COBIT 2019 as EGIT Framework for Internal Control and Audit

Andrei Drozdov, KPMG Moscow, Associate Director, IT Advisory

CISA, CISM, CGEIT, COBIT 2019 Accredited Trainer

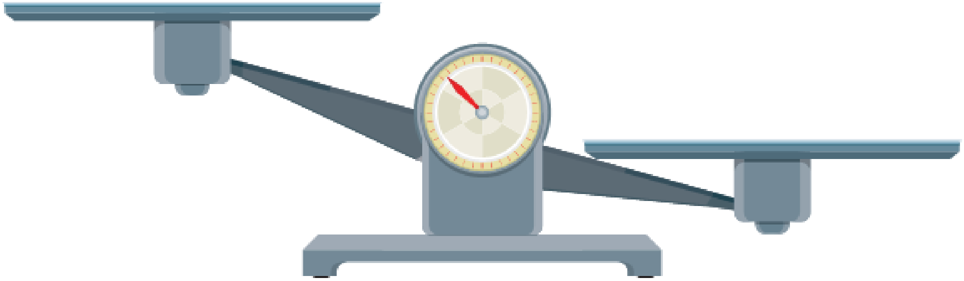
CONTROL ENVIRONMENT

- Includes three lines of defense (Operational Management, Risk & Compliance, Audit)
- Required by audit standards and Regulators, e.g. for financial sector
- IT-related Controls present in most of control environments
- Regulators mostly provide detailed specification only for security and privacy controls

ROLES OF INTERNAL AUDIT IN EGIT

Assurance on Conformance

Consulting on Performance



Normative requirements for control environment

Best practices to increase effectiveness and efficiency

ISACA

Trust in, and value from, information systems

protiviti

Face the Future with Confidence

Business and Digital Transformation's Effects on IT Audit Groups

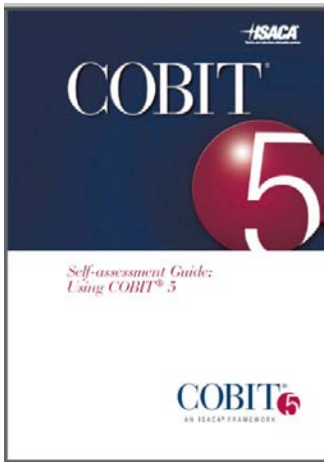
A Global Look at IT Audit Best Practices – Assessing the International Leaders in an Annual ISACA-Protiviti Survey

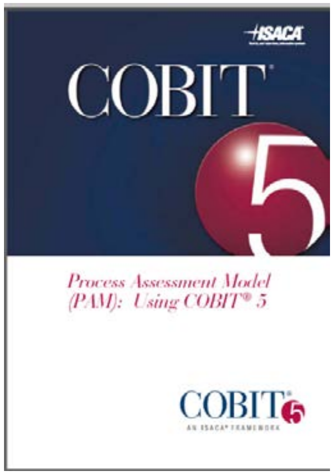
- ✓ Emerging technologies
- ✓ Digital transformation
- ✓ Security, Privacy, Compliance
- ✓ IT audit function in IA
- ✓ Shortage of skilled IT audit recourses
- ✓ COBIT is used in more than 50% organization as a framework for IT audit

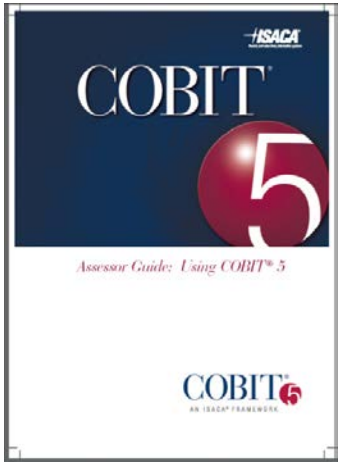
http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/a-global-look-at-it-audit-best-practices.aspx

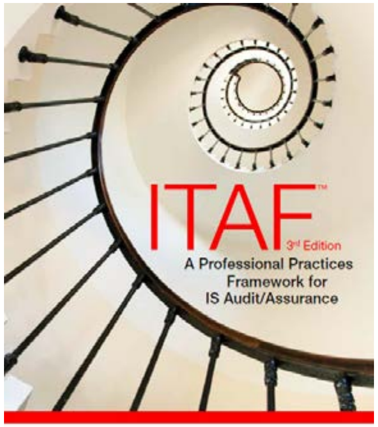
KPMG

ISACA IT AUDIT RELATED PUBLICATIONS

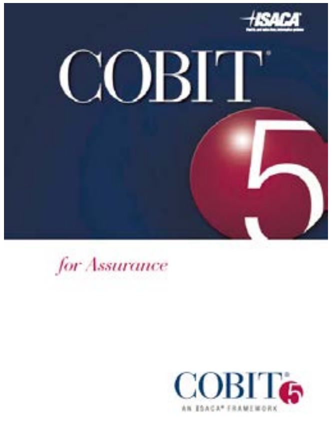








ISACA



2014
ISACA
Build, Acquire and Implement
BAI01 Manage Programmes and Projects
Audit/Assurance Program
COBIT 5

SOME ISSUES WITH COBIT 5

Developed 7 years ago, not cover new technology trends (e.g. digital transformation) and latest IT standards

Assessment of capability levels based on PAM (ISO 15504) is more complicated than CMMI model (used in COBIT 4.1) and could be even more sophisticated in case of adopting ISO 33001

COBIT 5 terminology sometimes is too difficult to understand (“enables”)

Lack of practices for “tailoring” EGIT model

A HISTORICAL TIMELINE

The COBIT® Framework

COBIT®2019

1996

ISACA released the first edition of COBIT framework.

1998

The debut of the second edition of COBIT added Control to its framework.

2000

A third edition of COBIT, with new Management Guidelines, was published.

2003

ISACA created an online version of the third edition of COBIT.

2005

COBIT 4.0 becomes the fourth edition in the COBIT series of releases.

2007

COBIT upgraded to version 4.1.

2012

COBIT 5 integrated the COBIT 4.1, Val IT 2.0 and Risk IT frameworks, and drew from ISACA's IT Assurance Framework (ITAF) and the Business Model for Information Security (BMIS). COBIT 5 also coordinated with frameworks and standards such as ITIL, ISO, PMBOK, PRINCE2 and TOGAF.

2018

ISACA publishes COBIT 2019, an update that adds design factors and focus areas to make it more practical and customizable.

1995
2000
2005
2010
2015

1995

Windows 95, Java, and HTML 2.0 (first formal html standard) debuted, as did Amazon.com, craigslist.com, match.com and ebay.com

1997

Original wireless LAN standard (IEEE 802.11) released, DVD technology appeared, and Google.com registered as domain—incorporating a year later and launching in 1999.

2001

Internet Archive "Wayback Machine" (archive.org) launched, Wikipedia started publishing, and Apple released iPod.

2002

U.S. Sarbanes-Oxley law revolutionized corporate recordkeeping and retention standards, leading to new IT regulatory requirements.

2003

Third WiFi standard created proliferation of "hotspots" as Skype, LinkedIn and WordPress started up. U.S. CAN-SPAM Act became law.

2006

Twitter founded and Google acquired YouTube.

2007

Apple iPhone signaled move to touchscreen devices; Apple App Store went online one year later.

2012

Worldwide e-commerce tops $1 trillion in sales.

2014

Internet of Things (IoT) technology standard ushered new wave of smart devices.

2016

ISACA acquired CMMI Institute and its business maturity and capability models, adding these resources to the ISACA/COBIT framework portfolio.

For more information, visit www.isaca.org/cobit

50 ISACA

COBIT 2019 FRAMEWORK

COBIT ® is a framework for the enterprise governance and management of information and technology (I&T) that supports enterprise goal achievement.

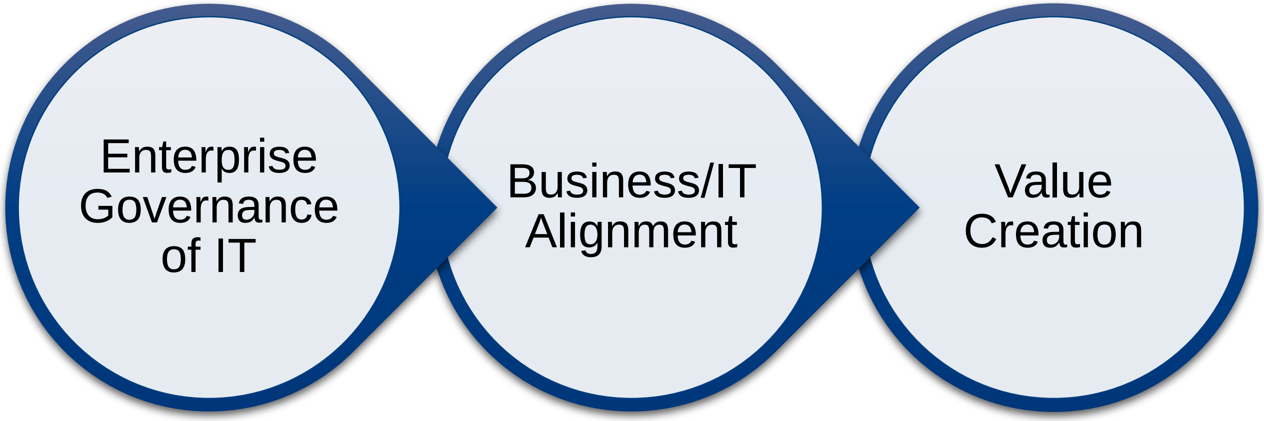
For each of 40 objectives provides detailed description of components (former 7 enables) including processes, practices, activities, metrics, organization structures (e.g. CDO), references to latest standards

COBIT 2019
FRAMEWORK
Governance and Management Objectives

COBIT 2019
FRAMEWORK
Introduction and Methodology

ENTERPRISE GOVERNANCE OF INFORMATION AND TECHNOLOGY

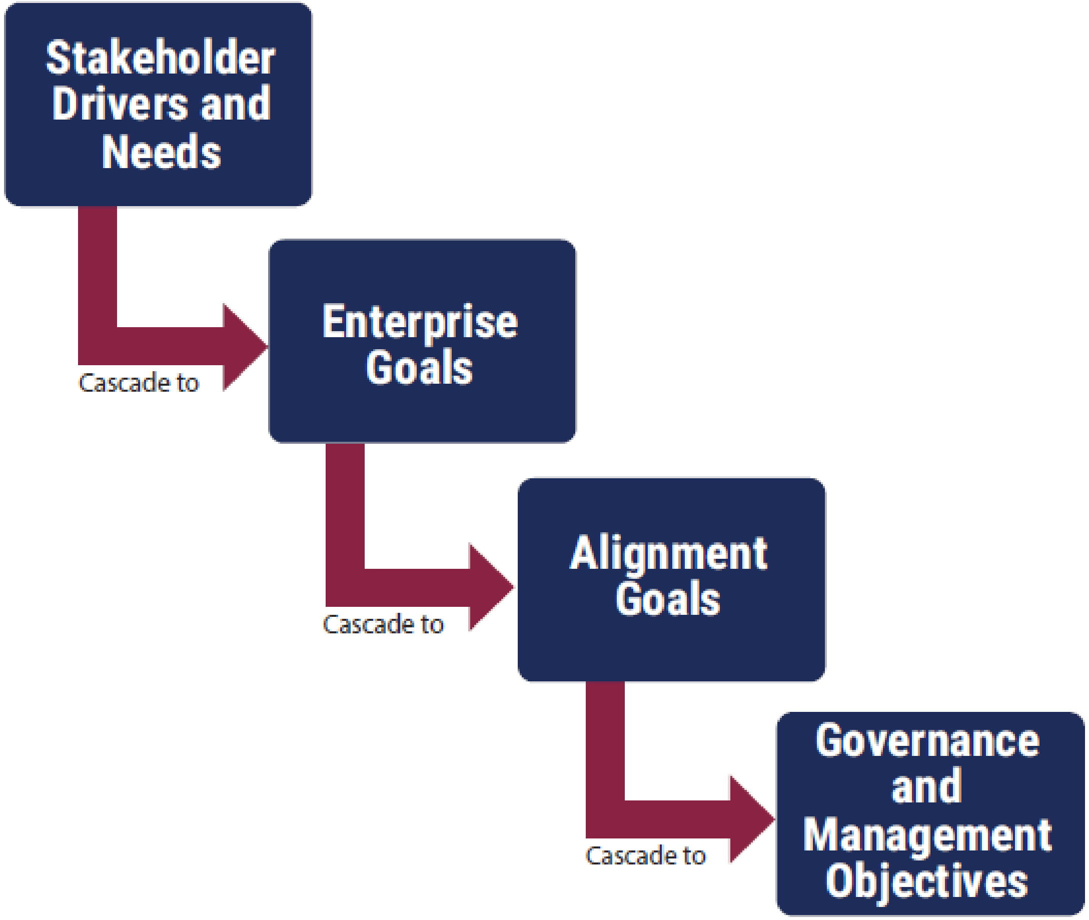
The context of Enterprise Governance of Information and Technology includes:



Good governance leads to alignment, which leads to value creation.

Reference: COBIT 2019 Framework: Introduction and Methodology Chapter 1 Introduction

GOALS CASCADE


Stakeholder Drivers and Needs
Cascade to
Enterprise Goals
Cascade to
Alignment Goals
Cascade to
Governance and Management Objectives

Reference: COBIT 2019 Framework: Basic Concepts: Governance Systems and Components, Chapter 4

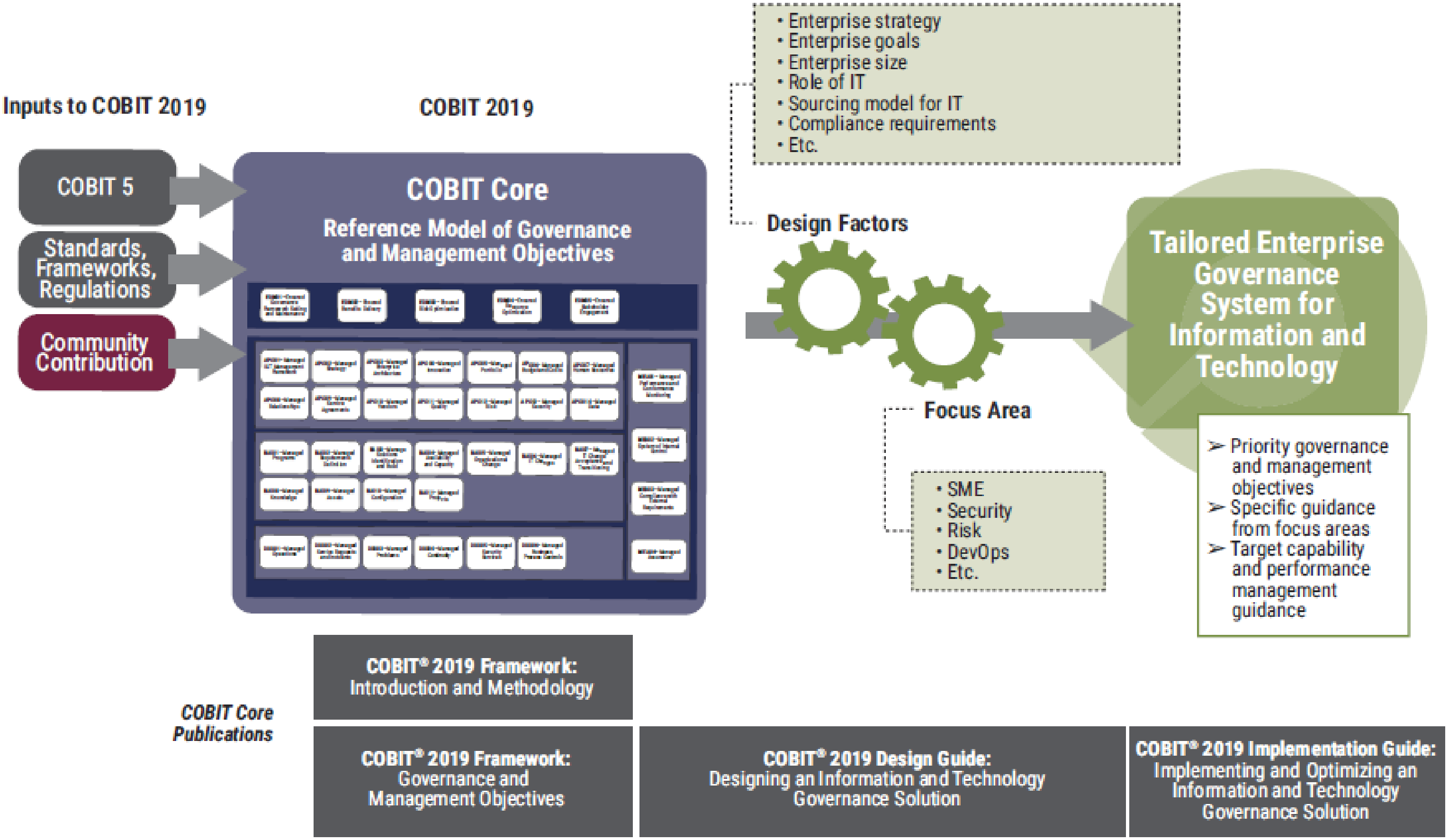
GOALS CASCADE –ENTERPRISE GOALS

REF	BSC DIMENSION	ENTERPRISE GOAL
EG01	Financial	Portfolio of competitive products and services
EG02	Financial	Managed business risk
EG03	Financial	Compliance with external laws and regulations
EG04	Financial	Quality of financial information
EG05	Customer	Customer-oriented service culture
EG06	Customer	Business service continuity and availability
EG07	Customer	Quality of management information

REF	BSC DIMENSION	ENTERPRISE GOAL
EG08	Internal	Optimization of internal business process functionality
EG09	Internal	Optimization of business process costs
EG10	Internal	Staff skills, motivation and productivity
EG11	Internal	Compliance with internal policies
EG12	Growth	Managed digital transformation programs
EG13	Growth	Product and business innovation

Reference: COBIT 2019 Framework: Basic Concepts: Governance Systems and Components, Chapter 4

COBIT OVERVIEW AND PRODUCT ARCHITECTURE



Inputs to COBIT 2019

COBIT 5

Standards, Frameworks, Regulations

Community Contribution

COBIT 2019

COBIT Core

Reference Model of Governance and Management Objectives

- Enterprise strategy
- Enterprise goals
- Enterprise size
- Role of IT
- Sourcing model for IT
- Compliance requirements
- Etc.

Design Factors

Focus Area

- SME
- Security
- Risk
- DevOps
- Etc.

Tailored Enterprise Governance System for Information and Technology

- ➢ Priority governance and management objectives
- ➢ Specific guidance from focus areas
- ➢ Target capability and performance management guidance

COBIT Core Publications

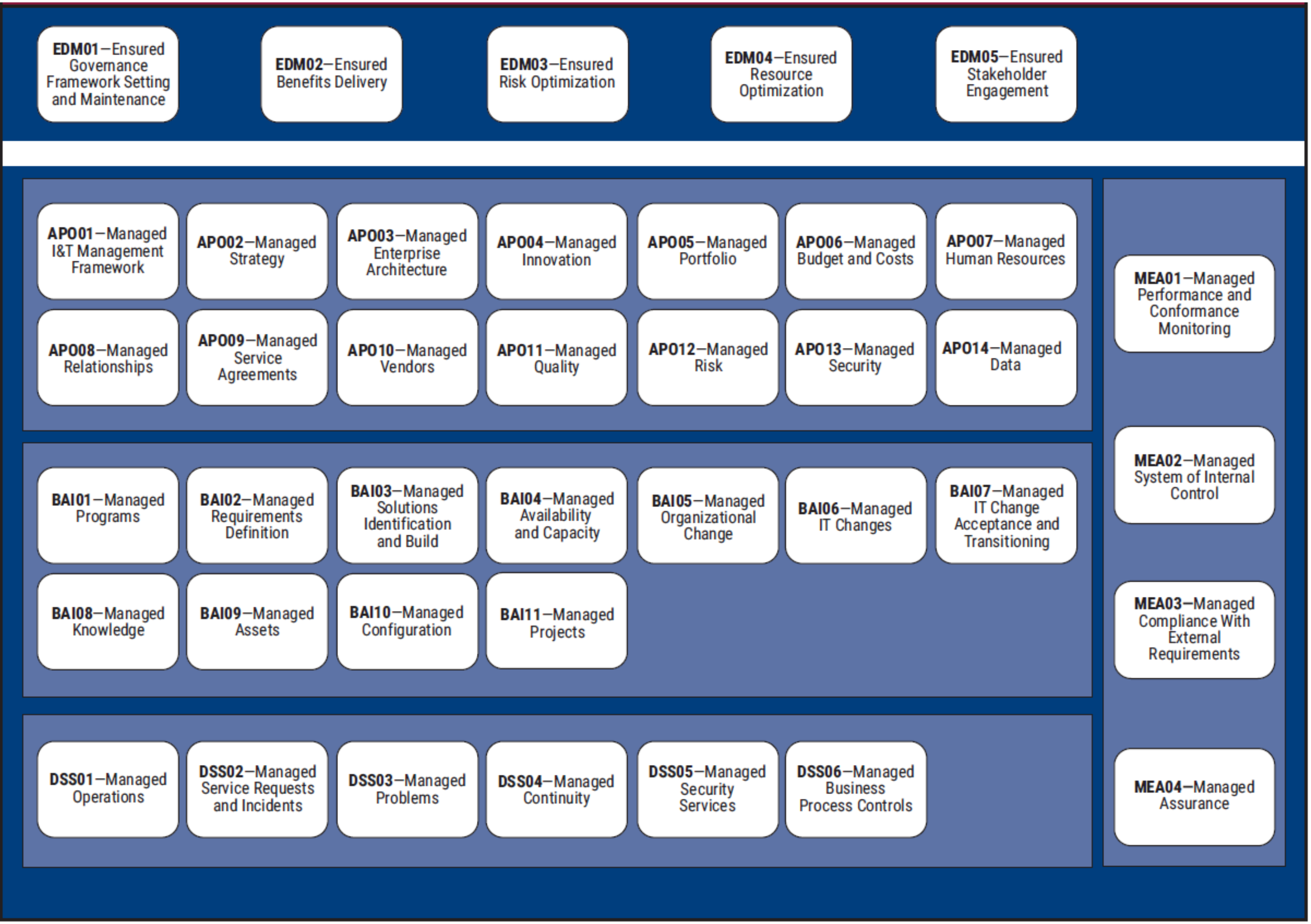
COBIT® 2019 Framework: Introduction and Methodology

COBIT® 2019 Framework: Governance and Management Objectives

COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution

COBIT® 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution

Reference: COBIT 2019 Framework: Introduction and Methodology Chapter 4 Basic Concepts



EDM01—Ensured Governance Framework Setting and Maintenance

EDM02—Ensured Benefits Delivery

EDM03—Ensured Risk Optimization

EDM04—Ensured Resource Optimization

EDM05—Ensured Stakeholder Engagement

APO01—Managed I&T Management Framework

APO02—Managed Strategy

APO03—Managed Enterprise Architecture

APO04—Managed Innovation

APO05—Managed Portfolio

APO06—Managed Budget and Costs

APO07—Managed Human Resources

APO08—Managed Relationships

APO09—Managed Service Agreements

APO10—Managed Vendors

APO11—Managed Quality

APO12—Managed Risk

APO13—Managed Security

APO14—Managed Data

BAI01—Managed Programs

BAI02—Managed Requirements Definition

BAI03—Managed Solutions Identification and Build

BAI04—Managed Availability and Capacity

BAI05—Managed Organizational Change

BAI06—Managed IT Changes

BAI07—Managed IT Change Acceptance and Transitioning

BAI08—Managed Knowledge

BAI09—Managed Assets

BAI10—Managed Configuration

BAI11—Managed Projects

DSS01—Managed Operations

DSS02—Managed Service Requests and Incidents

DSS03—Managed Problems

DSS04—Managed Continuity

DSS05—Managed Security Services

DSS06—Managed Business Process Controls

MEA01—Managed Performance and Conformance Monitoring

MEA02—Managed System of Internal Control

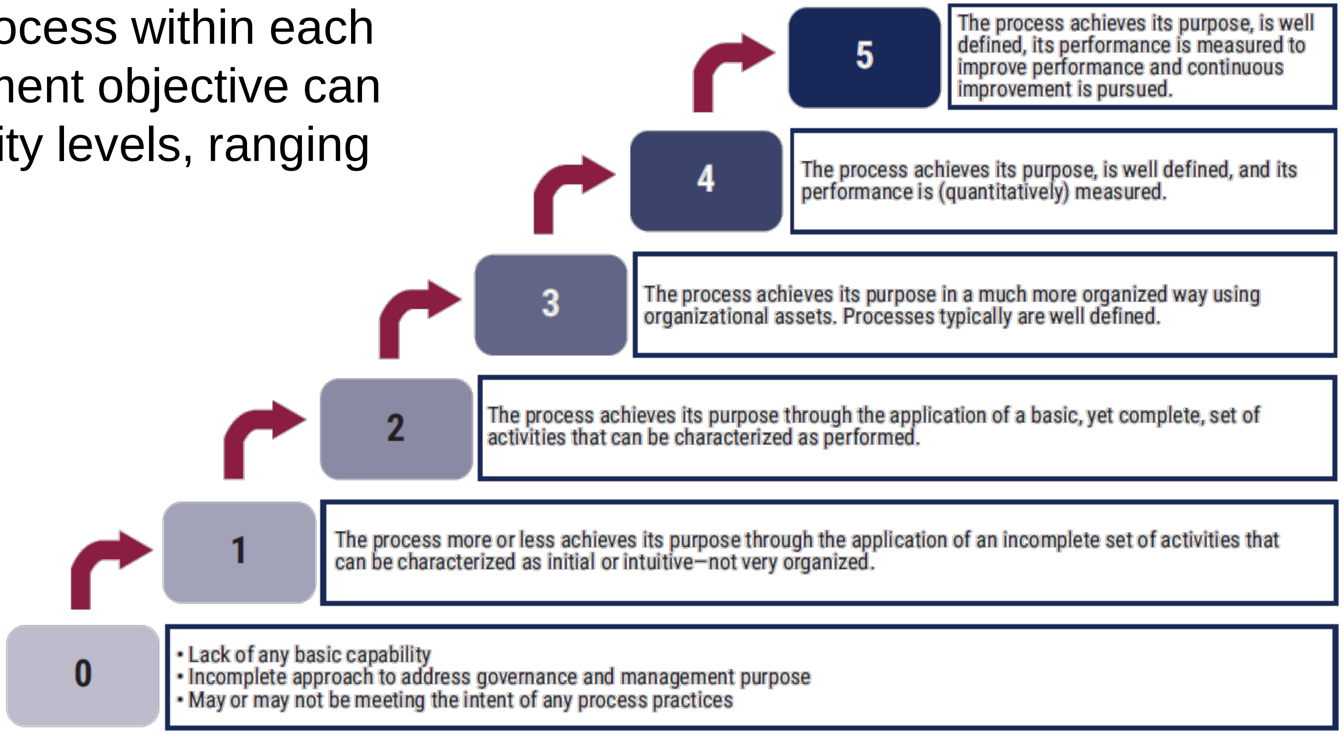
MEA03—Managed Compliance With External Requirements

MEA04—Managed Assurance

Known as the Process Reference Model, or PRM in COBIT 5, COBIT 2019 identifies this as the **COBIT Core Model**.

PROCESS CAPABILITY LEVELS

COBIT 2019 supports a CMMI-based process capability scheme. The process within each governance and management objective can operate at various capability levels, ranging from 0 to 5.



5 The process achieves its purpose, is well defined, its performance is measured to improve performance and continuous improvement is pursued.

4 The process achieves its purpose, is well defined, and its performance is (quantitatively) measured.

3 The process achieves its purpose in a much more organized way using organizational assets. Processes typically are well defined.

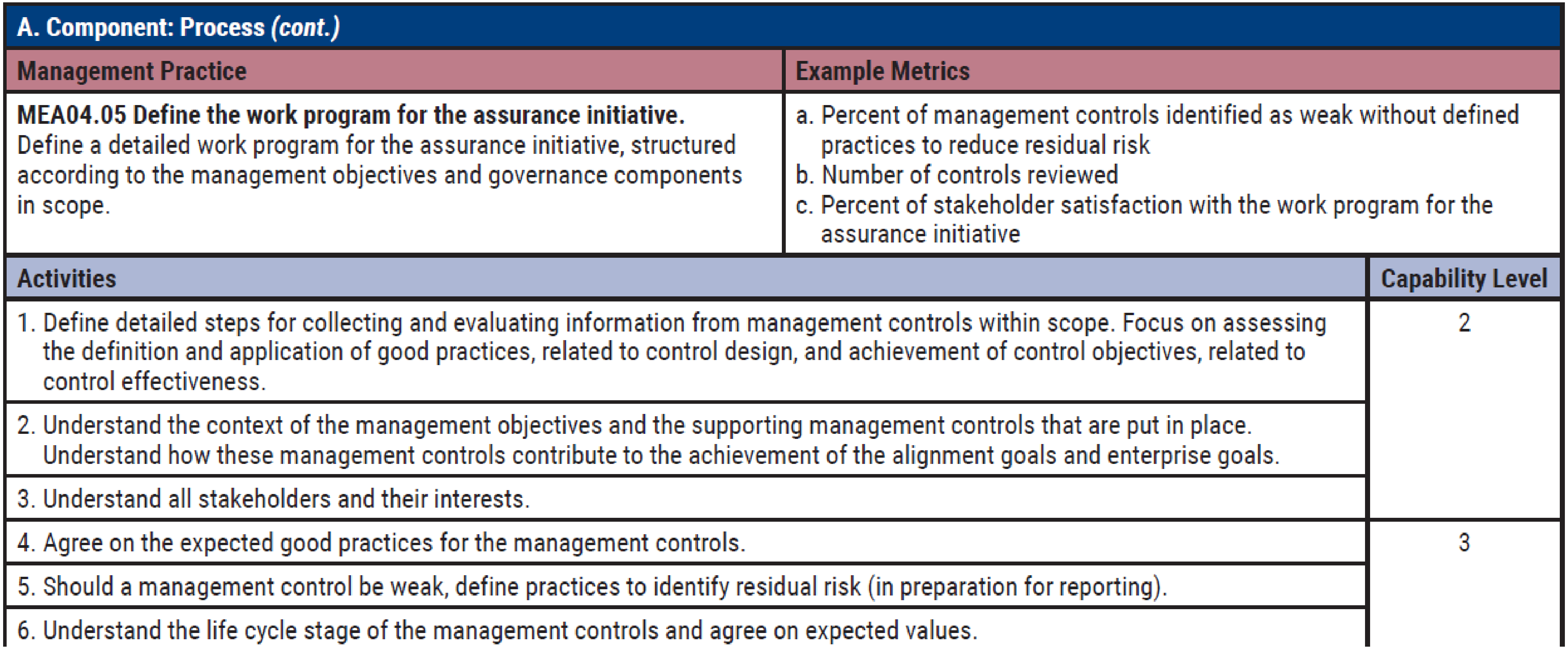
2 The process achieves its purpose through the application of a basic, yet complete, set of activities that can be characterized as performed.

1 The process more or less achieves its purpose through the application of an incomplete set of activities that can be characterized as initial or intuitive—not very organized.

0
- Lack of any basic capability
- Incomplete approach to address governance and management purpose
- May or may not be meeting the intent of any process practices

Reference: COBIT 2019 Framework: Introduction and Methodology Chapter 6 Performance Management in COBIT

MANAGEMENT OBJECTIVE: MEA04 — MANAGED ASSURANCE



A. Component: Process *(cont.)*

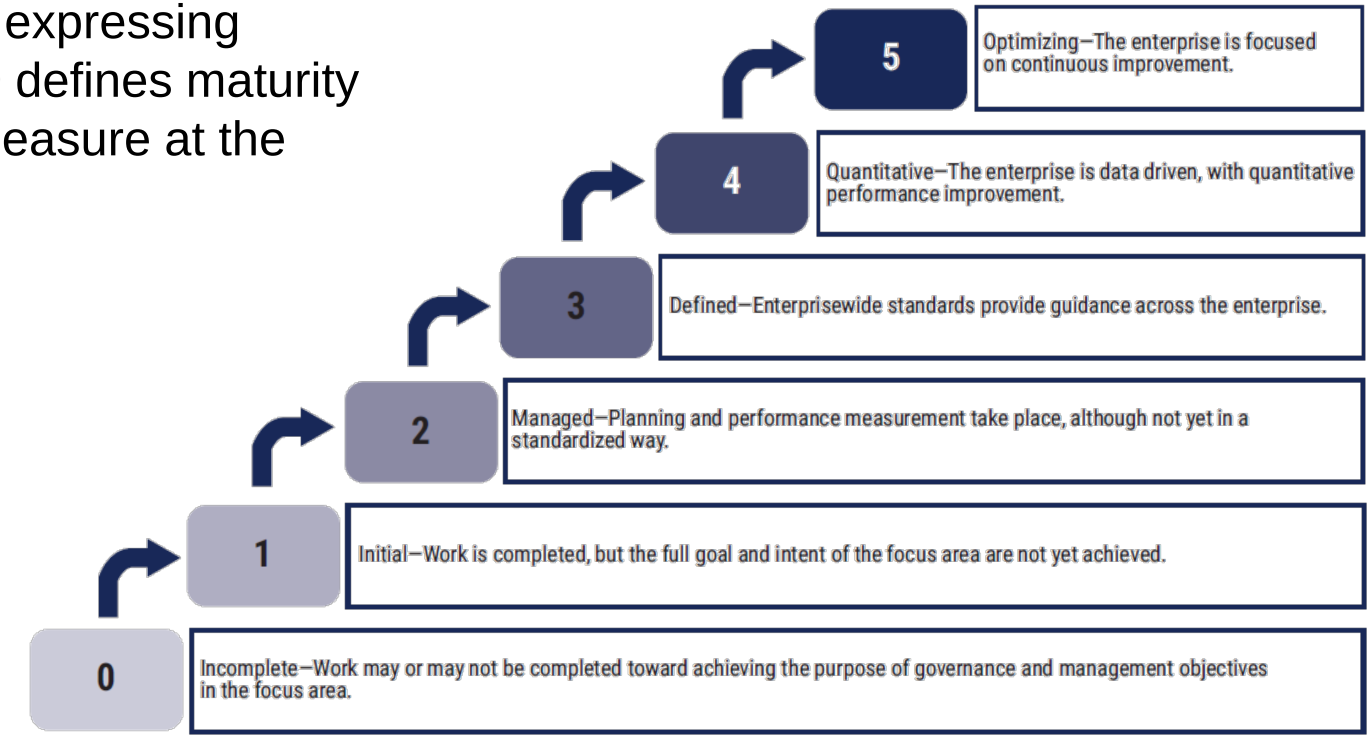
Management Practice	Example Metrics
MEA04.05 Define the work program for the assurance initiative. Define a detailed work program for the assurance initiative, structured according to the management objectives and governance components in scope.	a. Percent of management controls identified as weak without defined practices to reduce residual risk b. Number of controls reviewed c. Percent of stakeholder satisfaction with the work program for the assurance initiative

Activities	Capability Level
1. Define detailed steps for collecting and evaluating information from management controls within scope. Focus on assessing the definition and application of good practices, related to control design, and achievement of control objectives, related to control effectiveness.	2
2. Understand the context of the management objectives and the supporting management controls that are put in place. Understand how these management controls contribute to the achievement of the alignment goals and enterprise goals.	
3. Understand all stakeholders and their interests.	
4. Agree on the expected good practices for the management controls.	3
5. Should a management control be weak, define practices to identify residual risk (in preparation for reporting).	
6. Understand the life cycle stage of the management controls and agree on expected values.	

Reference: COBIT 2019 Framework: Governance and Management Objectives Chapter 4 Detailed Guidance

FOCUS AREA MATURITY LEVELS

Maturity levels can be used for when a higher level is required for expressing performance. COBIT 2019 defines maturity levels as a performance measure at the focus area level.



5 Optimizing—The enterprise is focused on continuous improvement.

4 Quantitative—The enterprise is data driven, with quantitative performance improvement.

3 Defined—Enterprisewide standards provide guidance across the enterprise.

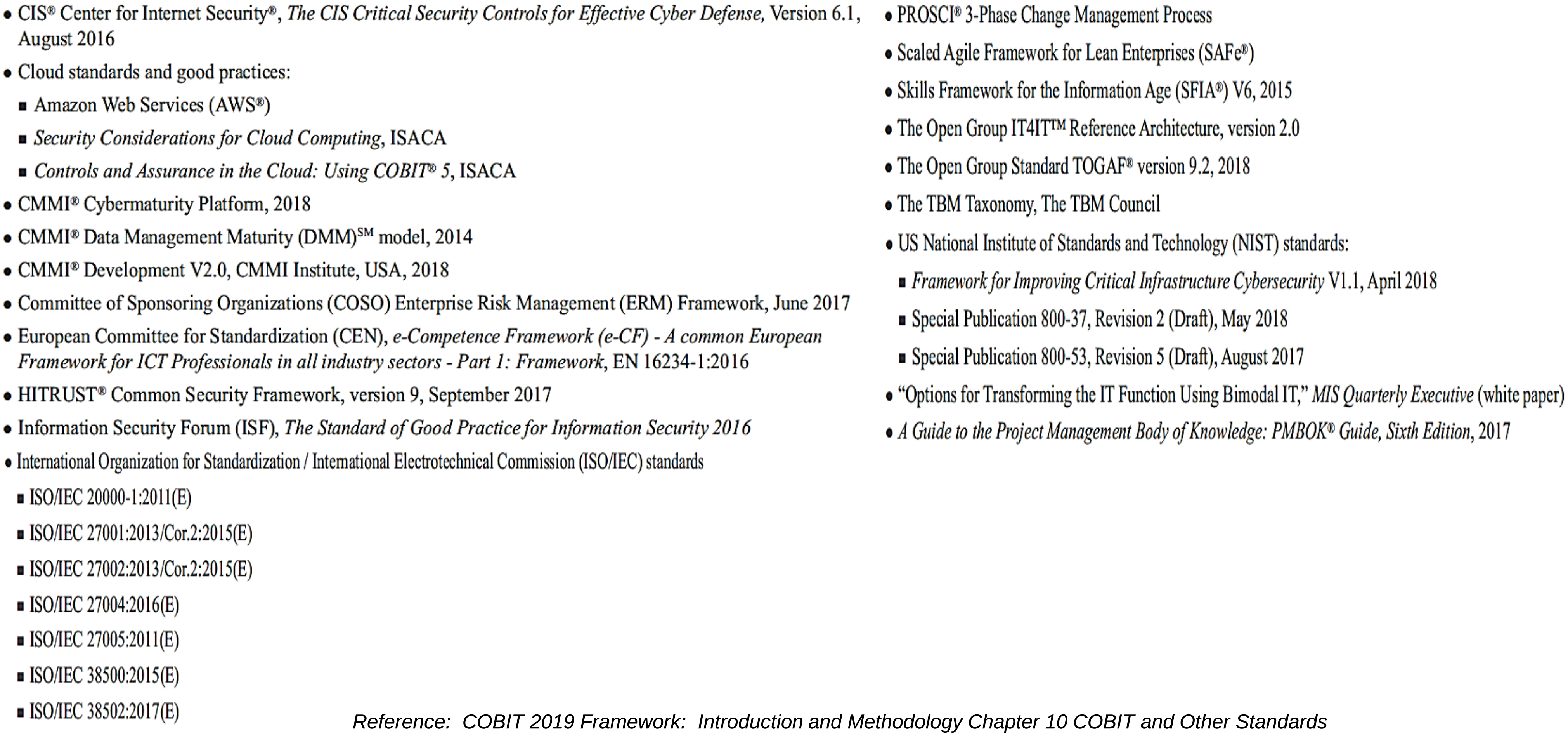
2 Managed—Planning and performance measurement take place, although not yet in a standardized way.

1 Initial—Work is completed, but the full goal and intent of the focus area are not yet achieved.

0 Incomplete—Work may or may not be completed toward achieving the purpose of governance and management objectives in the focus area.

Reference: COBIT 2019 Framework: Introduction and Methodology Chapter 6 Performance Management in COBIT

COBIT AND OTHER STANDARDS



- CIS® Center for Internet Security®, *The CIS Critical Security Controls for Effective Cyber Defense*, Version 6.1, August 2016
- Cloud standards and good practices:
  - Amazon Web Services (AWS®)
  - *Security Considerations for Cloud Computing*, ISACA
  - *Controls and Assurance in the Cloud: Using COBIT® 5*, ISACA
- CMMI® Cybermaturity Platform, 2018
- CMMI® Data Management Maturity (DMM)^{SM} model, 2014
- CMMI® Development V2.0, CMMI Institute, USA, 2018
- Committee of Sponsoring Organizations (COSO) Enterprise Risk Management (ERM) Framework, June 2017
- European Committee for Standardization (CEN), *e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework*, EN 16234-1:2016
- HITRUST® Common Security Framework, version 9, September 2017
- Information Security Forum (ISF), *The Standard of Good Practice for Information Security 2016*
- International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) standards
  - ISO/IEC 20000-1:2011(E)
  - ISO/IEC 27001:2013/Cor.2:2015(E)
  - ISO/IEC 27002:2013/Cor.2:2015(E)
  - ISO/IEC 27004:2016(E)
  - ISO/IEC 27005:2011(E)
  - ISO/IEC 38500:2015(E)
  - ISO/IEC 38502:2017(E)
- PROSCI® 3-Phase Change Management Process
- Scaled Agile Framework for Lean Enterprises (SAFe®)
- Skills Framework for the Information Age (SFIA®) V6, 2015
- The Open Group IT4IT™ Reference Architecture, version 2.0
- The Open Group Standard TOGAF® version 9.2, 2018
- The TBM Taxonomy, The TBM Council
- US National Institute of Standards and Technology (NIST) standards:
  - *Framework for Improving Critical Infrastructure Cybersecurity* V1.1, April 2018
  - Special Publication 800-37, Revision 2 (Draft), May 2018
  - Special Publication 800-53, Revision 5 (Draft), August 2017
- "Options for Transforming the IT Function Using Bimodal IT," *MIS Quarterly Executive* (white paper)
- *A Guide to the Project Management Body of Knowledge: PMBOK® Guide, Sixth Edition*, 2017

Reference: COBIT 2019 Framework: Introduction and Methodology Chapter 10 COBIT and Other Standards

IT INTERNAL AUDIT FUNCTION IMPLEMENTATION

- COBIT 2019 publications
- ITAF, COBIT 5 for Assurance publications
- COBIT 2019 training (Foundation, Design & Implementation) and exams
- CISA training and exams

Questions

KPMG

kpmg.ru

Download on the App Store

kpmg.com/app

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.