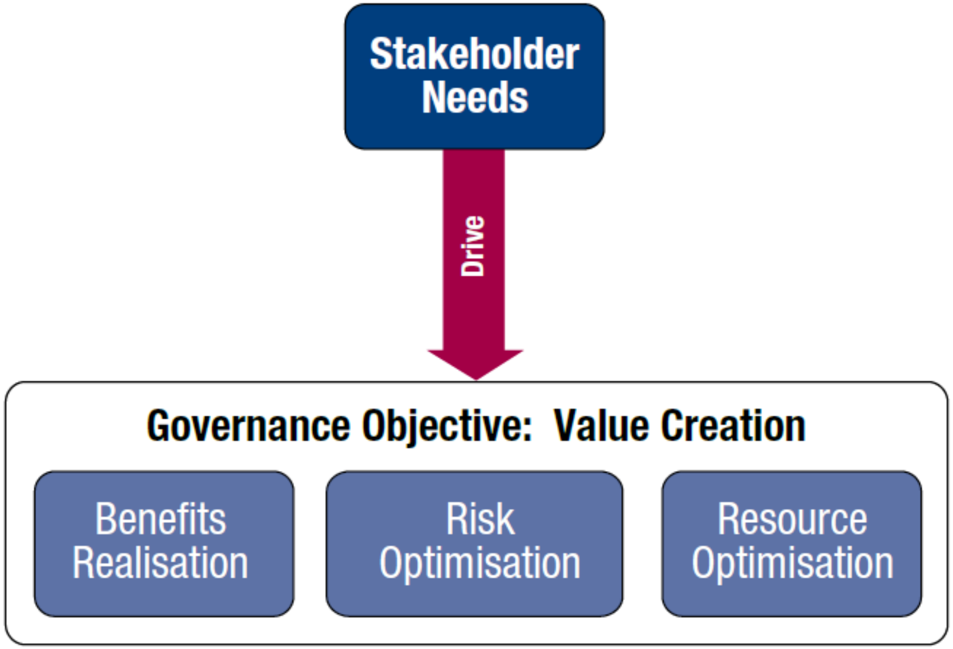
COBIT 5 Refresher

COBIT PRINCIPLES

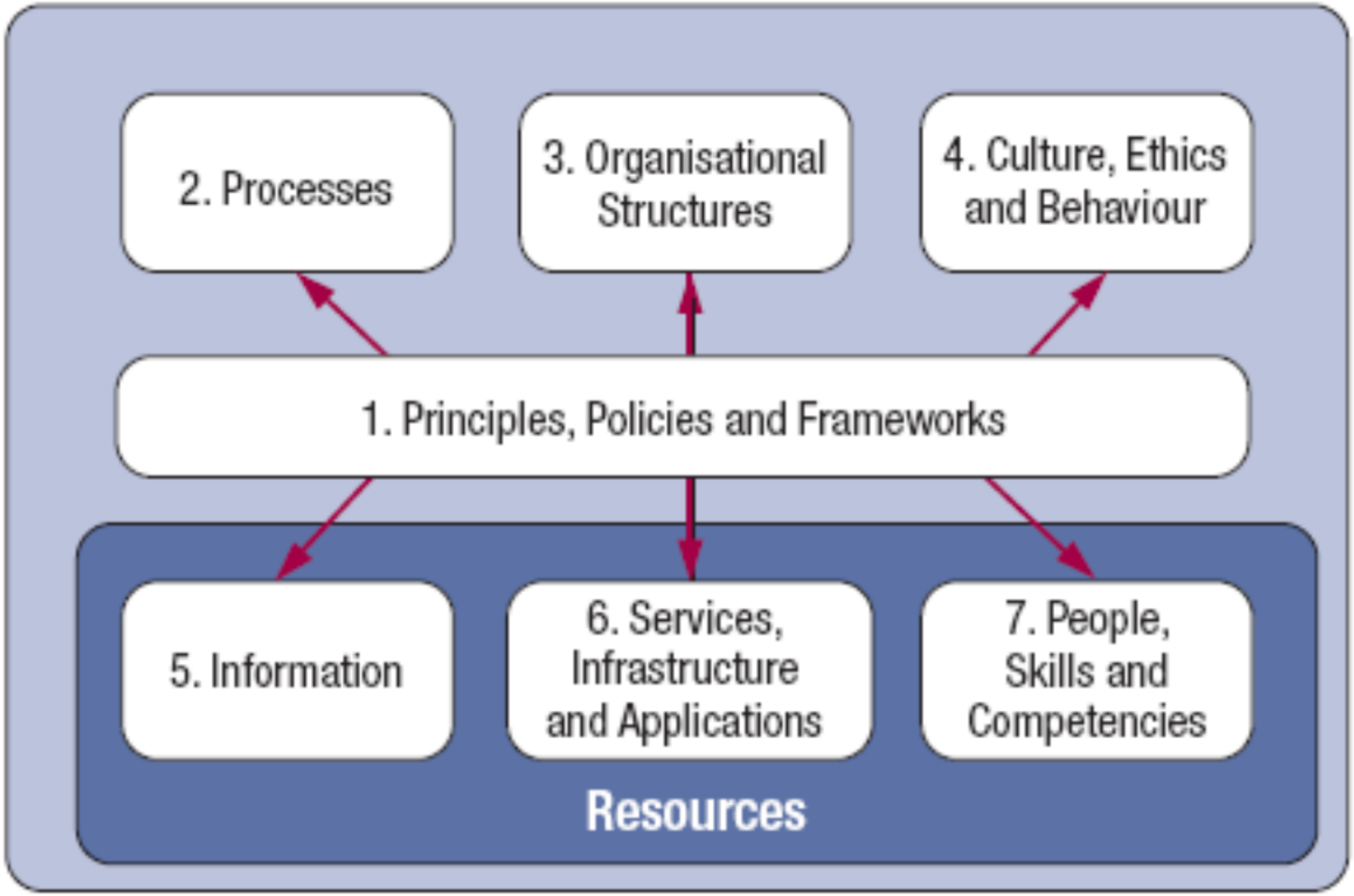

1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management
COBIT 5 Principles

Meeting Stakeholder Needs

Figure 3—The Governance Objective: Value Creation



COBIT 5 ENABLERS



2. Processes

3. Organisational Structures

4. Culture, Ethics and Behaviour

1. Principles, Policies and Frameworks

5. Information

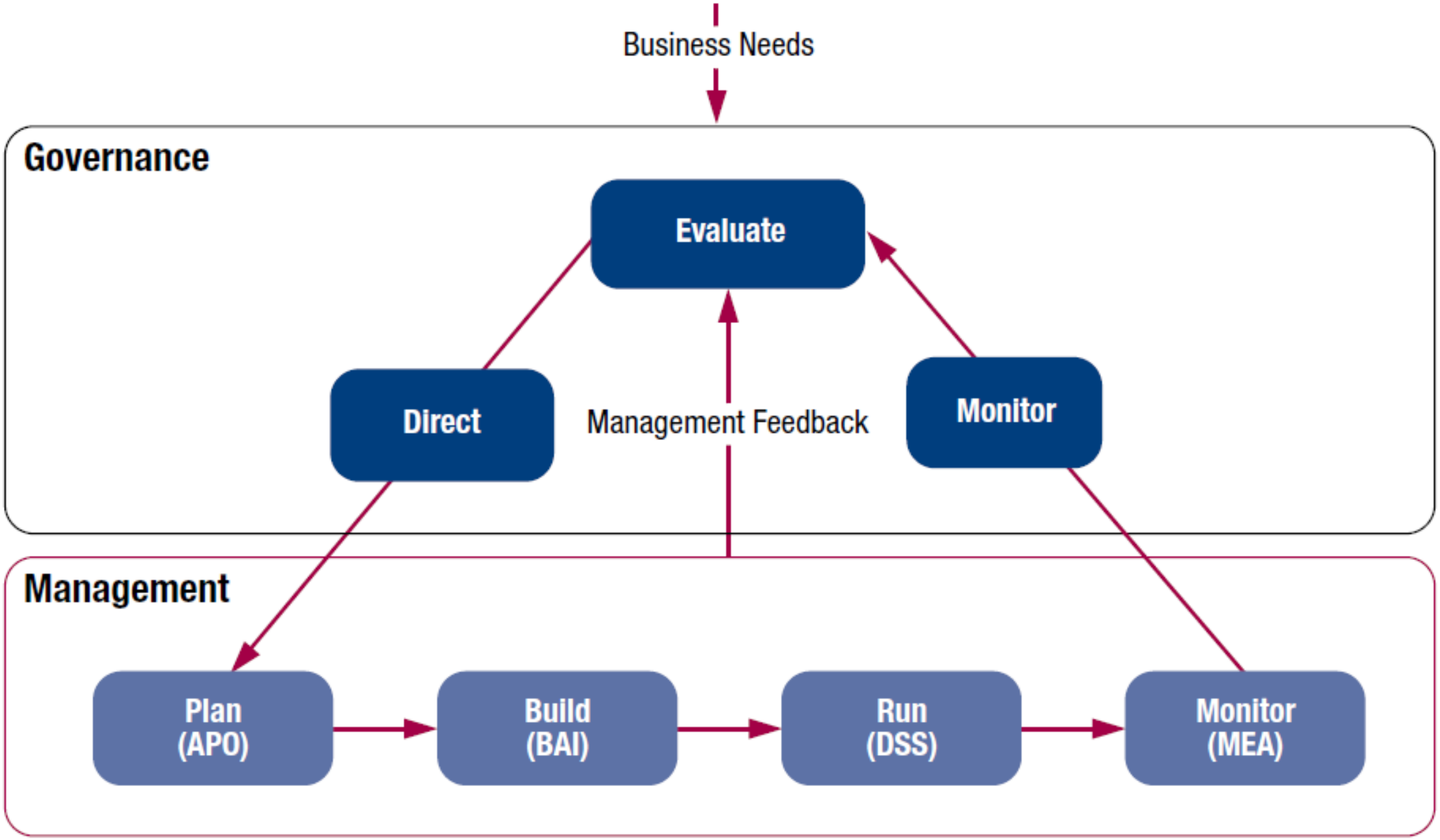
6. Services, Infrastructure and Applications

7. People, Skills and Competencies

Resources

GOVERNANCE VS MANAGEMENT

Figure 15—COBIT 5 Governance and Management Key Areas



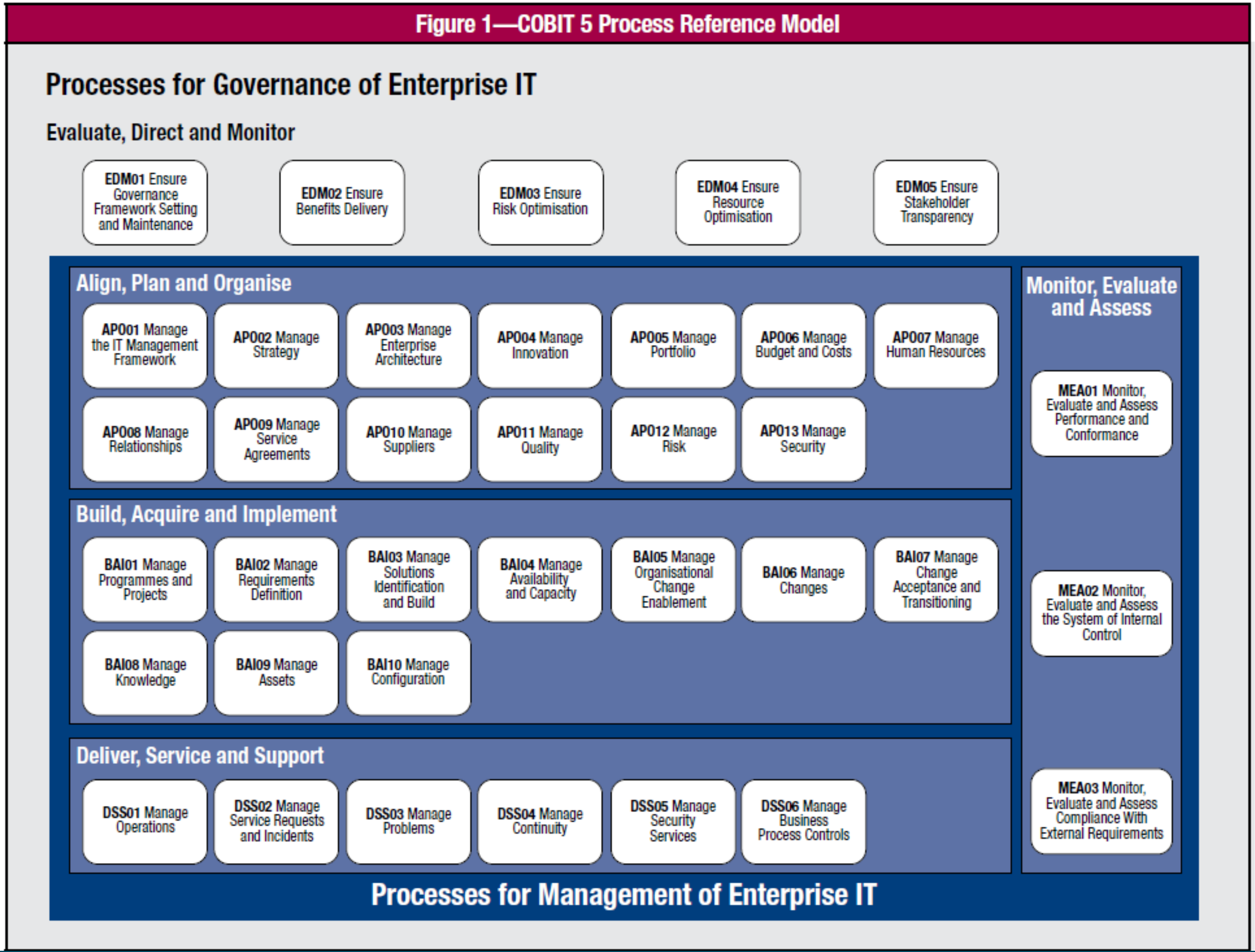


Figure 1—COBIT 5 Process Reference Model

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

- **APO01** Manage the IT Management Framework
- **APO02** Manage Strategy
- **APO03** Manage Enterprise Architecture
- **APO04** Manage Innovation
- **APO05** Manage Portfolio
- **APO06** Manage Budget and Costs
- **APO07** Manage Human Resources
- **APO08** Manage Relationships
- **APO09** Manage Service Agreements
- **APO10** Manage Suppliers
- **APO11** Manage Quality
- **APO12** Manage Risk
- **APO13** 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 Configuration

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

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

Why COBIT 5?

Alignment

“How do I ensure all of our Digital investments contribute to Stakeholder Value and enable the strategy of my Institution?

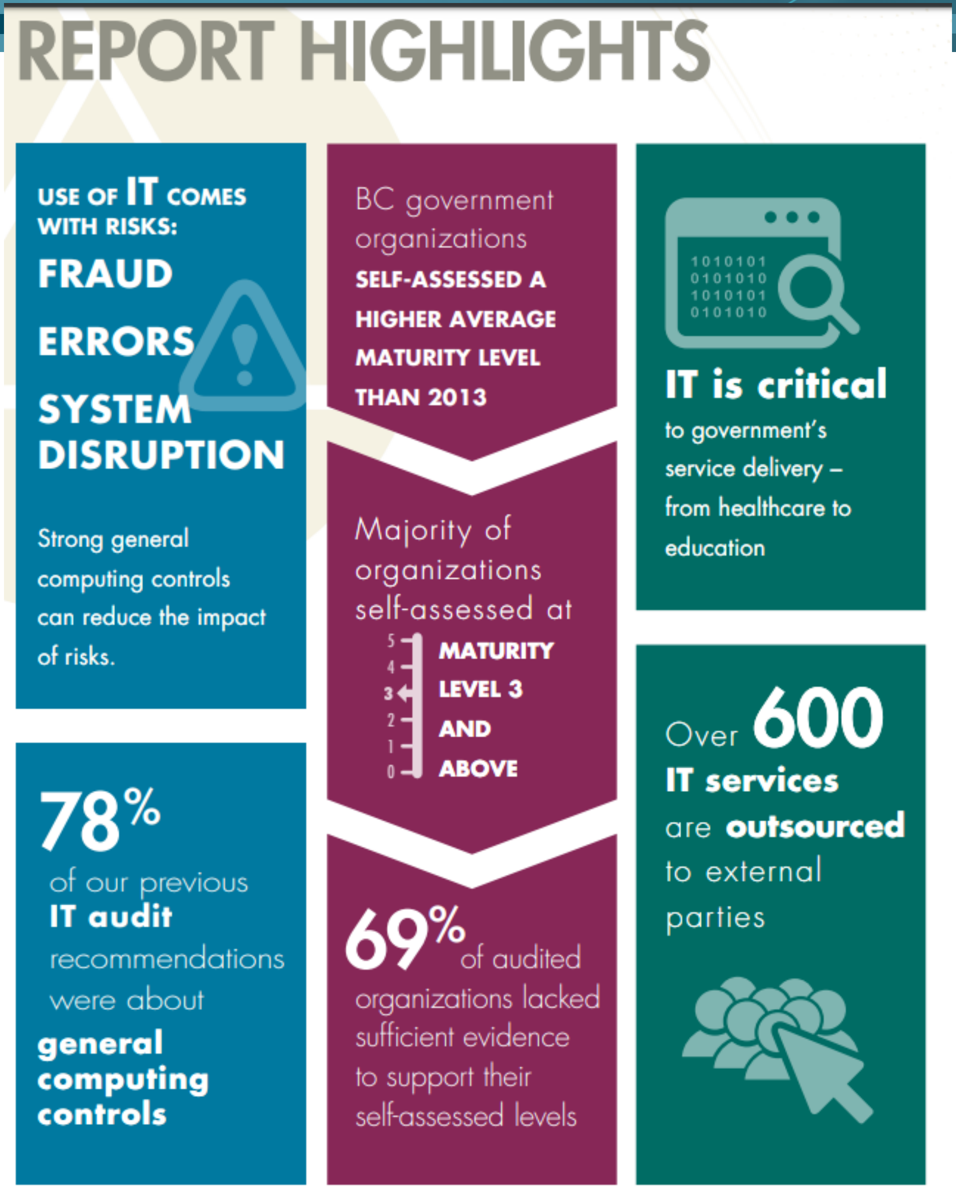
Tell a better story (funding)

“How do I better communicate the gaps in our environment and achieve better funding?

Audit preparation (Risk Management)

“How do I ensure benefits are realized and IT risks are mitigated? How can I prepare for upcoming Audit and/or review activity?

OAGBC General Computing Controls Report



REPORT HIGHLIGHTS

USE OF IT COMES WITH RISKS:
FRAUD
ERRORS
SYSTEM DISRUPTION

Strong general computing controls can reduce the impact of risks.

78% of our previous **IT audit** recommendations were about **general computing controls**

BC government organizations **SELF-ASSESSED A HIGHER AVERAGE MATURITY LEVEL THAN 2013**

Majority of organizations self-assessed at **MATURITY LEVEL 3 AND ABOVE**

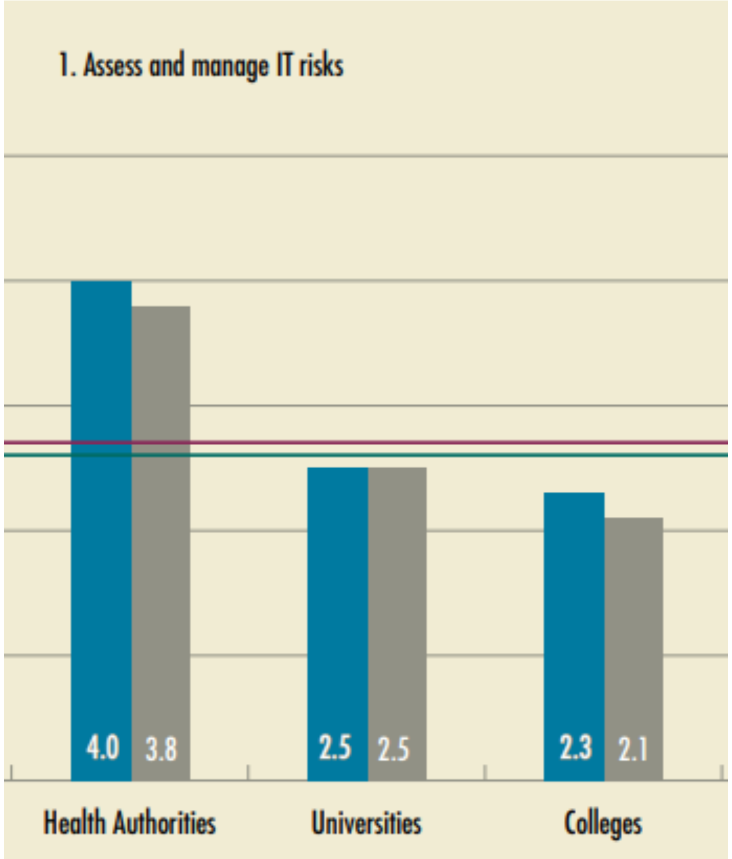
69% of audited organizations lacked sufficient evidence to support their self-assessed levels

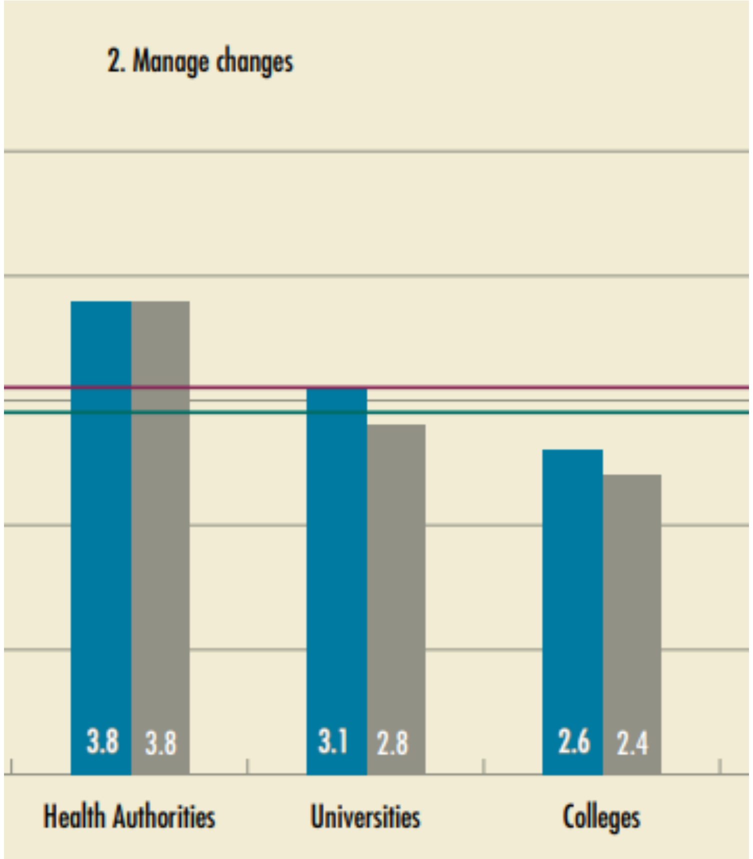
IT is critical to government's service delivery – from healthcare to education

Over **600 IT services** are **outsourced** to external parties

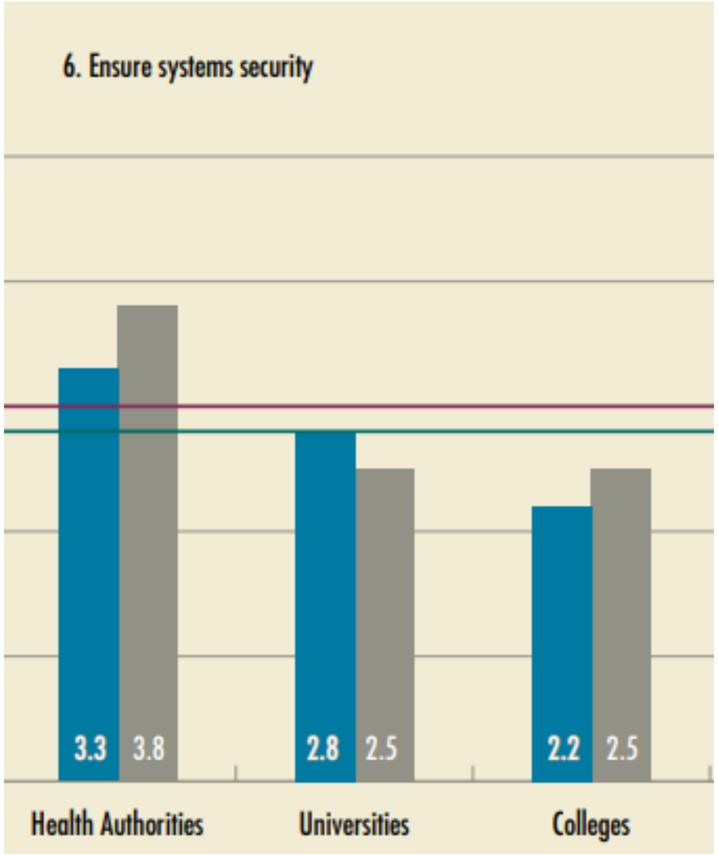
http://www.bcauditor.com/sites/default/files/publications/reports/OAGBC%20General%20Computing%20Controls%20Report_FINAL.pdf

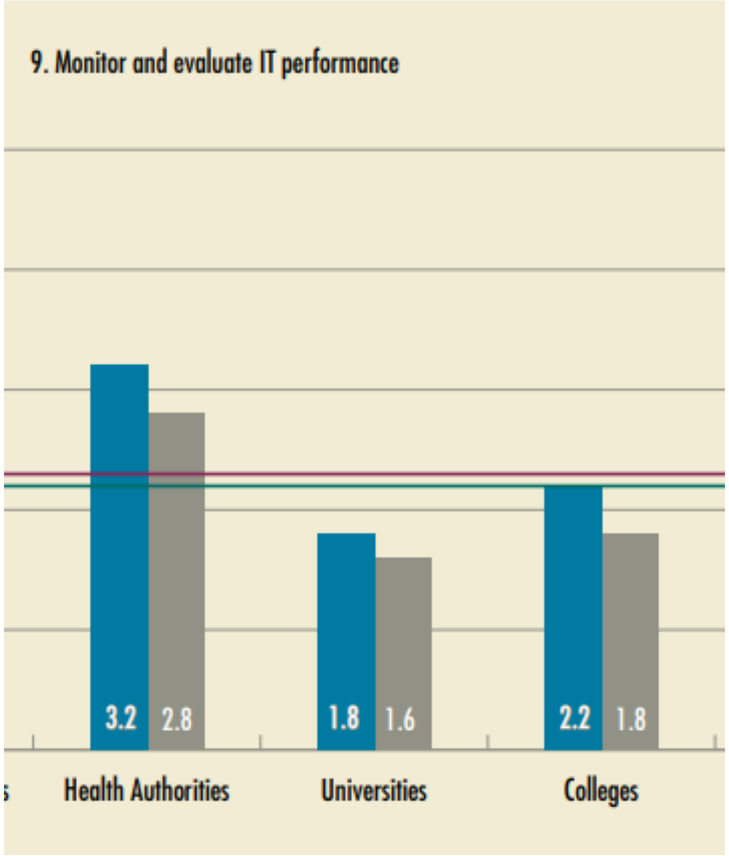
COBIT Maturity





COBIT Maturity





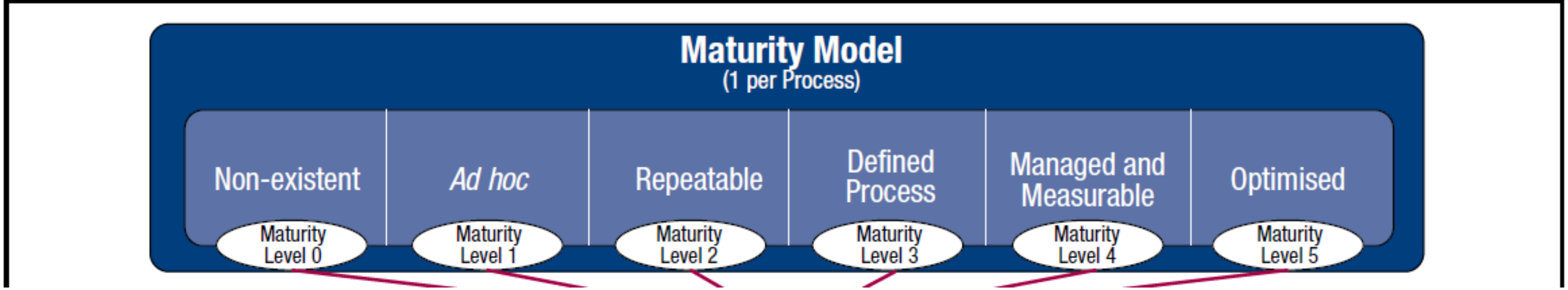
Assessments

Assessment vs Audit

Or is it really Gap Analysis vs. Internal Audit vs. Pre-Assessment

Differences Between the COBIT 4.1 and the COBIT 5

Figure 18—Summary of the COBIT 4.1 Maturity Model



Maturity Model
(1 per Process)

Non-existent — Maturity Level 0

Ad hoc — Maturity Level 1

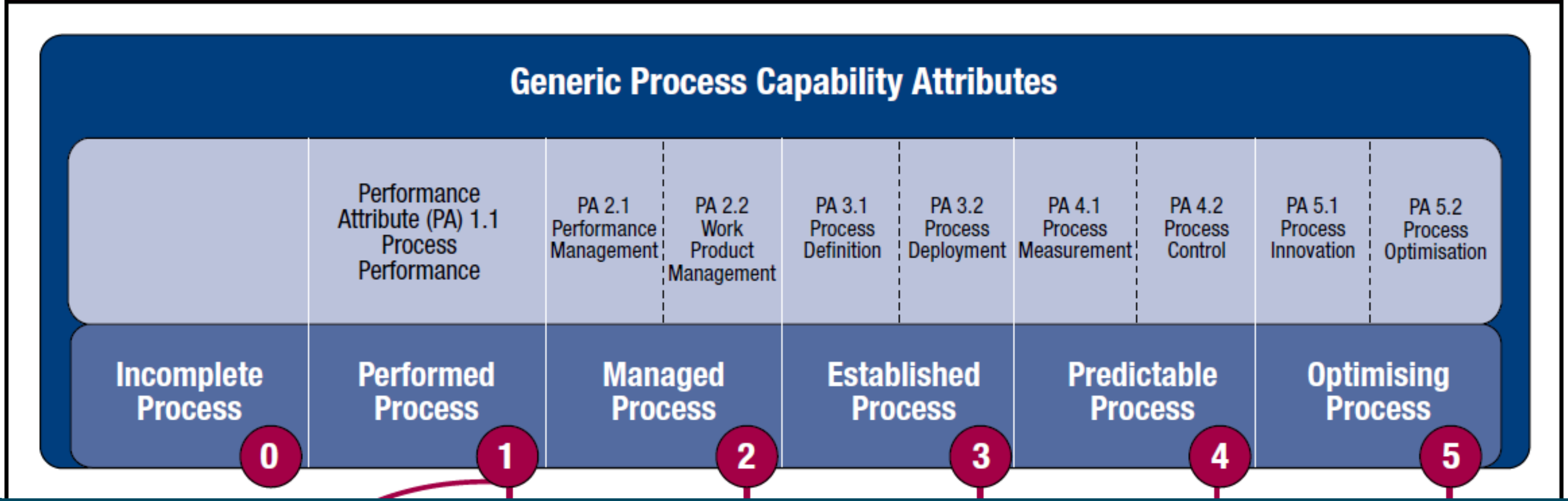
Repeatable — Maturity Level 2

Defined Process — Maturity Level 3

Managed and Measurable — Maturity Level 4

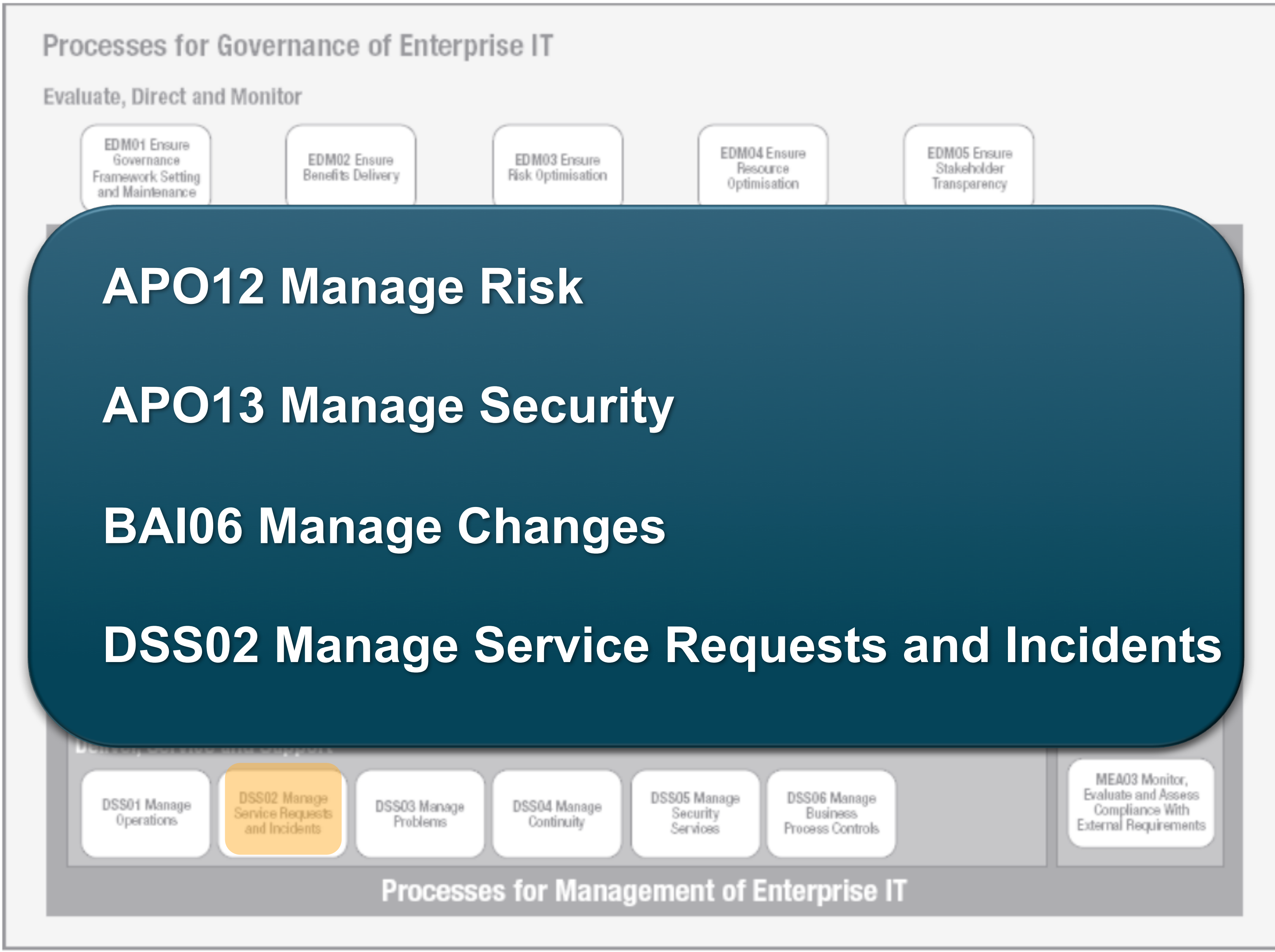
Optimised — Maturity Level 5

Figure 19—Summary of the COBIT 5 Process Capability Model



Generic Process Capability Attributes

Incomplete Process 0	Performed Process 1	Managed Process 2		Established Process 3		Predictable Process 4		Optimising Process 5	
	Performance Attribute (PA) 1.1 Process Performance	PA 2.1 Performance Management	PA 2.2 Work Product Management	PA 3.1 Process Definition	PA 3.2 Process Deployment	PA 4.1 Process Measurement	PA 4.2 Process Control	PA 5.1 Process Innovation	PA 5.2 Process Optimisation


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
DSS01 Manage Operations
DSS02 Manage Service Requests and Incidents
DSS03 Manage Problems
DSS04 Manage Continuity
DSS05 Manage Security Services
DSS06 Manage Business Process Controls
MEA03 Monitor, Evaluate and Assess Compliance With External Requirements
Processes for Management of Enterprise IT

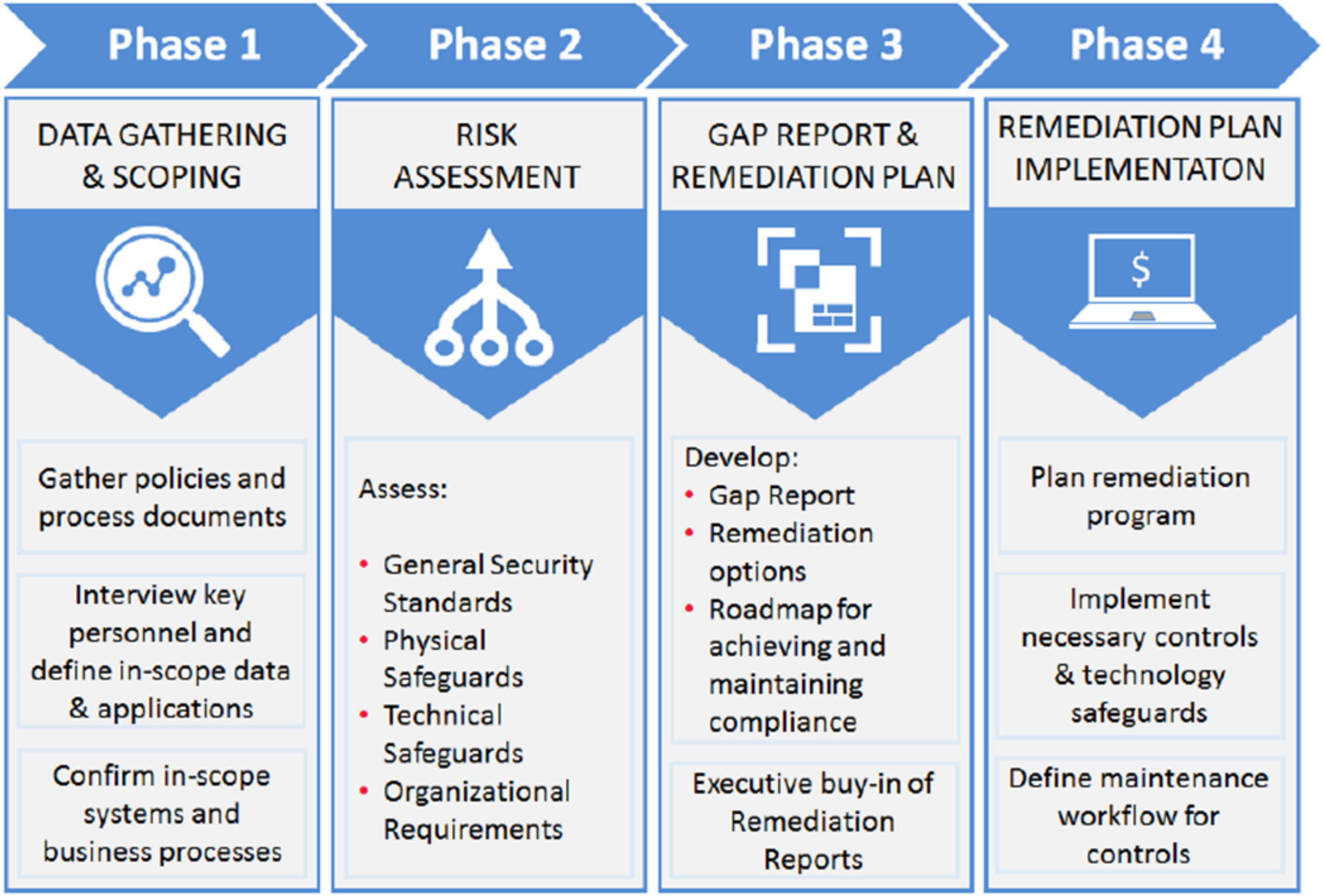
APO12 Manage Risk

APO13 Manage Security

BAI06 Manage Changes

DSS02 Manage Service Requests and Incidents

Assessment Methodology



Phase 1

DATA GATHERING & SCOPING

Gather policies and process documents

Interview key personnel and define in-scope data & applications

Confirm in-scope systems and business processes

Phase 2

RISK ASSESSMENT

Assess:

- General Security Standards
- Physical Safeguards
- Technical Safeguards
- Organizational Requirements

Phase 3

GAP REPORT & REMEDIATION PLAN

Develop:

- Gap Report
- Remediation options
- Roadmap for achieving and maintaining compliance

Executive buy-in of Remediation Reports

Phase 4

REMEDIATION PLAN IMPLEMENTATON

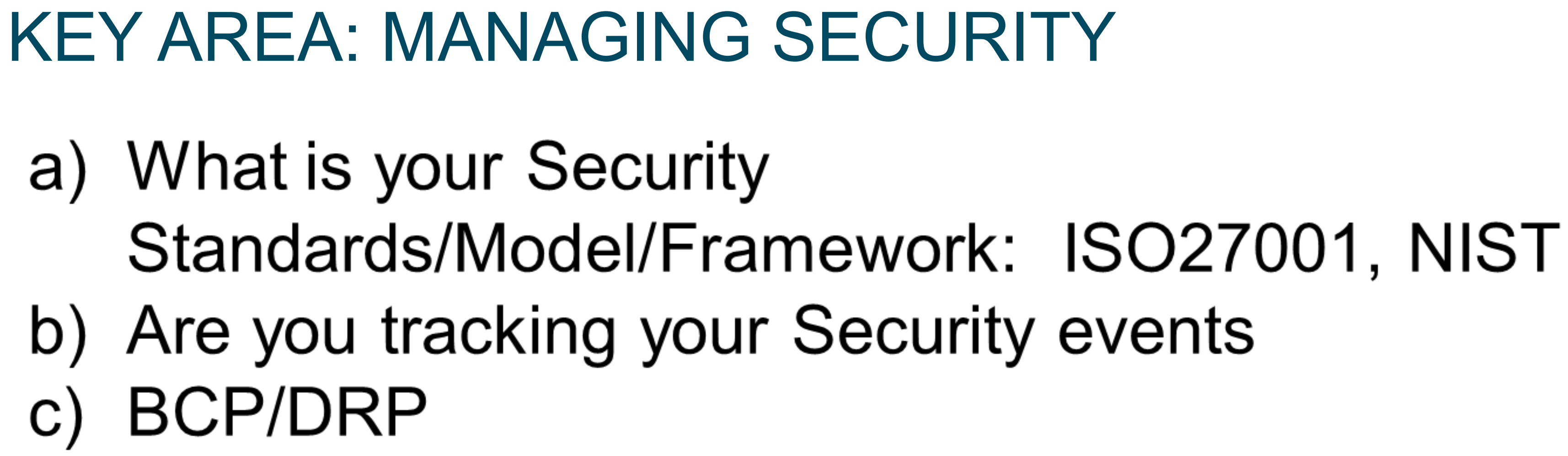
Plan remediation program

Implement necessary controls & technology safeguards

Define maintenance workflow for controls

KEY AREA: RISK

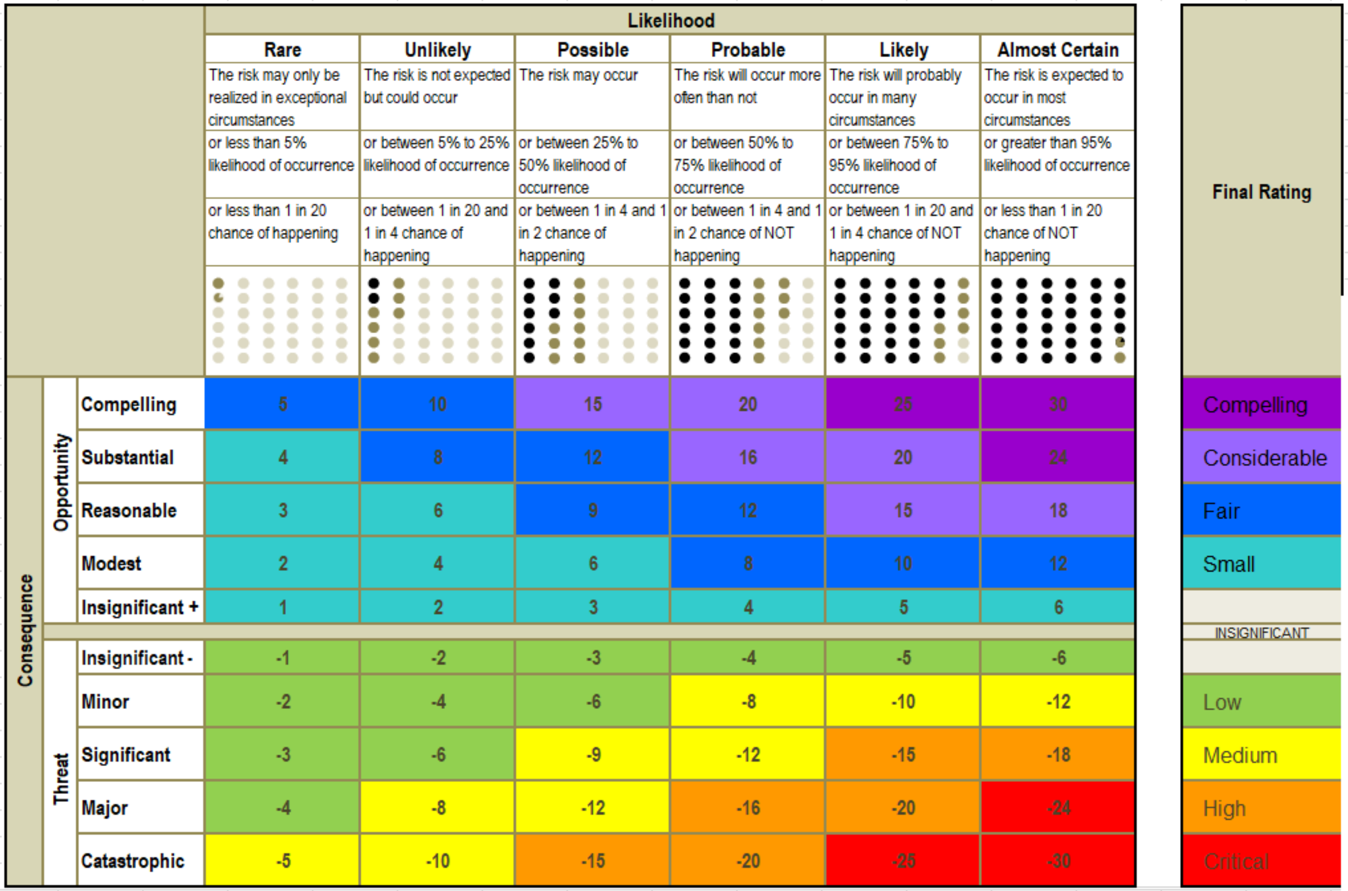
a) Level of risk acceptance
b) Risk review
c) Risk approval



KEY AREA: MANAGING SECURITY

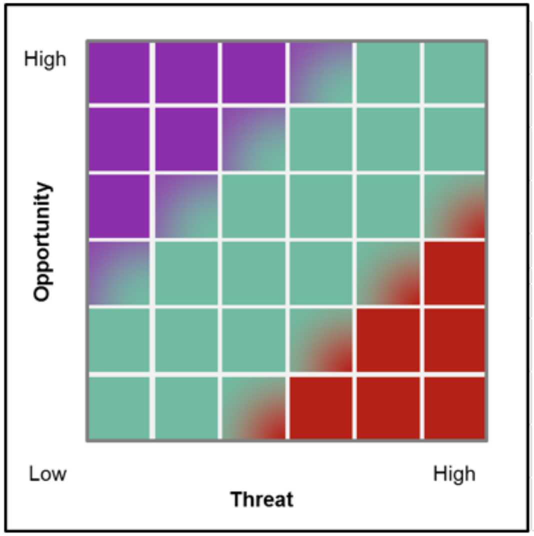
a) What is your Security Standards/Model/Framework: ISO27001, NIST
b) Are you tracking your Security events
c) BCP/DRP

Risk Assessment Consequence Table



			Likelihood						Final Rating
			Rare	Unlikely	Possible	Probable	Likely	Almost Certain	
			The risk may only be realized in exceptional circumstances	The risk is not expected but could occur	The risk may occur	The risk will occur more often than not	The risk will probably occur in many circumstances	The risk is expected to occur in most circumstances	
			or less than 5% likelihood of occurrence	or between 5% to 25% likelihood of occurrence	or between 25% to 50% likelihood of occurrence	or between 50% to 75% likelihood of occurrence	or between 75% to 95% likelihood of occurrence	or greater than 95% likelihood of occurrence	
			or less than 1 in 20 chance of happening	or between 1 in 20 and 1 in 4 chance of happening	or between 1 in 4 and 1 in 2 chance of happening	or between 1 in 4 and 1 in 2 chance of NOT happening	or between 1 in 20 and 1 in 4 chance of NOT happening	or less than 1 in 20 chance of NOT happening	
Consequence	Opportunity	Compelling	5	10	15	20	25	30	Compelling
		Substantial	4	8	12	16	20	24	Considerable
		Reasonable	3	6	9	12	15	18	Fair
		Modest	2	4	6	8	10	12	Small
		Insignificant +	1	2	3	4	5	6	
									INSIGNIFICANT
	Threat	Insignificant -	-1	-2	-3	-4	-5	-6	
		Minor	-2	-4	-6	-8	-10	-12	Low
		Significant	-3	-6	-9	-12	-15	-18	Medium
		Major	-4	-8	-12	-16	-20	-24	High
		Catastrophic	-5	-10	-15	-20	-25	-30	Critical

Threat / Opportunity Matrix



KEY AREA: MANAGING CHANGE

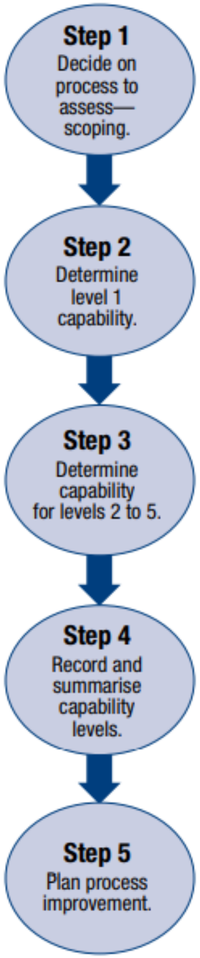
a) Methods of assessing change and its risks
b) Approval process

KEY AREA: MANAGE SERVICE REQUESTS AND INCIDENTS

a) Problem tracking
b) Evidence of reviewing Incidents and Requests

Self-Assessment

Figure 6–Self-assessment Process



Step 1
Decide on process to assess—scoping.

Step 2
Determine level 1 capability.

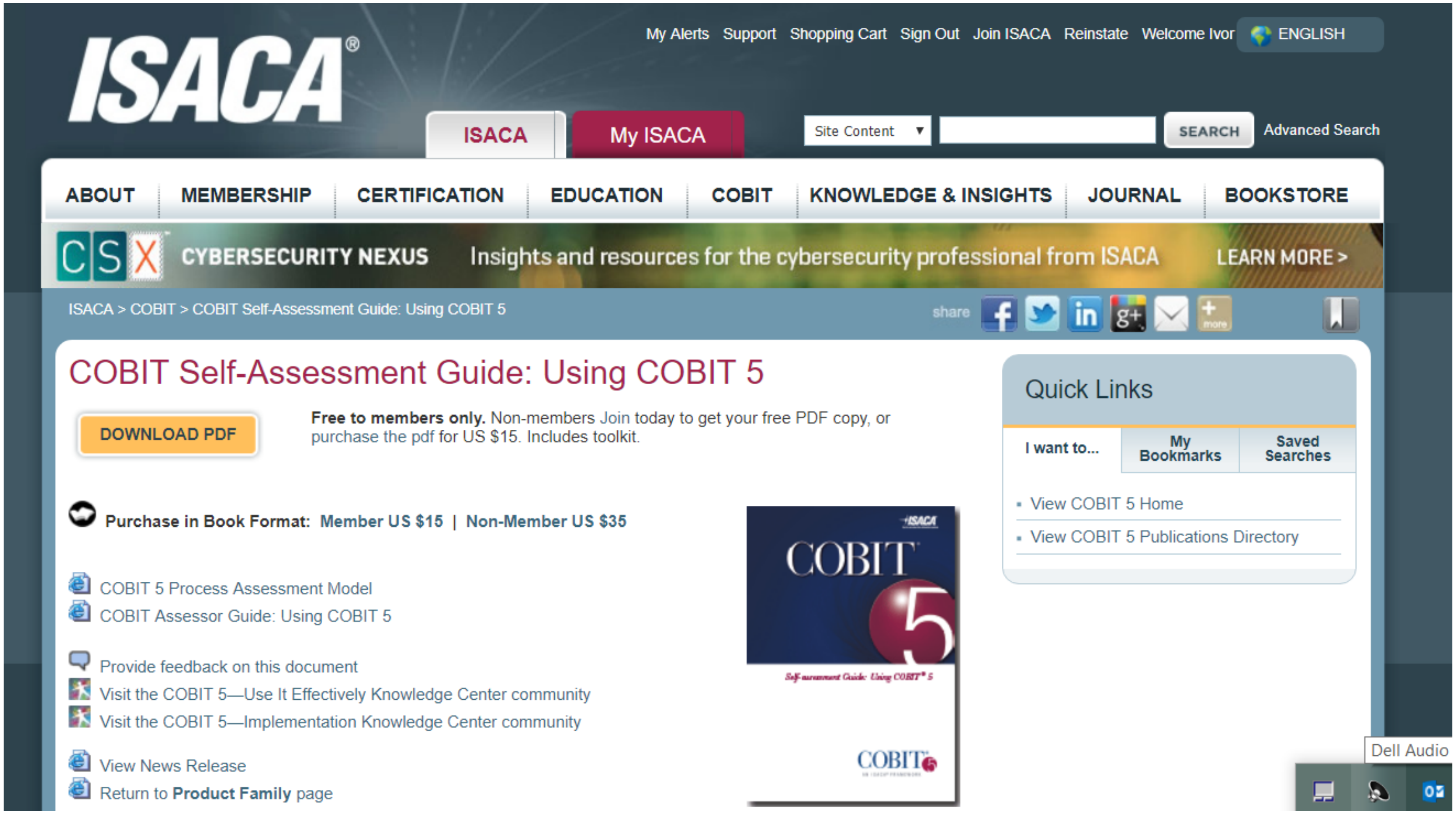
Step 3
Determine capability for levels 2 to 5.

Step 4
Record and summarise capability levels.

Step 5
Plan process improvement.

Self-Assessment

http://www.isaca.org/COBIT/Pages/Self-Assessment-Guide.aspx



ISACA
My Alerts Support Shopping Cart Sign Out Join ISACA Reinstate Welcome Ivor ENGLISH
ISACA
My ISACA
Site Content
SEARCH
Advanced Search
ABOUT MEMBERSHIP CERTIFICATION EDUCATION COBIT KNOWLEDGE & INSIGHTS JOURNAL BOOKSTORE
CSX CYBERSECURITY NEXUS Insights and resources for the cybersecurity professional from ISACA LEARN MORE >
ISACA > COBIT > COBIT Self-Assessment Guide: Using COBIT 5
share

COBIT Self-Assessment Guide: Using COBIT 5

DOWNLOAD PDF

Free to members only. Non-members Join today to get your free PDF copy, or purchase the pdf for US $15. Includes toolkit.

Purchase in Book Format: Member US $15 | Non-Member US $35

- COBIT 5 Process Assessment Model
- COBIT Assessor Guide: Using COBIT 5
- Provide feedback on this document
- Visit the COBIT 5—Use It Effectively Knowledge Center community
- Visit the COBIT 5—Implementation Knowledge Center community
- View News Release
- Return to **Product Family** page

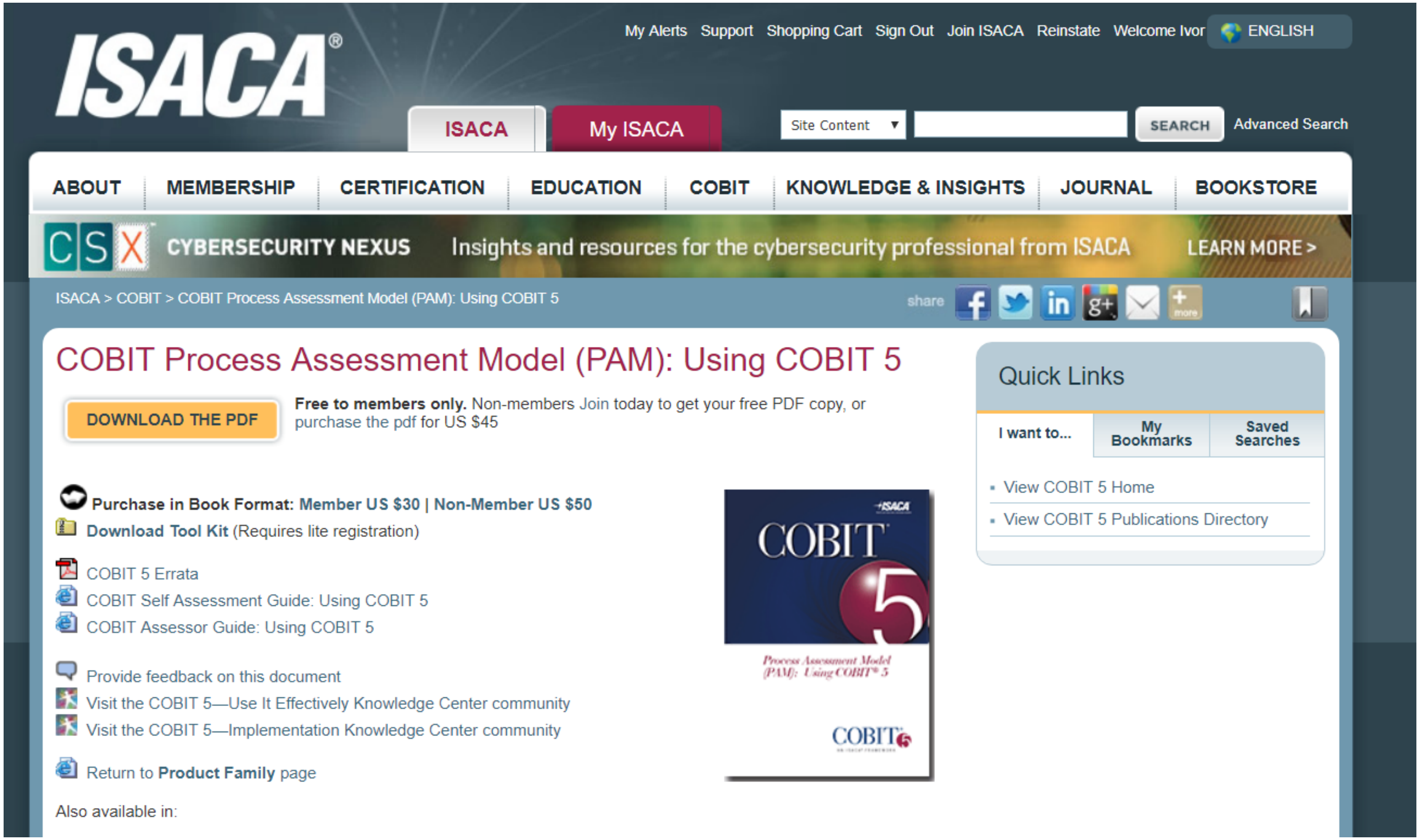
Quick Links

I want to...	My Bookmarks	Saved Searches

- View COBIT 5 Home
- View COBIT 5 Publications Directory

Self-Assessment

http://www.isaca.org/COBIT/Pages/COBIT-5-PAM.aspx



My Alerts Support Shopping Cart Sign Out Join ISACA Reinstate Welcome Ivor ENGLISH
ISACA
ISACA
My ISACA
Site Content
SEARCH
Advanced Search
ABOUT
MEMBERSHIP
CERTIFICATION
EDUCATION
COBIT
KNOWLEDGE & INSIGHTS
JOURNAL
BOOKSTORE
CSX CYBERSECURITY NEXUS Insights and resources for the cybersecurity professional from ISACA LEARN MORE >
ISACA > COBIT > COBIT Process Assessment Model (PAM): Using COBIT 5
share

COBIT Process Assessment Model (PAM): Using COBIT 5

DOWNLOAD THE PDF

Free to members only. Non-members Join today to get your free PDF copy, or purchase the pdf for US $45

Purchase in Book Format: **Member US $30 | Non-Member US $50**

Download Tool Kit (Requires lite registration)

COBIT 5 Errata

COBIT Self Assessment Guide: Using COBIT 5

COBIT Assessor Guide: Using COBIT 5

Provide feedback on this document

Visit the COBIT 5—Use It Effectively Knowledge Center community

Visit the COBIT 5—Implementation Knowledge Center community

Return to **Product Family** page

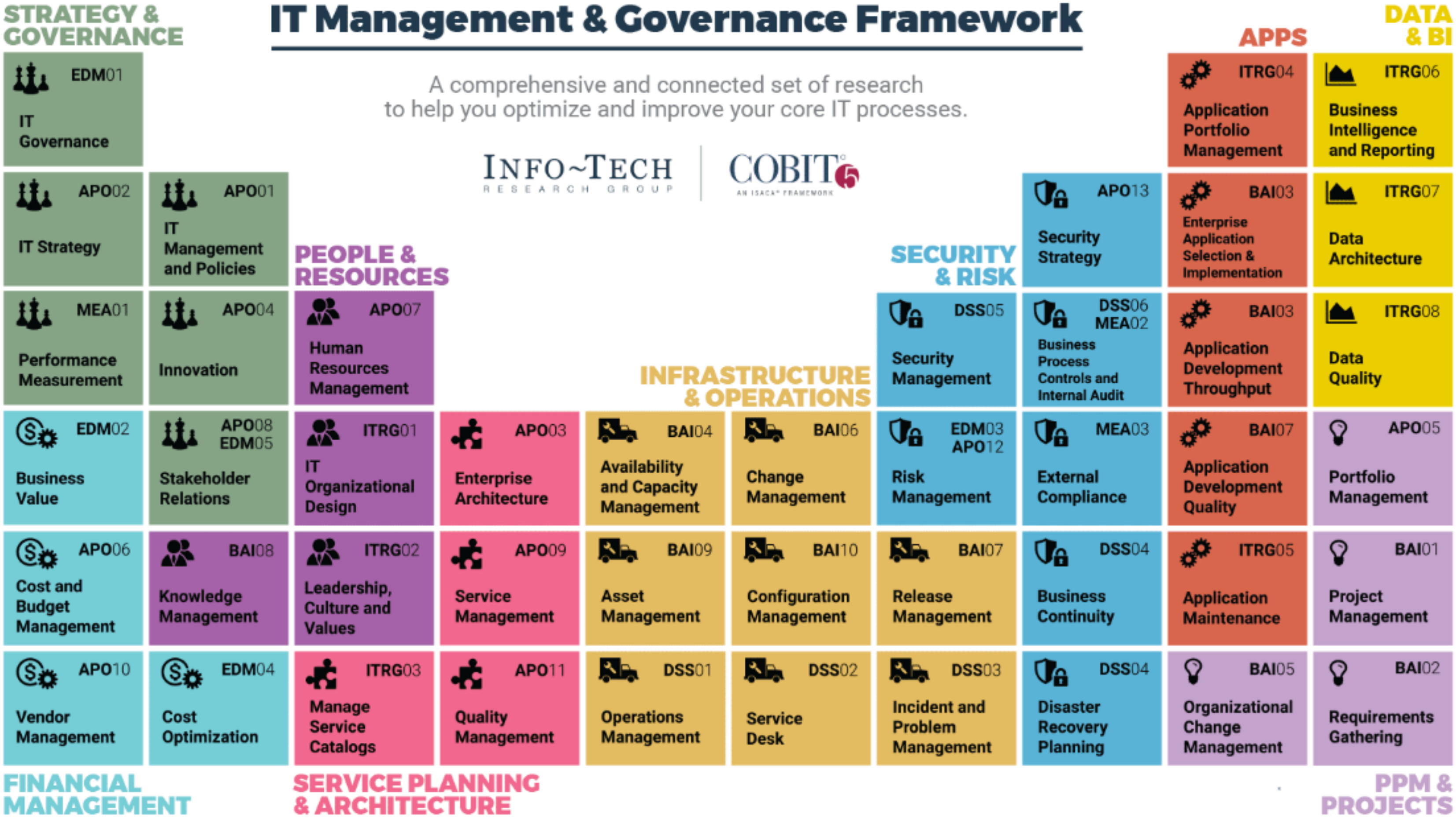
Also available in:

Quick Links

I want to... | My Bookmarks | Saved Searches

- View COBIT 5 Home
- View COBIT 5 Publications Directory

Info~Tech



IT Management & Governance Framework

A comprehensive and connected set of research
to help you optimize and improve your core IT processes.

INFO~TECH RESEARCH GROUP | COBIT 5 AN ISACA® FRAMEWORK

STRATEGY & GOVERNANCE								APPS	DATA & BI
EDM01 IT Governance								ITRG04 Application Portfolio Management	ITRG06 Business Intelligence and Reporting
APO02 IT Strategy	APO01 IT Management and Policies	PEOPLE & RESOURCES				SECURITY & RISK	APO13 Security Strategy	BAI03 Enterprise Application Selection & Implementation	ITRG07 Data Architecture
MEA01 Performance Measurement	APO04 Innovation	APO07 Human Resources Management		INFRASTRUCTURE & OPERATIONS		DSS05 Security Management	DSS06 MEA02 Business Process Controls and Internal Audit	BAI03 Application Development Throughput	ITRG08 Data Quality
EDM02 Business Value	APO08 EDM05 Stakeholder Relations	ITRG01 IT Organizational Design	APO03 Enterprise Architecture	BAI04 Availability and Capacity Management	BAI06 Change Management	EDM03 APO12 Risk Management	MEA03 External Compliance	BAI07 Application Development Quality	APO05 Portfolio Management
APO06 Cost and Budget Management	BAI08 Knowledge Management	ITRG02 Leadership, Culture and Values	APO09 Service Management	BAI09 Asset Management	BAI10 Configuration Management	BAI07 Release Management	DSS04 Business Continuity	ITRG05 Application Maintenance	BAI01 Project Management
APO10 Vendor Management	EDM04 Cost Optimization	ITRG03 Manage Service Catalogs	APO11 Quality Management	DSS01 Operations Management	DSS02 Service Desk	DSS03 Incident and Problem Management	DSS04 Disaster Recovery Planning	BAI05 Organizational Change Management	BAI02 Requirements Gathering
FINANCIAL MANAGEMENT		SERVICE PLANNING & ARCHITECTURE							PPM & PROJECTS