COBIT® 2019

FRAMEWORK

Governance and Management Objectives

ISACA®

About ISACA

Nearing its 50th year, ISACA® (isaca.org) is a global association helping individuals and enterprises achieve the positive potential of technology. Technology powers today's world and ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organizations. ISACA leverages the expertise of its half-million engaged professionals in information and cyber security, governance, assurance, risk and innovation, as well as its enterprise performance subsidiary, CMMI® Institute, to help advance innovation through technology. ISACA has a presence in more than 188 countries, including more than 217 chapters and offices in both the United States and China.

Disclaimer

ISACA has designed and created *COBIT® 2019 Framework: Governance and Management Objectives* (the "Work") primarily as an educational resource for governance of enterprise IT (GEIT), assurance, risk and security professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, governance of enterprise IT (GEIT), assurance, risk and security professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

Copyright

© 2018 ISACA. All rights reserved. For usage guidelines, see *www.isaca.org/COBITuse*.

ISACA

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA
Phone: +1.847.660.5505
Fax: +1.847.253.1755
Contact us: https://support.isaca.org
Website: www.isaca.org

Participate in the ISACA Online Forums: https://engage.isaca.org/onlineforums

Twitter: http://twitter.com/ISACANews
LinkedIn: http://linkd.in/ISACAOfficial
Facebook: www.facebook.com/ISACAHQ
Instagram: www.instagram.com/isacanews/

COBIT® 2019 Framework: Governance and Management Objectives
ISBN 978-1-60420-764-4

In Memoriam: John Lainhart (1946-2018)

Dedicated to John Lainhart, ISACA Board chair 1984-1985. John was instrumental in the creation of the COBIT® framework and most recently served as chair of the working group for COBIT® 2019, which culminated in the creation of this work. Over his four decades with ISACA, John was involved in numerous aspects of the association as well as holding ISACA's CISA, CRISC, CISM and CGEIT certifications. John leaves behind a remarkable personal and professional legacy, and his efforts significantly impacted ISACA.

Page intentionally left blank

Acknowledgments

ISACA wishes to recognize:

COBIT Working Group (2017-2018)
John Lainhart, Chair, CISA, CRISC, CISM, CGEIT, CIPP/G, CIPP/US, Grant Thornton, USA
Matt Conboy, Cigna, USA
Ron Saull, CGEIT, CSP, Great-West Lifeco & IGM Financial (retired), Canada

Development Team
Steven De Haes, Ph.D., Antwerp Management School, University of Antwerp, Belgium
Matthias Goorden, PwC, Belgium
Stefanie Grijp, PwC, Belgium
Geert Poels, PhD, Ghent University, Belgium
Dirk Steuperaert, CISA, CRISC, CGEIT, IT In Balance, Belgium

Expert Reviewers
Sarah Ahmad Abedin, CISA, CRISC, CGEIT, Grant Thornton LLP, USA
Floris Ampe, CISA, CRISC, CGEIT, CIA, ISO27000, PRINCE2, TOGAF, PwC, Belgium
Elisabeth Antonssen, Nordea Bank, Sweden
Krzystof Baczkiewicz, CHAMP, CITAM, CSAM, Transpectit, Poland
Christopher M. Ballister, CRISC, CISM, CGEIT, Grant Thornton, USA
Gary Bannister, CGEIT, CGMA, FCMA, Austria
Graciela Braga, CGEIT, Auditor and Advisor, Argentina
Ricardo Bria, CISA, CRISC, CGEIT, COTO CICSA, Argentina
Sushil Chatterji, CGEIT, Edutech Enterprises, Singapore
Peter T. Davis, CISA, CISM, CGEIT, COBIT 5 Assessor, CISSP, CMA, CPA, PMI-RMP, PMP, Peter Davis+Associates, Canada
James Doss, CISM, CGEIT, EMCCA, ITIL Expert, PMP, SSGB, TOGAF 9, ITvalueQuickStart.com, USA
Yalcin Gerek, CISA, CRISC, CGEIT, ITIL Expert, Prince2, ISO 20000LI, ISO27001LA, TAC AS., Turkey
James L. Golden, Golden Consulting Associates, USA
J. Winston Hayden, CISA, CISM, CRISC, CGEIT, South Africa
Jimmy Heschl, CISA, CISM, CGEIT, Red Bull, Austria
Jorge Hidalgo, CISA, CISM, CGEIT, Chile
John Jasinski, CISA, CRISC, CISM, CGEIT, COBIT 5 Assessor, CSM, CSPO, IT4IT-F, ITIL Expert, Lean IT-F, MOF, SSBB, TOGAF-F, USA
Joanna Karczewska, CISA, Poland
Glenn Keaveny, CEH, CISSP, Grant Thornton, USA
Eddy Khoo S. K., CGEIT, Kuala Lumpur, Malaysia
Joao Souza Neto, CRISC, CGEIT, Universidade Católica de Brasília, Brazil
Tracey O'Brien, CISA, CISM, CGEIT, IBM Corp (retired), USA
Zachy Olorunojowon, CISA, CGEIT, PMP, BC Ministry of Health, Victoria, BC Canada
Opeyemi Onifade, CISA, CISM, CGEIT, BRMP, CISSP, ISO 27001LA, M.IoD, Afenoid Enterprise Limited, Nigeria
Abdul Rafeq, CISA, CGEIT, FCA, Managing Director, Wincer Infotech Limited, India
Dirk Reimers, Entco Deutschland GmbH, A Micro Focus Company
Steve Reznik, CISA, CRISC, ADP, LLC., USA
Bruno Horta Soares, CISA, CRISC, CGEIT, PMP, GOVaaS - Governance Advisors, as-a-Service, Portugal
Dr. Katalin Szenes, Ph.D., CISA, CISM, CGEIT, CISSP, John von Neumann Faculty of Informatics, Obuda University, Hungary
Mark Thomas, CRISC, CGEIT, Escoute, USA
John Thorp, CMC, ISP, ITCP, The Thorp Network, Canada
Greet Volders, CGEIT, COBIT Assessor, Voquals N.V., Belgium

Acknowledgments *(cont.)*

Expert Reviewers *(cont.)*

Markus Walter, CISA, CISM, CISSP, ITIL, PMP, TOGAF, PwC Singapore/Switzerland
David M. Williams, CISA, CAMS, Westpac, New Zealand
Greg Witte, CISM, G2 Inc., USA

ISACA Board of Directors

Rob Clyde, Chair, CISM, Clyde Consulting LLC, USA
Brennan Baybeck, Vice-Chair, CISA, CRISC, CISM, CISSP, Oracle Corporation, USA
Tracey Dedrick, Former Chief Risk Officer with Hudson City Bancorp, USA
Leonard Ong, CISA, CRISC, CISM, CGEIT, COBIT 5 Implementer and Assessor, CFE, CIPM, CIPT, CISSP, CITBCM, CPP, CSSLP, GCFA, GCIA, GCIH, GSNA, ISSMP-ISSAP, PMP, Merck & Co., Inc., Singapore
R.V. Raghu, CISA, CRISC, Versatilist Consulting India Pvt. Ltd., India
Gabriela Reynaga, CISA, CRISC, COBIT 5 Foundation, GRCP, Holistics GRC, Mexico
Gregory Touhill, CISM, CISSP, Cyxtera Federal Group, USA
Ted Wolff, CISA, Vanguard, Inc., USA
Tichaona Zororo, CISA, CRISC, CISM, CGEIT, COBIT 5 Assessor, CIA, CRMA, EGIT, Enterprise Governance of IT, South Africa
Theresa Grafenstine, CISA, CRISC, CGEIT, CGAP, CGMA, CIA, CISSP, CPA, Deloitte & Touche LLP, USA, ISACA Board Chair, 2017-2018
Chris K. Dimitriadis, Ph.D., CISA, CRISC, CISM, INTRALOT, Greece, ISACA Board Chair, 2015-2017
Matt Loeb, CGEIT, CAE, FASAE, Chief Executive Officer, ISACA, USA
Robert E Stroud (1965-2018), CRISC, CGEIT, XebiaLabs, Inc., USA, ISACA Board Chair, 2014-2015
ISACA is deeply saddened by the passing of Robert E Stroud in September 2018.

TABLE OF CONTENTS

Chapter 1. Introduction to COBIT® 2019 9
1.1 COBIT as an Information and Technology Governance Framework 9
1.1.1 What Is COBIT and What Is It Not? 9
1.2 Overview of COBIT® 2019 10
1.3 Terminology and Key Concepts of the COBIT Framework 11
1.3.1 Governance and Management Objectives 11
1.3.2 Components of the Governance System 12
1.3.3 Focus Areas 14

Chapter 2. Structure of This Publication and Intended Audience 15
2.1 Structure of This Publication 15
2.2 Intended Audience 15

Chapter 3. Structure of COBIT Governance and Management Objectives 17
3.1 Introduction 17
3.2 Governance and Management Objectives 17
3.3 Goals Cascade 18
3.4 Component: Process 19
3.5 Component: Organizational Structures 20
3.6 Component: Information Flows and Items 22
3.7 Component: People, Skills and Competencies 24
3.8 Component: Policies and Procedures 25
3.9 Component: Culture, Ethics and Behavior 25
3.10 Component: Services, Infrastructure and Applications 25

Chapter 4. COBIT Governance and Management Objectives – Detailed Guidance 27
COBIT Core Model 27
4.1 Evaluate, Direct and Monitor (EDM) 27
4.2 Align, Plan and Organize (APO) 53
4.3 Build, Acquire and Implement (BAI) 151
4.4 Deliver, Service and Support (DSS) 229
4.5 Monitor, Evaluate and Assess (MEA) 271

Appendices 297
5.1 Appendix A: Goals Cascade—Mapping Tables 297
5.2 Appendix B: Organizational Structures—Overview and Descriptions 299
5.3 Appendix C: Detailed List of References 300

LIST OF FIGURES

Chapter 1. Introduction to COBIT® 2019

Figure 1.1—COBIT Overview 10
Figure 1.2—COBIT Core Model 12
Figure 1.3—COBIT Components of a Governance System 13

Chapter 3. Structure of COBIT Governance and Management Objectives

Figure 3.1—Display of Governance and Management Objectives 18
Figure 3.2—Display of Applicable Enterprise and Alignment Goals 18
Figure 3.3—Display of Applicable Goals and Example Metrics 19
Figure 3.4—Display of Process Component 19
Figure 3.5—Capability Levels for Processes 20
Figure 3.6—Display of Organizational Structures Component 21
Figure 3.7—Display of Information Flows and Items Component 23
Figure 3.8—Outputs to Multiple Processes 23
Figure 3.9—Display of People, Skills and Competencies Component 24
Figure 3.10—Display of Policies and Procedures Component 25
Figure 3.11—Display of Culture, Ethics and Behavior Component 25
Figure 3.12—Display of Services, Infrastructure and Applications Component 25

Appendices

Figure 5.1—Mapping Enterprise Goals and Alignment Goals 297
Figure 5.2—Mapping Governance and Management Objectives to Alignment Goals 298
Figure 5.3—COBIT Roles and Organizational Structures 299

Chapter 1
Introduction to COBIT® 2019

1.1 COBIT as an Information and Technology Governance Framework

Over the years, best-practice frameworks have been developed and promoted to assist in the process of understanding, designing and implementing enterprise governance of IT (EGIT). COBIT® 2019 builds on and integrates more than 25 years of development in this field, not only incorporating new insights from science, but also operationalizing these insights as practice.

From its foundation in the IT audit community, COBIT® has developed into a broader and more comprehensive information and technology (I&T) governance and management framework and continues to establish itself as a generally accepted framework for I&T governance.

1.1.1 What Is COBIT and What Is It Not?

Before describing the updated COBIT framework, it is important to explain what COBIT is and is not:

COBIT is a framework for the governance and management of information and technology, aimed at the whole enterprise. Enterprise I&T means all the technology and information processing the enterprise puts in place to achieve its goals, regardless of where this happens in the enterprise. In other words, enterprise I&T is not limited to the IT department of an organization but certainly includes it.

The COBIT framework makes a clear distinction between governance and management. These two disciplines encompass different activities, require different organizational structures and serve different purposes.

- **Governance** ensures that:
  - Stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives.
  - Direction is set through prioritization and decision making.
  - Performance and compliance are monitored against agreed-on direction and objectives.

  In most enterprises, governance is the responsibility of the board of directors, under the leadership of the chairperson. Specific governance responsibilities may be delegated to special organizational structures at an appropriate level, particularly in larger, complex enterprises.
- **Management** plans, builds, runs and monitors activities, in alignment with the direction set by the governance body, to achieve enterprise objectives.

  In most enterprises, management is the responsibility of the executive management under the leadership of the chief executive officer (CEO).

COBIT defines the components to build and sustain a governance system: processes, organizational structures, policies and procedures, information flows, culture and behaviors, skills, and infrastructure.[1]

COBIT defines the design factors that should be considered by the enterprise to build a best-fit governance system.

COBIT addresses governance issues by grouping relevant governance components into governance and management objectives that can be managed to the required capability levels.

[1] These components were termed enablers in COBIT® 5.

Several misconceptions about COBIT should be dispelled:

- COBIT is not a full description of the whole IT environment of an enterprise.
- COBIT is not a framework to organize business processes.
- COBIT is not an (IT-)technical framework to manage all technology.
- COBIT does not make or prescribe any IT-related decisions. It will not decide what the best IT strategy is, what the best architecture is, or how much IT can or should cost. Rather, COBIT defines all the components that describe which decisions should be taken, and how and by whom they should be taken.

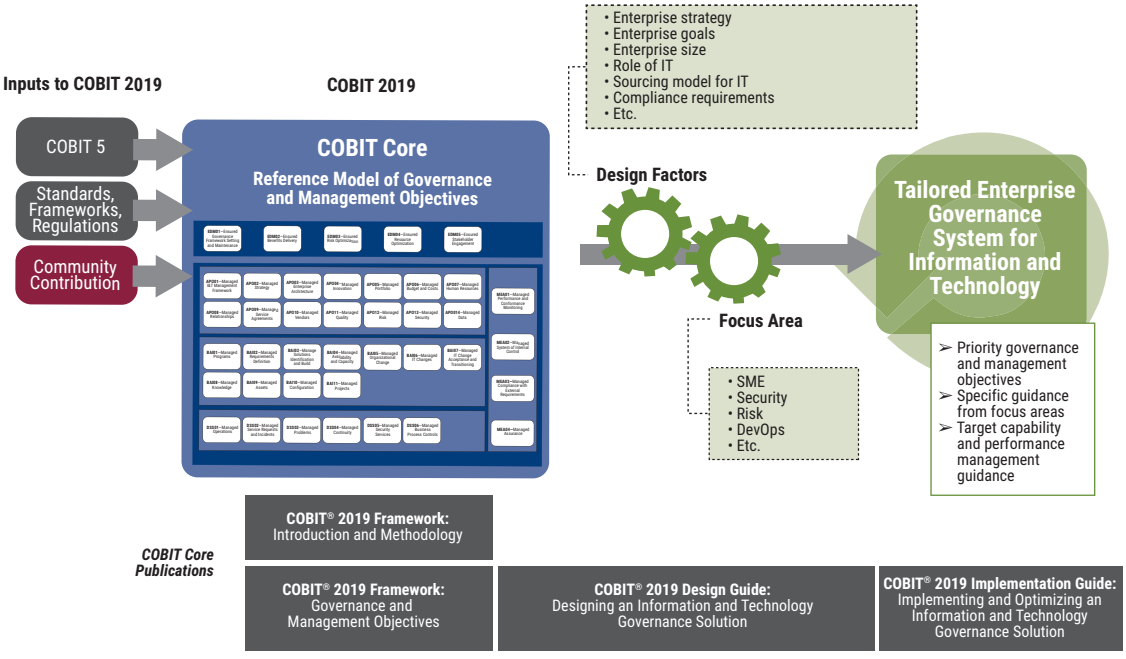
1.2 Overview of COBIT® 2019

The COBIT® 2019 product family is open-ended and designed for customization. The following publications are currently available.[2]

- ***COBIT® 2019 Framework: Introduction and Methodology*** introduces the key concepts of COBIT® 2019.
- ***COBIT® 2019 Framework: Governance and Management Objectives*** comprehensively describes the 40 core governance and management objectives, the processes contained therein, and other related components. This guide also references other standards and frameworks.
- ***COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*** explores design factors that can influence governance and includes a workflow for planning a tailored governance system for the enterprise.
- ***COBIT® 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution*** represents an evolution of the *COBIT® 5 Implementation* guide and develops a road map for continuous governance improvement. It may be used in combination with the *COBIT® 2019 Design Guide.*

Figure 1.1 shows the high-level overview of COBIT® 2019 and illustrates how different publications within the set cover different aspects.

Figure 1.1—COBIT Overview



[2] At the time of publication of this *COBIT® 2019 Framework: Governance and Management Objectives* title, additional titles are planned for the COBIT® 2019 product family but not yet released.

The content identified as focus areas in **figure 1.1** will contain more detailed guidance on specific themes.[3]

In the future, COBIT will call upon its user community to propose content updates, to be applied as controlled contributions on a continuous basis, to keep COBIT up to date with the latest insights and evolutions.

The following sections explain the key concepts and terms used in COBIT® 2019.

1.3 Terminology and Key Concepts of the COBIT Framework

1.3.1 Governance and Management Objectives

For information and technology to contribute to enterprise goals, a number of governance and management objectives should be achieved. Basic concepts relating to governance and management objectives are:

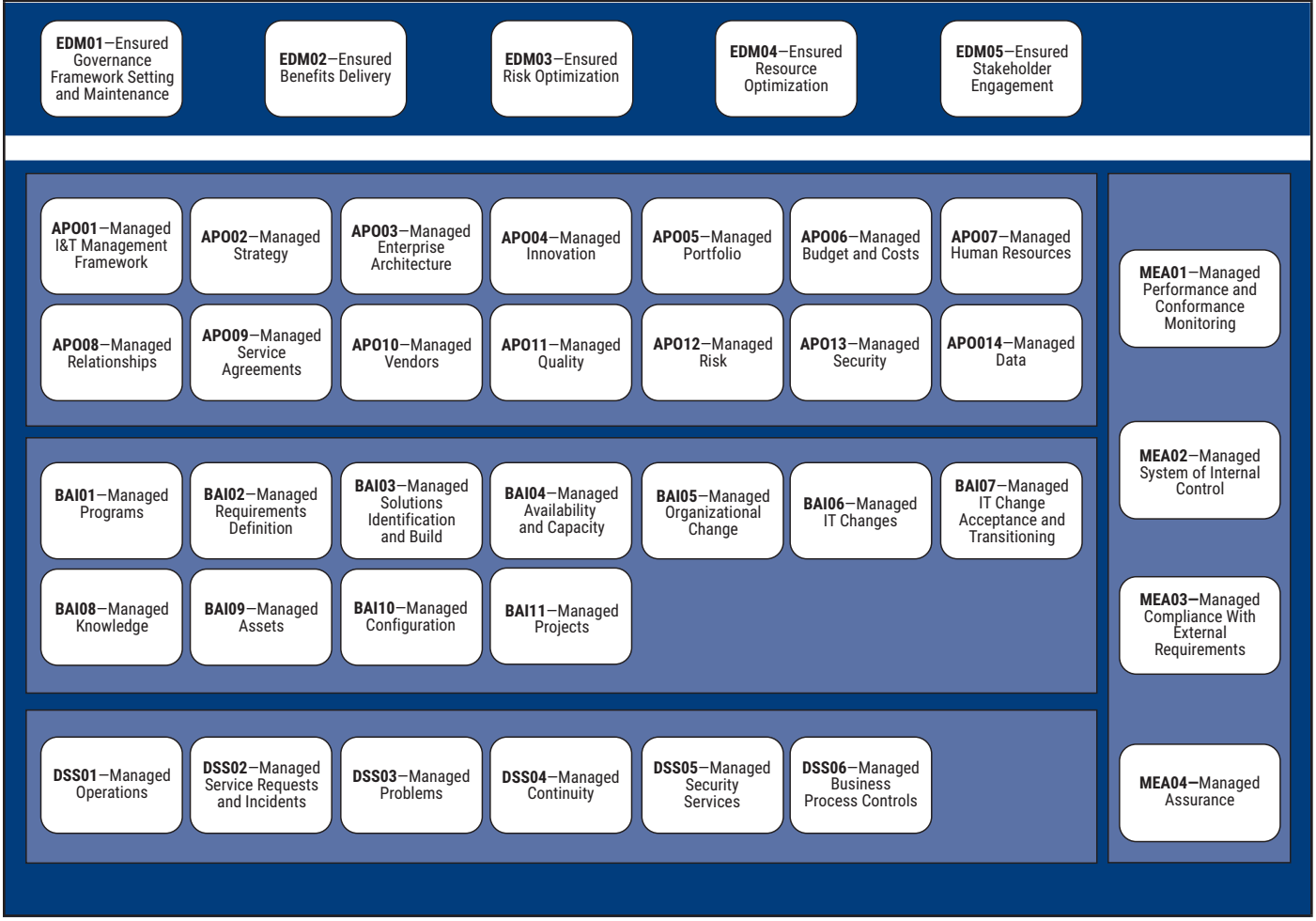
- A governance or management objective **always relates to one process** (with an identical or similar name) and a series of related components of other types to help achieve the objective.
- A governance objective relates to a governance process (depicted on the dark blue background in **figure 1.2**), while a management objective relates to management processes (depicted on the lighter blue background in **figure 1.2**). Boards and executive management are typically accountable for governance processes, while management processes are the domain of senior and middle management.

The governance and management objectives in COBIT are grouped into five domains. The domains have names with verbs that express the key purpose and areas of activity of the objectives contained in them:

- Governance objectives are grouped in the **Evaluate, Direct and Monitor** (EDM) domain. In this domain, the governing body evaluates strategic options, directs senior management on the chosen strategic options and monitors the achievement of the strategy.
- Management objectives are grouped in four domains.
  - **Align, Plan and Organize** (APO) addresses the overall organization, strategy and supporting activities for I&T.
  - **Build, Acquire and Implement** (BAI) treats the definition, acquisition and implementation of I&T solutions and their integration in business processes.
  - **Deliver, Service and Support** (DSS) addresses the operational delivery and support of I&T services, including security.
  - **Monitor, Evaluate and Assess** (MEA) addresses performance monitoring and conformance of I&T with internal performance targets, internal control objectives and external requirements.

[3] A number of these focus area content guides are already in preparation; others are planned. The set of focus area guides is open-ended and will continue to evolve. For the latest information on currently available and planned publications and other content, please visit *www.isaca.org/cobit*.

Figure 1.2—COBIT Core Model



1.3.2 Components of the Governance System

To satisfy governance and management objectives, each enterprise needs to establish, tailor and sustain a governance system built from a number of components.

- Components are factors that, individually and collectively, contribute to the good operations of the enterprise's governance system over I&T.
- Components interact with each other, resulting in a holistic governance system for I&T.
- Components can be of different types. The most familiar are processes. However, components of a governance system also include organizational structures; policies and procedures; information items; culture and behavior; skills and competencies; and services, infrastructure and applications (**figure 1.3**).
  - **Processes** describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs that support achievement of overall IT-related goals.
  - **Organizational structures** are the key decision-making entities in an enterprise.
  - **Principles, policies and frameworks** translate desired behavior into practical guidance for day-to-day management.
  - **Information** is pervasive throughout any organization and includes all information produced and used by the enterprise. COBIT focuses on the information required for the effective functioning of the governance system of the enterprise.

- **Culture, ethics and behavior** of individuals and of the enterprise are often underestimated as factors in the success of governance and management activities.
- **People, skills and competencies** are required for good decisions, execution of corrective action and successful completion of all activities.
- **Services, infrastructure and applications** include the infrastructure, technology and applications that provide the enterprise with the governance system for I&T processing.

Figure 1.3—COBIT Components of a Governance System



Components of all types can be generic or can be variants of generic components:

- **Generic** components are described in the COBIT core model (see **figure 1.2**) and apply in principle to any situation. However, they are generic in nature and generally need customization before being practically implemented.
- **Variants** are based on generic components but are tailored for a specific purpose or context within a focus area (e.g., for information security, DevOps, a particular regulation).

1.3.3 Focus Areas

A **focus area** describes a certain governance topic, domain or issue that can be addressed by a collection of governance and management objectives and their components. Examples of focus areas include small and medium enterprises, cybersecurity, digital transformation, cloud computing, privacy, and DevOps.[4]

The COBIT core model is the subject of this publication, and it provides the generic governance components. Focus areas may contain a combination of generic governance components and variants on certain components tailored to that focus area topic.

The number of focus areas is virtually unlimited. That is what makes COBIT open-ended. New focus areas can be added as required or as subject matter experts and practitioners contribute to the open-ended COBIT model.

A number of focus area content guides are in preparation, and the set will continue to evolve. For the latest information on currently available and pending publications and other content, please visit *www.isaca.org/cobit*.

[4] DevOps exemplifies both a component variant and a focus area. Why? DevOps is a current theme in the marketplace and definitely requires specific guidance, making it a focus area. DevOps includes a number of generic governance and management objectives of the core COBIT model, along with a number of variants of development-, operational- and monitoring-related processes and organizational structures.

Chapter 2
Structure of This Publication and Intended Audience

2.1 Structure of This Publication

This publication provides a comprehensive description of the 40 core governance and management objectives defined in the COBIT core model (**figure 1.2**), the processes contained therein, other related components, and references to related guidance such as other standards and frameworks. A detailed listing of the sources of the included references is located in Appendix C.

The remainder of this document contains the following sections and appendices:

- Chapter 3 explains the structure that is used to detail the guidance for the 40 governance and management objectives across components.
- Chapter 4 provides a comprehensive description of the 40 core governance and management objectives defined in the COBIT core model (**figure 1.2**), the processes contained therein, other related components, and references to related guidance such as other standards and frameworks.
- The appendices include more detail on the:
  - Mapping tables that inform the goals cascade
  - Descriptions of organizational structures
  - List of source references

2.2 Intended Audience

This guide is written for professionals throughout the enterprise, including business, audit, security, risk management, IT and other practitioners who will benefit from detailed guidance on the 40 governance and management objectives of the COBIT core model. A certain level of experience and understanding of the enterprise is required to customize COBIT into tailored and focused governance practices for the enterprise.

Page intentionally left blank

Chapter 3
Structure of COBIT Governance and Management Objectives

3.1 Introduction

This chapter describes the structure used to detail each of the COBIT governance and management objectives. For each governance and management objective, Chapter 4 of this publication provides information related to each of the **governance components** applicable to that governance or management objective:

- Process
- Organizational structures
- Information flows and items
- People, skills and competencies
- Policies and procedures
- Culture, ethics and behavior
- Services, infrastructure and applications

The structure for this information is detailed in the following sections.

3.2 Governance and Management Objectives

As previously explained, COBIT® 2019 includes 40 governance and management objectives, organized into five domains (see **figure 1.2**).

- **Governance** domain
  - Evaluate, Direct and Monitor (EDM)
- **Management** domains
  - Align, Plan and Organize (APO)
  - Build, Acquire and Implement (BAI)
  - Deliver, Service and Support (DSS)
  - Monitor, Evaluate and Assess (MEA)

The high-level information detailed for each objective (**figure 3.1**) includes:

- Domain name
- Focus area (in the case of this publication, this is the COBIT core model)
- Governance or management objective name
- Description
- Purpose statement

Figure 3.1—Display of Governance and Management Objectives	
Domain: <NAME> **Governance/Management Objective:** <NAME>	**Focus Area:** <NAME>
Description	
<TEXT>	
Purpose	
<TEXT>	

3.3 Goals Cascade

Each governance or management objective supports the achievement of alignment goals that are related to larger enterprise goals (see Section 4.6 of *COBIT® 2019 Framework: Introduction and Methodology* for more information and see the goals cascade mapping tables in Appendix A for an example).

Alignment goals that have a primary link to the governance or management objective at hand are listed on the right-hand side of the detailed guidance section covering the goals (**figure 3.2**).

Figure 3.2—Display of Applicable Enterprise and Alignment Goals		
The governance/management objective supports the achievement of a set of primary enterprise and alignment goals:		
Enterprise Goals	➡	**Alignment Goals**
• <EG REF> <GOAL DESCRIPTION>		• <AG REF> <GOAL DESCRIPTION>

Alignment goals include:

- AG01: I&T compliance and support for business compliance with external laws and regulations
- AG02: Managed I&T-related risk
- AG03: Realized benefits from I&T-enabled investments and services portfolio
- AG04: Quality of technology-related financial information
- AG05: Delivery of I&T services in line with business requirements
- AG06: Agility to turn business requirements into operational solutions
- AG07: Security of information, processing infrastructure and applications, and privacy
- AG08: Enabling and supporting business processes by integrating applications and technology
- AG09: Delivering programs on time, on budget and meeting requirements and quality standards
- AG10: Quality of I&T management information
- AG11: I&T compliance with internal policies
- AG12: Competent and motivated staff with mutual understanding of technology and business
- AG13: Knowledge, expertise and initiatives for business innovation

Enterprise goals that have a primary link to the listed alignment goals are included on the left-hand side of the detailed guidance in Chapter 4 covering the goals. Enterprise goals include:

- EG01: Portfolio of competitive products and services
- EG02: Managed business risk

- EG03: Compliance with external laws and regulations
- EG04: Quality of financial information
- EG05: Customer-oriented service culture
- EG06: Business service continuity and availability
- EG07: Quality of management information
- EG08: Optimization of business process functionality
- EG09: Optimization of business process costs
- EG10: Staff skills, motivation and productivity
- EG11: Compliance with internal policies
- EG12: Managed digital transformation programs
- EG13: Product and business innovation

Example metrics for both enterprise goals and alignment goals are also provided in the tables (**figure 3.3**).

Figure 3.3—Display of Applicable Goals and Example Metrics

The governance/management objective supports the achievement of a set of primary enterprise and alignment goals:	
Enterprise Goals	**Alignment Goals**
<EG REF> <GOAL DESCRIPTION>	<AG REF> <GOAL DESCRIPTION>
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
<EG REF> • <METRIC>	<AG REF> • <METRIC>
<EG REF> • <METRIC>	<AG REF> • <METRIC>

3.4 Component: Process

Each governance and management objective includes several process practices. Each process has one or more activities. A limited number of example metrics accompanies each process practice, to measure the achievement of the practice and its contribution to the achievement of the overall objective (**figure 3.4**).

Figure 3.4—Display of Process Component

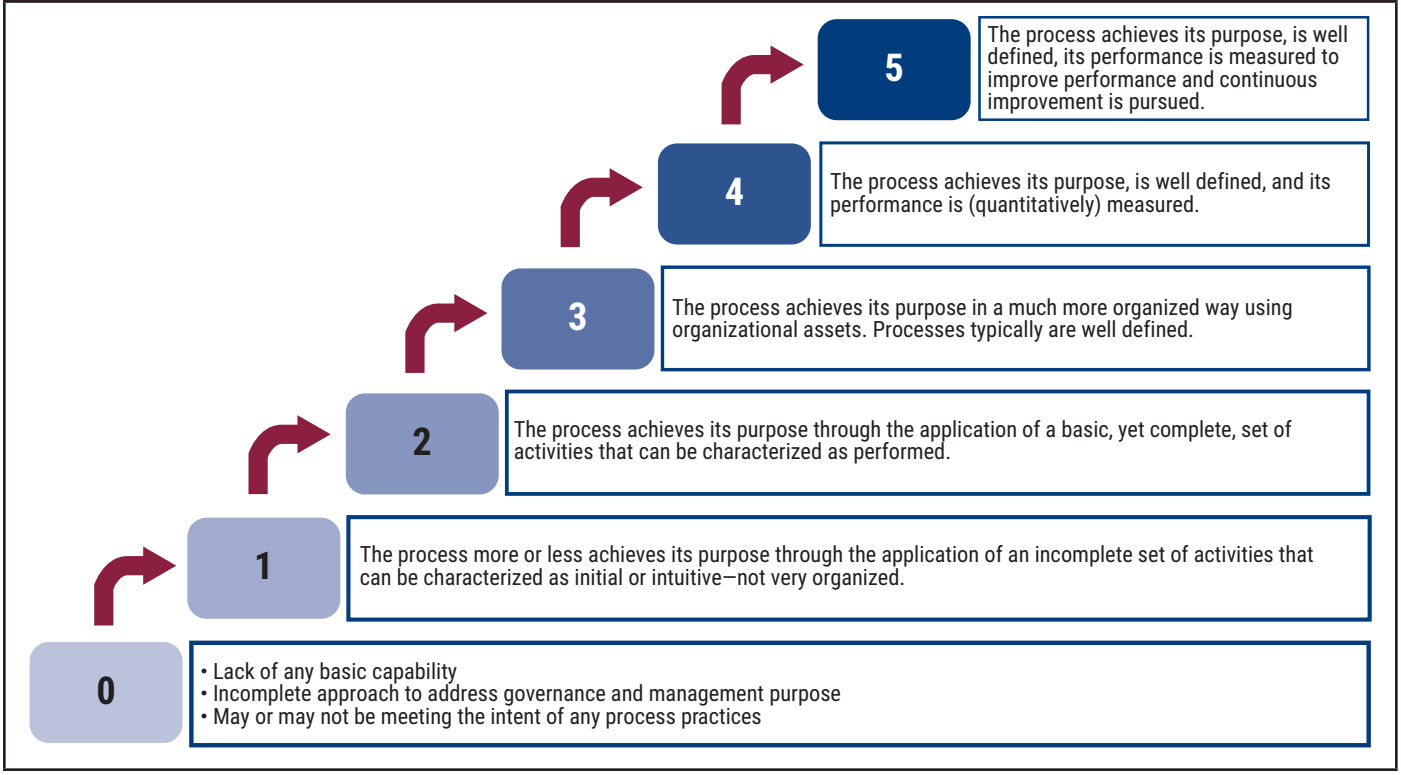
A. Component: Process	
Governance/Management Practice	**Example Metrics**
<REF> <NAME> <DESCRIPTION>	<METRIC>

Activities	Capability Level
1. <TEXT>	<NR>
2. <TEXT>	<NR>
n. <TEXT>	<NR>

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
<STANDARD NAME>	<TEXT>
<STANDARD NAME>	<TEXT>

A capability level is assigned to all process activities, enabling clear definition of processes at different capability levels. A process reaches a certain capability level as soon as all activities of that level are performed successfully. COBIT® 2019 supports a Capability Maturity Model Integration® (CMMI)-based process-capability scheme, ranging from 0 to 5. The capability level is a measure of how well a process is implemented and performing. **Figure 3.5** depicts the model, the increasing capability levels and the general characteristics of each.

Figure 3.5—Capability Levels for Processes



See Chapter 6 of the *COBIT® 2019 Framework: Introduction and Methodology* for additional details on performance management and capability measurement.

Where relevant, references to other standards and guidance are included in this section as well (see **figure 3.4**). The related guidance refers to all standards, frameworks, compliance requirements and other guidance that are relevant for the process at hand. The detailed reference area cites specific chapters or sections within related guidance. A complete list of sources for the related guidance is included in Appendix C.

If no related guidance is listed for a particular component, no applicable references are known from the sources mapped. The practitioner community is encouraged to suggest related guidance.

3.5 Component: Organizational Structures

The organizational structures governance component suggests levels of responsibility and accountability for process practices (**figure 3.6**). The charts include individual roles as well as organizational structures, from both business and IT.

Figure 3.6—Display of Organizational Structures Component								
B. Component: Organizational Structures								
Key Governance/Management Practice	**Organizational Structure 1**	**Organizational Structure 2**	**Organizational Structure 3**	**Organizational Structure 4**	**Organizational Structure 5**	**Organizational Structure 6**	**Organizational Structure 7**	**Organizational Structure 8, etc.**
<REF> <NAME>								

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
<STANDARD NAME>	<TEXT>
<STANDARD NAME>	<TEXT>

The following roles and organizational structures have been defined in the context of COBIT® 2019:

- Board
- Executive Committee
- Chief Executive Officer
- Chief Financial Officer
- Chief Operating Officer
- Chief Risk Officer
- Chief Information Officer
- Chief Technology Officer
- Chief Digital Officer
- I&T Governance Board
- Architecture Board
- Enterprise Risk Committee
- Chief Information Security Officer
- Business Process Owner
- Portfolio Manager
- Steering (Programs/Projects) Committee
- Program Manager
- Project Manager
- Project Management Office
- Data Management Function
- Head Human Resources
- Relationship Manager

- Head Architect
- Head Development
- Head IT Operations
- Head IT Administration
- Service Manager
- Information Security Manager
- Business Continuity Manager
- Privacy Officer
- Legal Counsel
- Compliance
- Audit

A detailed description of each of these roles and organizational structures is included in Appendix B. The different levels of involvement included for these structures can be divided into responsible and accountable levels.

- **Responsible** (R) roles take the main operational stake in fulfilling the practice and create the intended outcome. Who is getting the task done? Who drives the task?
- **Accountable** (A) roles carry overall accountability. As a principle, accountability cannot be shared. Who accounts for the success and achievement of the task?

Each domain describes the organizational structures that have responsibility and/or accountability in the domain. A detailed description of each of role and organizational structure is included. Other organizational structures without responsibility or accountability have been omitted to improve readability of the chart.

Practitioners can complete charts by adding two levels of involvement for roles and organizational structures. Since the attribution of consulted and informed roles depends on organizational context and priorities, they are not included in this detailed guidance.

- **Consulted** (C) roles provide input for the practice. Who is providing input?
- **Informed** (I) roles are informed of the achievements and/or deliverables of the practice. Who is receiving information?

Enterprises should review levels of responsibility and accountability, consulted and informed, and update roles and organizational structures in the chart according to the enterprise's context, priorities and preferred terminology.

Where relevant, references to other standards and additional guidance are included in the organizational structure components section. The Related Guidance refers to all standards, frameworks, compliance requirements and other guidance that are relevant for the organizational structures at hand and their levels of involvement in the process. The detailed reference area cites specific chapters or sections within related guidance. A complete list of sources is included in Appendix C.

3.6 Component: Information Flows and Items

The third governance component provides guidance on the information flows and items linked with process practices. Each practice includes inputs and outputs, with indications of origin and destination.

In general, each output is sent to one or a limited number of destinations, typically another COBIT process practice. That output then becomes an input to its destination (**figure 3.7**).

Figure 3.7—Display of Information Flows and Items Component				
C. Component: Information Flows and Items				
Governance/Management Practice	Inputs		Outputs	
<REF> <NAME>	From	Description	Description	To
	<REF>	<TEXT>	<TEXT>	<REF>

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
<STANDARD NAME>	<TEXT>
<STANDARD NAME>	<TEXT>

A number of outputs, however, have many destinations (e.g., all COBIT processes or all processes within a domain). For readability reasons, these outputs are not listed as inputs in the target processes. A complete list of such outputs is included in **figure 3.8**.

For some inputs/outputs, "internal" is cited as a destination if input and output are shared between activities within the same process.

Figure 3.8—Outputs to Multiple Processes		
Outputs to All Processes		
From Key Practice	Output Description	Destination
APO13.02	Information security risk treatment plan	All EDM, All APO; All BAI, All DSS; All MEA
From Governance Practice	Output Description	Destination
EDM01.01	Enterprise governance guiding principles	All EDM
EDM01.01	Decision-making model	All EDM
EDM01.02	Enterprise governance communication	All EDM
EDM01.01	Authority levels	All EDM
EDM01.03	Feedback on governance effectiveness and performance	All EDM
Outputs to All Management Processes		
From Management Practice	Output Description	Destination
APO01.01	Management system design	All APO; All BAI; All DSS; All MEA
APO01.01	Priority governance and management objectives	All APO; All BAI; All DSS; All MEA
APO01.02	Communication on I&T objectives	All APO; All BAI; All DSS; All MEA
APO01.02	Communication ground rules	All APO; All BAI; All DSS; All MEA
APO01.03	Target model gap analysis	All APO; All BAI; All DSS; All MEA
APO01.11	Process improvement opportunities	All APO; All BAI; All DSS; All MEA
APO02.05	I&T strategy and objectives	All APO; All BAI; All DSS; All MEA
APO02.06	Communication package	All APO; All BAI; All DSS; All MEA
APO11.03	Quality management standards	All APO; All BAI; All DSS; All MEA
APO11.04	Process quality of service goals and metrics	All APO; All BAI; All DSS; All MEA
APO11.05	Communications on continual improvement and best practices	All APO; All BAI; All DSS; All MEA
APO11.05	Examples of good practice to be shared	All APO; All BAI; All DSS; All MEA
APO11.05	Quality review benchmark results	All APO; All BAI; All DSS; All MEA

Figure 3.8—Outputs to Multiple Processes *(cont.)*		
Outputs to All Management Processes		
From Management Practice	**Output Description**	**Destination**
MEA01.02	Monitoring targets	All APO; All BAI; All DSS; All MEA
MEA01.04	Performance reports	All APO; All BAI; All DSS; All MEA
MEA01.05	Remedial actions and assignments	All APO; All BAI; All DSS; All MEA
MEA02.01	Results of internal control monitoring and reviews	All APO; All BAI; All DSS; All MEA
MEA02.01	Results of benchmarking and other evaluations	All APO; All BAI; All DSS; All MEA
MEA02.03	Results of reviews of self-assessments	All APO; All BAI; All DSS; All MEA
MEA02.03	Self-assessment plans and criteria	All APO; All BAI; All DSS; All MEA
MEA02.04	Control deficiencies	All APO; All BAI; All DSS; All MEA
MEA02.04	Remedial actions	All APO; All BAI; All DSS; All MEA
MEA03.02	Communications of changed compliance requirements	All APO; All BAI; All DSS; All MEA
MEA04.02	Assurance plans	All APO; All BAI; All DSS; All MEA
MEA04.08	Assurance review report	All APO; All BAI; All DSS; All MEA
MEA04.08	Assurance review results	All APO; All BAI; All DSS; All MEA
MEA04.09	Remedial actions	All APO; All BAI; All DSS; All MEA

Where relevant, references to other standards and additional guidance are included in the information flows and items component. The Related Guidance refers to all standards, frameworks, compliance requirements and other guidance that are relevant for the information item at hand. The detailed reference area cites specific chapters or sections within related guidance. A complete list of sources is included in Appendix C.

3.7 Component: People, Skills and Competencies

The people, skills and competencies governance component identifies human resources and skills required to achieve the governance or management objective. COBIT® 2019 based this guidance on the Skills Framework for the Information Age (SFIA®) V6 (version 6).[5] All listed skills are described in detail in the SFIA framework. The Detailed Reference provides a unique code that correlates to SFIA guidance on the skill (**figure 3.9**). In addition, references are included for several governance and management objectives to the *e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework*[6] and the Institute of Internal Auditors' "Core Principles for the Professional Practice of Internal Auditing."[7]

Figure 3.9—Display of People, Skills and Competencies Component		
D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
<NAME>	Skills Framework for the Information Age, V6 (SFIA 6), 2015	<SFIA CODE>
<NAME>	Skills Framework for the Information Age, V6 (SFIA 6), 2015	<SFIA CODE>

[5] SFIA Foundation, "SFIA V6, the sixth major version of the Skills Framework for the Information Age.," *https://www.sfia-online.org/en/framework/sfia-6*
[6] 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, *https://standards.cen.eu/dyn/www/f?p=204:110:0:::FSP_PROJECT:41798&cs=13E00999DD92E702F0E171397CF76EC87*
[7] The Institute of Internal Auditors® (IIA®), "Core Principles for the Professional Practice of Internal Auditing," *https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Core-Principles-for-the-Professional-Practice-of-Internal-Auditing.aspx*

3.8 Component: Policies and Procedures

This component provides detailed guidance on policies and procedures that are relevant for the governance or management objective. The name of relevant policies and procedures is included, with a description of the purpose and content of the policy (**figure 3.10**).

Where relevant, references to other standards and additional guidance are included. The Related Guidance cites specific chapters or sections within the related guidance where more information can be consulted. A complete list of sources is included in Appendix C.

Figure 3.10—Display of Policies and Procedures Component			
E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
<NAME>	<DESCRIPTION>	<STANDARD NAME>	<TEXT>

3.9 Component: Culture, Ethics and Behavior

The governance component on culture, ethics and behavior provides detailed guidance on desired cultural elements within the organization that support the achievement of a governance or management objective (**figure 3.11**). Where relevant, references to other standards and additional guidance are included. The Related Guidance cites specific chapters or sections within related guidance where more information can be consulted. A complete list of sources is included in Appendix C.

Figure 3.11—Display of Culture, Ethics and Behavior Component		
F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
<NAME>	<STANDARD NAME>	<TEXT>

3.10 Component: Services, Infrastructure and Applications

The services, infrastructure and applications governance component provides detailed guidance on third-party services, types of infrastructure and categories of applications that can be applied to support the achievement of a governance or management objective. Guidance is generic (to avoid naming specific vendors or products); however, entries do provide direction for enterprises to build their governance system for I&T (**figure 3.12**).

Figure 3.12—Display of Services, Infrastructure and Applications Component
G. Component: Services, Infrastructure and Applications
<CATEGORY OF SERVICES, INFRASTRUCTURE OR APPLICATIONS>

Page intentionally left blank

Chapter 4
COBIT Governance and Management Objectives—Detailed Guidance

COBIT Core Model

4.1 Evaluate, Direct and Monitor (EDM)

01 Ensured Governance Framework Setting and Maintenance

02 Ensured Benefits Delivery

03 Ensured Risk Optimization

04 Ensured Resource Optimization

05 Ensured Stakeholder Engagement

Page intentionally left blank

Domain: Evaluate, Direct and Monitor Governance Objective: EDM01 — Ensured Governance Framework Setting and Maintenance	Focus Area: COBIT Core Model

Description

Analyze and articulate the requirements for the governance of enterprise I&T. Put in place and maintain governance components with clarity of authority and responsibilities to achieve the enterprise's mission, goals and objectives.

Purpose

Provide a consistent approach integrated and aligned with the enterprise governance approach. I&T-related decisions are made in line with the enterprise's strategies and objectives and desired value is realized. To that end, ensure that I&T-related processes are overseen effectively and transparently; compliance with legal, contractual and regulatory requirements is confirmed; and the governance requirements for board members are met.

The governance objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG03 Compliance with external laws and regulations • EG08 Optimization of internal business process functionality • EG12 Managed digital transformation programs	• AG01 I&T compliance and support for business compliance with external laws and regulations • AG03 Realized benefits from I&T-enabled investments and services portfolio

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG03	a. Cost of regulatory noncompliance, including settlements and fines b. Number of regulatory noncompliance issues causing public comment or negative publicity c. Number of noncompliance matters noted by regulators d. Number of regulatory noncompliance issues relating to contractual agreements with business partners	AG01	a. Cost of IT noncompliance, including settlements and fines, and the impact of reputational loss b. Number of IT-related noncompliance issues reported to the board, or causing public comment or embarrassment c. Number of noncompliance issues relating to contractual agreements with IT service providers
EG08	a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities	AG03	a. Percent of I&T-enabled investments for which claimed benefits in the business case are met or exceeded b. Percent of I&T services for which expected benefits (as stated in service level agreements) are realized
EG12	a. Number of programs on time and within budget b. Percent of stakeholders satisfied with program delivery c. Percent of business transformation programs stopped d. Percent of business transformation programs with regular reported status updates		

A. Component: Process

Governance Practice	Example Metrics
EDM01.01 Evaluate the governance system. Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and evaluate the current and future design of governance of enterprise I&T.	a. Number of guiding principles defined for I&T governance and decision making b. Number of senior executives involved in setting governance direction for I&T

Activities	Capability Level
1. Analyze and identify the internal and external environmental factors (legal, regulatory and contractual obligations) and trends in the business environment that may influence governance design.	2
2. Determine the significance of I&T and its role with respect to the business.	
3. Consider external regulations, laws and contractual obligations and determine how they should be applied within the governance of enterprise I&T.	
4. Determine the implications of the overall enterprise control environment with regard to I&T.	
5. Align the ethical use and processing of information and its impact on society, the natural environment, and internal and external stakeholder interests with the enterprise's direction, goals and objectives.	3
6. Articulate principles that will guide the design of governance and decision making of I&T.	
7. Determine the optimal decision-making model for I&T.	
8. Determine the appropriate levels of authority delegation, including threshold rules, for I&T decisions.	

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	GE.AG Apply Governance System; GE.MG Monitor Governance System
ISO/IEC 38500:2015(E)	5.2 Principle 1: Responsibility (Evaluate)
ITIL V3, 2011	Service Strategy, 2.3 Governance and management systems
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.1 Preparation (Tasks 2, 3, 4, 5)
Governance Practice	**Example Metrics**
EDM01.02 Direct the governance system. Inform leaders on I&T governance principles and obtain their support, buy-in and commitment. Guide the structures, processes and practices for the governance of I&T in line with the agreed governance principles, decision-making models and authority levels. Define the information required for informed decision making.	a. Degree to which agreed-on I&T governance principles are evident in processes and practices (percentage of processes and practices traceable to principles) b. Frequency of I&T governance reporting to executive committee and board c. Number of roles, responsibilities and authorities for I&T governance that are defined, assigned and accepted by appropriate business and I&T management

Activities	Capability Level
1. Communicate governance of I&T principles and agree with executive management on the way to establish informed and committed leadership.	2
2. Establish or delegate the establishment of governance structures, processes and practices in line with agreed-on design principles.	
3. Establish an I&T governance board (or equivalent) at the board level. This board should ensure that governance of information and technology, as part of enterprise governance, is adequately addressed; advise on strategic direction; and determine prioritization of I&T-enabled investment programs in line with the enterprise's business strategy and priorities.	
4. Allocate responsibility, authority and accountability for I&T decisions in line with agreed-on governance design principles, decision-making models and delegation.	3
5. Ensure that communication and reporting mechanisms provide those responsible for oversight and decision making with appropriate information.	
6. Direct that staff follow relevant guidelines for ethical and professional behavior and ensure that consequences of noncompliance are known and enforced.	
7. Direct the establishment of a reward system to promote desirable cultural change.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	GE.DG Direct Governance System
ISF, The Standard of Good Practice for Information Security 2016	SG1.1 Security Governance Framework
ISO/IEC 38500:2015(E)	5.2 Principle 1: Responsibility (Direct)
ISO/IEC 38502:2017(E)	Governance of IT - Framework and model (all chapters)
King IV Report on Corporate Governance for South Africa, 2016	Part 5.4: Governance functional areas - Principle 12
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.14 Planning (PL-2, PL-10)
Governance Practice	**Example Metrics**
EDM01.03 Monitor the governance system. Monitor the effectiveness and performance of the enterprise's governance of I&T. Assess whether the governance system and implemented mechanisms (including structures, principles and processes) are operating effectively and provide appropriate oversight of I&T to enable value creation.	a. Actual vs. target cycle time for key decisions b. Frequency of independent reviews of I&T governance c. Level of stakeholder satisfaction (measured through surveys) d. Number of I&T governance issues reported

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Assess the effectiveness and performance of those stakeholders given delegated responsibility and authority for governance of enterprise I&T.	3
2. Periodically assess whether agreed-on governance of I&T mechanisms (structures, principles, processes, etc.) are established and operating effectively.	4
3. Assess the effectiveness of the governance design and identify actions to rectify any deviations found.	
4. Maintain oversight of the extent to which I&T satisfies obligations (regulatory, legislation, common law, contractual), internal policies, standards and professional guidelines.	
5. Provide oversight of the effectiveness of, and compliance with, the enterprise's system of control.	
6. Monitor regular and routine mechanisms for ensuring that the use of I&T complies with relevant obligations (regulatory, legislation, common law, contractual), standards and guidelines.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISO/IEC 38500:2015(E)	5.2 Principle 1: Responsibility (Monitor)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.14 Planning (PL-11)

B. Component: Organizational Structures						
Key Governance Practice	**Board**	**Executive Committee**	**Chief Executive Officer**	**Chief Information Officer**	**I&T Governance Board**
EDM01.01 Evaluate the governance system.	A	R	R	R	R
EDM01.02 Direct the governance system.	A	R			R
EDM01.03 Monitor the governance system.	A	R	R	R	R

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
COSO Enterprise Risk Management, June 2017	6. Governance and Culture—Principle 2
ISO/IEC 38502:2017(E)	5.1 Responsibilities of the governing body
King IV Report on Corporate Governance for South Africa, 2016	Part 2: Fundamental concepts—Definition of corporate governance; Part 5.3: Governing structures and delegation—Principle 6 & 7

C. Component: Information Flows and Items (see also Section 3.6)				
Governance Practice	**Inputs**		**Outputs**	
EDM01.01 Evaluate the governance system.	**From**	**Description**	**Description**	**To**
	MEA03.02	Communications of changed compliance requirements	Enterprise governance guiding principles	All EDM; APO01.01; APO01.03 APO01.04
	Outside COBIT	• Constitution/bylaws/ statutes of organization • Governance/decision-making model • Laws/regulations • Business environment trends	Decision-making model	All EDM; APO01.01; APO01.04
			Authority levels	All EDM; APO01.05
EDM01.02 Direct the governance system.			Enterprise governance communication	All EDM; APO01.02
			Reward system approach	APO07.03; APO07.04
EDM01.03 Monitor the governance system.	MEA01.04	Performance reports	Feedback on governance effectiveness and performance	All EDM; APO01.11
	MEA01.05	Status and results of actions		
	MEA02.01	• Results of internal control monitoring and reviews • Results of benchmarking and other evaluations		
	MEA02.03	Results of reviews of self-assessments		
	MEA03.03	Compliance confirmations		
	MEA03.04	• Compliance assurance reports • Reports of noncompliance issues and root causes		
	MEA04.02	Assurance plans		
	Outside COBIT	• Audit reports • Obligations		

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.1 Preparation (Task 2, 3, 4, 5): Inputs and Outputs

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
IS governance	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.9. IS Governance
IT governance	Skills Framework for the Information Age V6, 2015	GOVN

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Delegation of authority policy	Specifies the authority that the board strictly retains for itself. Enumerates general principles of delegation of authority and schedule of delegation (including clear boundaries). Defines organizational structures to which the board delegates authority.	(1) ISO/IEC 38500:2015(E); (2) ISO/IEC 38502:2017(E); (3) King IV Report on Corporate Governance for South Africa, 2016	(1) 5.2 Principle 1: Responsibility; (2) 5.3 Delegation; (3) Part 5.3: Governing structures and delegation Principle—8 and 10
Governance policy	Provides guiding principles of governance (e.g., I&T governance is critical to enterprise success; I&T and the business align strategically; business requirements and benefits determine priorities; enforcement must be equitable, timely and consistent; industry best practices, frameworks and standards must be assessed and implemented as appropriate). Includes governance imperatives, such as building trust and partnerships, to be successful. Emphasizes that I&T governance reflects a process of continual improvement and must be tailored, maintained and updated to ensure relevance.	National Institute of Standards and Technology Special Publication 800- 53, Revision 5 (Draft), August 2017	3.14 Planning (PL-1)

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Identify and communicate the decision-making culture, organizational ethics and individual behaviors that embody enterprise values. Demonstrate ethical leadership and set the tone at the top.	(1) National Institute of Standards and Technology Special Publication 800-53, Revision 5, August 2017; (2) ISO/IEC 38500:2015(E); (3) King IV Report on Corporate Governance for South Africa, 2016	(1) 3.14 Planning (PL-4); (2) 4.1 Principles; (3) Part 5.1: Leadership, ethics and corporate citizenship - Principle 2

G. Component: Services, Infrastructure and Applications
• COBIT and related products/tools • Equivalent frameworks and standards

Page intentionally left blank

Domain: Evaluate, Direct and Monitor Governance Objective: EDM02 — Ensured Benefits Delivery	Focus Area: COBIT Core Model

Description

Optimize the value to the business from investments in business processes, I&T services and I&T assets.

Purpose

Secure optimal value from I&T-enabled initiatives, services and assets; cost-efficient delivery of solutions and services; and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.

The governance objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG08 Optimization of internal business process functionality • EG12 Managed digital transformation programs	AG03 Realized benefits from I&T-enabled investments and services portfolio
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG08 a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities	AG03 a. Percent of I&T-enabled investments for which claimed benefits in the business case are met or exceeded b. Percent of I&T services for which expected benefits (as stated in service level agreements) are realized
EG12 a. Number of programs on time and within budget b. Percent of stakeholders satisfied with program delivery c. Percent of business transformation programs stopped d. Percent of business transformation programs with regular reported status updates	

A. Component: Process

Governance Practice	Example Metrics
EDM02.01 Establish the target investment mix. Review and ensure clarity of the enterprise and I&T strategies and current services. Define an appropriate investment mix based on cost, alignment with strategy, type of benefit for the programs in the portfolio, degree of risk, and financial measures such as cost and expected return on investment (ROI) over the full economic life cycle. Adjust the enterprise and I&T strategies where necessary.	a. Percent of I&T investments traceable to enterprise strategy b. Percent of I&T investments based on cost, alignment with strategy, financial measures (e.g., cost and ROI over the full economic life cycle), degree of risk and type of benefit for the programs in the portfolio

Activities	Capability Level
1. Create and maintain portfolios of I&T-enabled investment programs, IT services and IT assets, which form the basis for the current IT budget and support the I&T tactical and strategic plans.	2
2. Obtain a common understanding between IT and the other business functions on the potential opportunities for IT to enable and contribute to enterprise strategy.	
3. Identify the broad categories of information systems, applications, data, IT services, infrastructure, I&T assets, resources, skills, practices, controls and relationships needed to support the enterprise strategy.	
4. Agree on I&T goals, taking into account the interrelationships between the enterprise strategy and the I&T services, assets and other resources. Identify and leverage synergies that can be achieved.	
5. Define an investment mix that achieves the right balance among a number of dimensions, including an appropriate balance of short- and long-term returns, financial and nonfinancial benefits, and high- and low-risk investments.	3

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
King IV Report on Corporate Governance for South Africa, 2016	Part 5.5: Stakeholder relationships—Principle 17
The Open Group IT4IT Reference Architecture, Version 2.0	3.2 IT Value Chain and IT4IT Reference Architecture

A. Component: Process *(cont.)*	
Governance Practice	**Example Metrics**
EDM02.02 Evaluate value optimization. Continually evaluate the portfolio of I&T-enabled investments, services and assets to determine the likelihood of achieving enterprise objectives and delivering value. Identify and evaluate any changes in direction to management that will optimize value creation.	a. Deviation between target and actual investment mix b. Percent of portfolio of I&T-enabled investments with a likelihood of achieving enterprise objectives and delivering value at a reasonable cost

Activities	Capability Level
1. Understand stakeholder requirements; strategic I&T issues, such as dependence on I&T; and technology insights and capabilities regarding the actual and potential significance of I&T for the enterprise's strategy.	2
2. Understand the key elements of governance required for the reliable, secure and cost-effective delivery of optimal value from the use of existing and new I&T services, assets and resources.	3
3. Understand and regularly discuss the opportunities that could arise for the enterprise from changes enabled by current, new or emerging technologies, and optimize the value created from those opportunities.	
4. Understand what constitutes value for the enterprise, and consider how well it is communicated, understood and applied throughout the enterprise's processes.	
5. Evaluate how effectively the enterprise and I&T strategies have been integrated and aligned within the enterprise and with enterprise goals for delivering value.	4
6. Understand and consider how effective current roles, responsibilities, accountabilities and decision-making bodies are in ensuring value creation from I&T-enabled investments, services and assets.	
7. Consider how well the management of I&T-enabled investments, services and assets aligns with enterprise value management and financial management practices.	
8. Evaluate the portfolio of investments, services and assets for alignment with the enterprise's strategic objectives; enterprise worth, both financial and nonfinancial; risk, both delivery risk and benefits risk; business process alignment; effectiveness in terms of usability, availability and responsiveness; and efficiency in terms of cost, redundancy and technical health.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
COSO Enterprise Risk Management, June 2017	7. Strategy and Objective-Setting—Principle 8
ISF, The Standard of Good Practice for Information Security 2016	SG2.2 Stakeholder Value Delivery
ISO/IEC 38500:2015(E)	5.3 Principle 2: Strategy (Evaluate)
King IV Report on Corporate Governance for South Africa, 2016	Part 5.2: Strategy, performance and reporting—Principle 4
The Open Group IT4IT Reference Architecture, Version 2.0	5. Strategy to Portfolio (S2P) Value Stream

Governance Practice	Example Metrics
EDM02.03 Direct value optimization. Direct value management principles and practices to enable optimal value realization from I&T-enabled investments throughout their full economic life cycle.	a. Percent of I&T initiatives in the overall portfolio in which value is managed through the full life cycle b. Percent of I&T initiatives using value management principles and practices

Activities	Capability Level
1. Define and communicate portfolio and investment types, categories, criteria and relative weightings to the criteria to allow for overall relative value scores.	2
2. Define requirements for stage-gates and other reviews for significance of the investment to the enterprise and associated risk, program schedules, funding plans, and the delivery of key capabilities and benefits and ongoing contribution to value.	3
3. Direct management to consider potential innovative uses of I&T that enable the enterprise to respond to new opportunities or challenges, undertake new business, increase competitiveness, or improve processes.	
4. Direct any required changes in assignment of accountabilities and responsibilities for executing the investment portfolio and delivering value from business processes and services.	
5. Direct any required changes to the portfolio of investments and services to realign with current and expected enterprise objectives and/or constraints.	
6. Recommend consideration of potential innovations, organizational changes or operational improvements that could drive increased value for the enterprise from I&T-enabled initiatives.	
7. Define and communicate enterprise-level value delivery goals and outcome measures to enable effective monitoring.	4

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISO/IEC 38500:2015(E)	5.3 Principle 2: Strategy (Direct)
Governance Practice	**Example Metrics**
EDM02.04 Monitor value optimization. Monitor key goals and metrics to determine whether the enterprise receives expected value and benefit from I&T-enabled investments and services. Identify significant issues and consider corrective actions.	a. Number of new enterprise opportunities realized as a direct result of I&T developments b. Percent of strategic enterprise objectives achieved as a result of strategic I&T initiatives c. Level of executive management satisfaction with I&T's value delivery and cost d. Level of stakeholder satisfaction with progress toward identified goals (value delivery based on surveys) e. Level of stakeholder satisfaction with the enterprise's ability to obtain value from I&T-enabled initiatives f. Number of incidents that occur due to actual or attempted circumvention of established value management principles and practices g. Percent of expected value realized

Activities	Capability Level
1. Define a balanced set of performance objectives, metrics, targets and benchmarks. Metrics should cover activity and outcome measures, including lead and lag indicators for outcomes, as well as an appropriate balance of financial and nonfinancial measures. Review and agree on them with IT and other business functions, and other relevant stakeholders.	4
2. Collect relevant, timely, complete, credible and accurate data to report on progress in delivering value against targets. Obtain a succinct, high-level, all-around view of portfolio, program and I&T (technical and operational capabilities) performance that supports decision making. Ensure that expected results are being achieved.	
3. Obtain regular and relevant portfolio, program and I&T (technological and functional) performance reports. Review the enterprise's progress toward identified goals and the extent to which planned objectives have been achieved, deliverables obtained, performance targets met and risk mitigated.	
4. Upon review of reports, ensure that appropriate management corrective action is initiated and controlled.	5
5. Upon review of reports, take appropriate management action as required to ensure that value is optimized.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISO/IEC 38500:2015(E)	5.3 Principle 2: Strategy (Monitor)

B. Component: Organizational Structures									
Key Governance Practice	**Board**	**Executive Committee**	**Chief Executive Officer**	**Chief Financial Officer**	**Chief Operating Officer**	**Chief Information Officer**	**I&T Governance Board**	**Portfolio Manager**	
EDM02.01 Establish the target investment mix.	A	R	R	R	R	R	R		
EDM02.02 Evaluate value optimization.	A	R	R	R	R	R	R		
EDM02.03 Direct value optimization.	A	R	R	R	R	R	R		
EDM02.04 Monitor value optimization.	A	R	R	R	R	R	R	R	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference	
King IV Report on Corporate Governance for South Africa, 2016	Part 2: Fundamental concepts—Definition of corporate governance	

C. Component: Information Flows and Items (see also Section 3.6)				
Governance Practice	**Inputs**		**Outputs**	
EDM02.01 Establish the target investment mix.	**From**	**Description**	**Description**	**To**
	APO02.05	• Definition of strategic initiatives • Risk assessment initiatives • Strategic road map	Feedback on strategy and goals	APO02.05
	APO09.01	Definitions of standard services	Identified resources and capabilities required to support strategy	Internal
	BAI03.11	Service definitions	Defined investment mix	Internal; EDM02.03
	EDM02.03	Investment types and criteria		
EDM02.02 Evaluate value optimization.	APO02.05	Strategic road map	Evaluation of strategic alignment	APO02.04; APO05.02
	APO05.01	Investment return expectations	Evaluation of investment and services portfolios	APO05.02; APO05.03; APO06.02
	APO05.02	Selected programs with ROI milestones		
	APO05.05	Benefit results and related communications		
	BAI01.06	Stage-gate review results		
EDM02.03 Direct value optimization.	APO05.03	Investment portfolio performance reports	Requirements for stage-gate reviews	BAI01.01; BAI11.01
	EDM02.01	Defined investment mix	Investment types and criteria	EDM02.01; APO05.02
EDM02.04 Monitor value optimization.	APO05.03	Investment portfolio performance reports	Actions to improve value delivery	APO05.03; APO06.02; BAI01.01; BAI11.01; EDM05.01
			Feedback on portfolio and program performance	APO05.03; APO06.05; BAI01.06
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
No related guidance for this component				

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Benefits management	Skills Framework for the Information Age V6, 2015	BENM

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Budgeting and delivery execution policy	Sets guidelines to identify needs and requirements for investments, monitor fulfillment, and ensure maximum benefit. Addresses formulation of budget requests. Monitors budget and technical performance execution to plan. Recommends reallocation or reprogramming as warranted. Addresses monitoring of performance against service level agreements and other performance-based metrics.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
The value that I&T adds depends on the degree to which I&T is aligned with the business and meets its expectations. Optimize I&T value by establishing a culture in which I&T services are delivered on time and within budget, with appropriate quality.		

G. Component: Services, Infrastructure and Applications
• Cost accounting system • Program management tool

Page intentionally left blank

Domain: Evaluate, Direct and Monitor Governance Objective: EDM03 — Ensured Risk Optimization	Focus Area: COBIT Core Model

Description

Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of I&T is identified and managed.

Purpose

Ensure that I&T-related enterprise risk does not exceed the enterprise's risk appetite and risk tolerance, the impact of I&T risk to enterprise value is identified and managed, and the potential for compliance failures is minimized.

The governance objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG02 Managed business risk • EG06 Business service continuity and availability	• AG02 Managed I&T-related risk • AG07 Security of information, processing infrastructure and applications, and privacy

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG02	a. Percent of critical business objectives and services covered by risk assessment b. Ratio of significant incidents that were not identified in risk assessments vs. total incidents c. Frequency of updating risk profile	AG02	a. Frequency of updating risk profile b. Percent of enterprise risk assessments including I&T-related risk c. Number of significant I&T-related incidents that were not identified in a risk assessment
EG06	a. Number of customer service or business process interruptions causing significant incidents b. Business cost of incidents c. Number of business processing hours lost due to unplanned service interruptions d. Percent of complaints as a function of committed service availability targets	AG07	a. Number of confidentiality incidents causing financial loss, business disruption or public embarrassment b. Number of availability incidents causing financial loss, business disruption or public embarrassment c. Number of integrity incidents causing financial loss, business disruption or public embarrassment

A. Component: Process

Governance Practice	Example Metrics
EDM03.01 Evaluate risk management. Continually examine and evaluate the effect of risk on the current and future use of I&T in the enterprise. Consider whether the enterprise's risk appetite is appropriate and ensure that risk to enterprise value related to the use of I&T is identified and managed.	a. Level of unexpected enterprise impact b. Percent of I&T risk that exceeds enterprise risk tolerance c. Refreshment rate of risk factor evaluation

Activities	Capability Level
1. Understand the organization and its context related to I&T risk.	2
2. Determine the risk appetite of the organization, i.e., the level of I&T-related risk that the enterprise is willing to take in its pursuit of enterprise objectives.	
3. Determine risk tolerance levels against the risk appetite, i.e., temporarily acceptable deviations from the risk appetite.	
4. Determine the extent of alignment of the I&T risk strategy to the enterprise risk strategy and ensure the risk appetite is below the organization's risk capacity.	
5. Proactively evaluate I&T risk factors in advance of pending strategic enterprise decisions and ensure that risk considerations are part of the strategic enterprise decision process.	3
6. Evaluate risk management activities to ensure alignment with the enterprise's capacity for I&T-related loss and leadership's tolerance of it.	
7. Attract and maintain necessary skills and personnel for I&T Risk Management	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
COSO Enterprise Risk Management, June 2017	Strategy and Objective-Setting—Principles 6 and 7; 9. Review and Revision—Principle 16

A. Component: Process *(cont.)*		
Governance Practice	**Example Metrics**	
EDM03.02 Direct risk management. Direct the establishment of risk management practices to provide reasonable assurance that I&T risk management practices are appropriate and that actual I&T risk does not exceed the board's risk appetite.	a. Level of alignment between I&T risk and enterprise risk b. Percent of enterprise projects that consider I&T risk	
Activities		**Capability Level**
1. Direct the translation and integration of the I&T risk strategy into risk management practices and operational activities.		2
2. Direct the development of risk communication plans (covering all levels of the enterprise).		
3. Direct implementation of the appropriate mechanisms to respond quickly to changing risk and report immediately to appropriate levels of management, supported by agreed principles of escalation (what to report, when, where and how).		
4. Direct that risk, opportunities, issues and concerns may be identified and reported by anyone to the appropriate party at any time. Risk should be managed in accordance with published policies and procedures and escalated to the relevant decision makers.		
5. Identify key goals and metrics of the risk governance and management processes to be monitored, and approve the approaches, methods, techniques and processes for capturing and reporting the measurement information.		3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
CMMI Cybermaturity Platform, 2018	RS.AS Apply Risk Management Strategy; BC.RO Determine Strategic Risk Objectives	
ISF, The Standard of Good Practice for Information Security 2016	IR1.1 Information Risk Assessment—Management Approach	
King IV Report on Corporate Governance for South Africa, 2016	Part 5.4: Governance functional areas—Principle 11	
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.5 Assessment (Task 2)	
Governance Practice	**Example Metrics**	
EDM03.03 Monitor risk management. Monitor the key goals and metrics of the risk management processes. Determine how deviations or problems will be identified, tracked and reported for remediation.	a. Number of potential I&T risk areas identified and managed b. Percent of critical risk that has been effectively mitigated c. Percent of I&T risk action plans executed on time	
Activities		**Capability Level**
1. Report any risk management issues to the board or executive committee.		2
2. Monitor the extent to which the risk profile is managed within the enterprise's risk appetite and tolerance thresholds.		3
3. Monitor key goals and metrics of risk governance and management processes against targets, analyze the cause of any deviations, and initiate remedial actions to address the underlying causes.		4
4. Enable key stakeholders' review of the enterprise's progress toward identified goals.		
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
COSO Enterprise Risk Management, June 2017	9. Review and Revision—Principle 17	
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.1 Preparation (Task 7); 3.5 Assessment (Task 1); 3.6 Authorization (Task 1)	
The Open Group IT4IT Reference Architecture, Version 2.0	6. Requirement to Deploy (R2D) Value Stream; 7. Request to Fulfill (R2F) Value Stream	

B. Component: Organizational Structures

Key Governance Practice	Board	Executive Committee	Chief Executive Officer	Chief Risk Officer	Chief Information Officer	I&T Governance Board	Enterprise Risk Committee	Chief Information Security Officer
EDM03.01 Evaluate risk management.	A	R	R	R	R	R	R	
EDM03.02 Direct risk management.	A	R	R	R	R	R	R	
EDM03.03 Monitor risk management.	A	R	R	R	R	R	R	R

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
COSO Enterprise Risk Management, June 2017	6. Governance and Culture—Principle
King IV Report on Corporate Governance for South Africa, 2016	Part 2: Fundamental concepts—Definition of corporate governance

C. Component: Information Flows and Items (see also Section 3.6)

Governance Practice	Inputs		Outputs	
	From	Description	Description	To
EDM03.01 Evaluate risk management.	APO12.01	Emerging risk issues and factors	Risk appetite guidance	APO04.01; APO12.03
	Outside COBIT	Enterprise risk management (ERM) principles	Evaluation of risk management activities	APO12.01
			Approved risk tolerance levels	APO12.03
EDM03.02 Direct risk management.	APO12.03	Aggregated risk profile, including status of risk management actions	Approved process for measuring risk management	APO12.01
	Outside COBIT	Enterprise risk management (ERM) profiles and mitigation plans	Key objectives to be monitored for risk management	APO12.01
			Risk management policies	APO12.01
EDM03.03 Monitor risk management.	APO12.02	Risk analysis results	Remedial actions to address risk management deviations	APO12.06
	APO12.04	• Risk analysis and risk profile reports for stakeholders • Results of third-party risk assessments • Opportunities for acceptance of greater risk	Risk management issues for the board	EDM05.01

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.1 Preparation (Task 7): Inputs and Outputs; 3.5 Assessment (Tasks 1, 2): Inputs 2, and Outputs; 3.6 Authorization (Task 1): Inputs and Outputs

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Business risk management	Skills Framework for the Information Age V6, 2015	BURM
Risk management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.3. Risk Management

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Enterprise risk policy	Defines governance and management of enterprise risk at strategic, tactical and operational levels, pursuant to business objectives. Translates enterprise governance into risk governance principles and policy and elaborates risk management activities.	National Institute of Standards and Technology Special Publication 800- 53, Revision 5 (Draft), August 2017	3.17 Risk assessment (RA-1)

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Promote an I&T risk-aware culture at all levels of the organization and empower the enterprise proactively to identify, report and escalate I&T risk, opportunity and potential business impacts. Senior management sets direction and demonstrates visible and genuine support for risk practices. Additionally, management must clearly define risk appetite and ensure an appropriate level of debate as part of business-as-usual activities. Desirable behaviors include encouraging employees to raise issues or negative outcomes and show transparency with regard to I&T risk. Business owners should accept ownership of I&T risk when applicable and demonstrate genuine commitment to I&T risk management by providing adequate resource levels.	COSO Enterprise Risk Management, June 2017	6. Governance and Culture—Principles 3 and 4

G. Component: Services, Infrastructure and Applications
Risk management system

Domain: Evaluate, Direct and Monitor Governance Objective: EDM04 — Ensured Resource Optimization	Focus Area: COBIT Core Model

Description

Ensure that adequate and sufficient business and I&T-related resources (people, process and technology) are available to support enterprise objectives effectively and, at optimal cost.

Purpose

Ensure that the resource needs of the enterprise are met in the optimal manner, I&T costs are optimized, and there is an increased likelihood of benefit realization and readiness for future change.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG08 Optimization of internal business process functionality • EG12 Managed digital transformation programs	AG09 Delivering programs on time, on budget and meeting requirements and quality standards

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG01	a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG09	a. Number of programs/projects on time and within budget b. Number of programs needing significant rework due to quality defects c. Percent of stakeholders satisfied with program/project quality
EG08	a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities		
EG12	a. Number of programs on time and within budget b. Percent of stakeholders satisfied with program delivery c. Percent of business transformation programs stopped d. Percent of business transformation programs with regular reported status updates		

A. Component: Process

Governance Practice	Example Metrics
EDM04.01 Evaluate resource management. Continually examine and evaluate the current and future need for business and I&T resources (financial and human), options for resourcing (including sourcing strategies), and allocation and management principles to meet the needs of the enterprise in the optimal manner.	a. Number of deviations from the resource plan b. Percent of resource plan and enterprise architecture strategies delivering value and mitigating risk with allocated resources

Activities	Capability Level
1. Starting from the current and future strategies, examine the potential options for providing I&T-related resources (technology, financial and human resources), and develop capabilities to meet current and future needs (including sourcing options).	2
2. Define the key principles for resource allocation and management of resources and capabilities so I&T can meet the needs of the enterprise according to the agreed priorities and budgetary constraints. For example, define preferred sourcing options for certain services and financial boundaries per sourcing option.	
3. Review and approve the resource plan and enterprise architecture strategies for delivering value and mitigating risk with the allocated resources.	
4. Understand requirements for aligning I&T resource management with enterprise financial and human resources (HR) planning.	
5. Define principles for the management and control of the enterprise architecture.	3

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	GR.DR Direct Resource Management Needs
ISO/IEC 38500:2015(E)	5.4 Principle 3: Acquisition (Evaluate)

A. Component: Process *(cont.)*	
Governance Practice	**Example Metrics**
EDM04.02 Direct resource management. Ensure the adoption of resource management principles to enable optimal use of business and I&T resources throughout their full economic life cycle.	a. Number of deviations from, and exceptions to, resource management principles b. Percent of reuse of architecture components
Activities	**Capability Level**
1. Assign responsibilities for executing resource management.	2
2. Establish principles related to safeguarding resources.	
3. Communicate and drive the adoption of the resource management strategies, principles, and agreed resource plan and enterprise architecture strategies.	3
4. Align resource management with enterprise financial and HR planning.	
5. Define key goals, measures and metrics for resource management.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	GR.ER Evaluate Resource Management Needs
COSO Enterprise Risk Management, June 2017	6. Governance and Culture—Principle 5
ISO/IEC 38500:2015(E)	5.4 Principle 3: Acquisition (Direct)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.14 Planning (PL-4)
Governance Practice	**Example Metrics**
EDM04.03 Monitor resource management. Monitor the key goals and metrics of the resource management processes. Determine how deviations or problems will be identified, tracked and reported for remediation.	a. Level of stakeholder feedback on resource optimization b. Number of benefits (e.g., cost savings) achieved through optimum utilization of resources c. Number of resource management performance targets realized d. Percent of projects and programs with a medium- or high-risk status due to resource management issues e. Percent of projects with appropriate resource allocations
Activities	**Capability Level**
1. Monitor the allocation and optimization of resources in accordance with enterprise objectives and priorities using agreed goals and metrics.	4
2. Monitor I&T-related sourcing strategies, enterprise architecture strategies, and business- and IT-related capabilities and resources to ensure that current and future needs and objectives of the enterprise can be met.	
3. Monitor resource performance against targets, analyze the cause of deviations, and initiate remedial action to address the underlying causes.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	GR.MR Monitor Resource Management Needs
ISO/IEC 38500:2015(E)	5.4 Principle 3: Acquisition (Evaluate)

B. Component: Organizational Structures						
Key Governance Practice	Board	Executive Committee	Chief Executive Officer	Chief Operating Officer	Chief Information Officer	I&T Governance Board
EDM04.01 Evaluate resource management.	A	R	R	R	R	R
EDM04.02 Direct resource management.	A	R	R	R	R	R
EDM04.03 Monitor resource management.	A	R	R	R	R	R

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
King IV Report on Corporate Governance for South Africa, 2016	Part 2: Fundamental concepts—Definition of corporate governance

C. Component: Information Flows and Items (see also Section 3.6)				
Governance Practice	Inputs		Outputs	
	From	Description	Description	To
EDM04.01 Evaluate resource management.	APO02.04	Gaps and changes required to realize target capability	Guiding principles for allocation of resources and capabilities	APO02.01; APO07.01; BAI03.11
	APO07.03	Skill development plans	Approved resources plan	APO02.05; APO07.01; APO09.02
	APO10.02	Decision results of vendor evaluations	Guiding principles for enterprise architecture	APO03.01
EDM04.02 Direct resource management.			Principles for safeguarding resources	APO01.02
			Assigned responsibilities for resource management	APO01.05; DSS06.03
			Communication of resourcing strategies	APO02.06; APO07.05; APO09.02
EDM04.03 Monitor resource management.			Remedial actions to address resource management deviations	APO02.05; APO07.01; APO07.03; APO09.04
			Feedback on allocation and effectiveness of resources and capabilities	EDM05.01; APO02.02; APO07.05; APO09.05

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Portfolio management	Skills Framework for the Information Age V6, 2015	POMG
Resourcing	Skills Framework for the Information Age V6, 2015	RESC

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Performance measurement policy	Identifies the need for a performance measurement system beyond conventional accounting. This system encompasses measurement of relationships and knowledge-based assets necessary to compete in the information age, including customer focus, process efficiency and the ability to learn and grow (balanced scorecard). The balanced scorecard translates strategy into action to achieve enterprise goals, taking into account intangibles like customer satisfaction, streamlining of internal functions, creation of operational efficiencies and development of staff skills. This holistic view of operations helps link long-term strategic objectives and short-term actions.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Establish a culture in which resources are valued and the investment, use and allocation of resources (whether people, information, applications, technology or facilities) align with organizational needs. Illustrate these values by ensuring that appropriate methods and adequate skills exist in the organization; for example, ensure that benefits from service procurement are real and achievable, and implement sound performance measurement systems (e.g., the balanced scorecard).		

G. Component: Services, Infrastructure and Applications
Performance measurement system (e.g., balanced scorecard, skills management tools)

Domain: Evaluate, Direct and Monitor Governance Objective: EDM05 — Ensured Stakeholder Engagement	Focus Area: COBIT Core Model

Description

Ensure that stakeholders are identified and engaged in the I&T governance system and that enterprise I&T performance and conformance measurement and reporting are transparent, with stakeholders approving the goals and metrics and necessary remedial actions.

Purpose

Ensure that stakeholders are supportive of the I&T strategy and road map, communication to stakeholders is effective and timely, and the basis for reporting is established to increase performance. Identify areas for improvement, and confirm that I&T-related objectives and strategies are in line with the enterprise's strategy.

The governance objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG04 Quality of financial information • EG07 Quality of management information	AG10 Quality of I&T management information

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG04	a. Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of enterprise financial information b. Cost of noncompliance with finance-related regulations	AG10	a. Level of user satisfaction with quality, timeliness and availability of I&T-related management information, taking into account available resources b. Ratio and extent of erroneous business decisions in which erroneous or unavailable I&T-related information was a key factor c. Percentage of information meeting quality criteria
EG07	a. Degree of board and executive management satisfaction with decision-making information b. Number of incidents caused by incorrect business decisions based on inaccurate information c. Time to provide information supporting effective business decisions d. Timeliness of management information		

A. Component: Process

Governance Practice	Example Metrics
EDM05.01 Evaluate stakeholder engagement and reporting requirements. Continually examine and evaluate current and future requirements for stakeholder engagement and reporting (including reporting mandated by regulatory requirements), and communication to other stakeholders. Establish principles for engaging and communicating with stakeholders.	a. Date of last revision to reporting requirements b. Percent of stakeholders covered in reporting requirements

Activities	Capability Level
1. Identify all relevant I&T stakeholders within and outside the enterprise. Group stakeholders in stakeholder categories with similar requirements.	2
2. Examine and make judgment on the current and future mandatory reporting requirements relating to the use of I&T within the enterprise (regulation, legislation, common law, contractual), including extent and frequency.	
3. Examine and make judgment on the current and future communication and reporting requirements for other stakeholders relating to the use of I&T within the enterprise, including required level of involvement/consultation and extent of communication/level of detail and conditions.	
4. Maintain principles for communication with external and internal stakeholders, including communication formats and channels, and for stakeholder acceptance and sign-off of reporting.	3

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	SR.DR Direct Stakeholder Communication and Reporting

A. Component: Process *(cont.)*	
Governance Practice	**Example Metrics**
EDM05.02 Direct stakeholder engagement, communication and reporting. Ensure the establishment of effective stakeholder involvement, communication and reporting, including mechanisms for ensuring the quality and completeness of information, overseeing mandatory reporting, and creating a communication strategy for stakeholders.	a. Number of breaches of mandatory reporting requirements b. Stakeholder satisfaction with communication and reporting

Activities	Capability Level
1. Direct the establishment of the consultation and communication strategy for external and internal stakeholders.	2
2. Direct the implementation of mechanisms to ensure that information meets all criteria for mandatory I&T reporting requirements for the enterprise.	
3. Establish mechanisms for validation and approval of mandatory reporting.	
4. Establish reporting escalation mechanisms.	3

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	SR.AR Apply Stakeholder Reporting Requirements
King IV Report on Corporate Governance for South Africa, 2016	Part 5.5: Stakeholder relationships—Principle 16
King IV Report on Corporate Governance for South Africa, 2016	Part 5.2: Strategy, performance and reporting—Principle 5
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity V1.1, April 2018	3.3 Communicating Cybersecurity Requirements with Stakeholders

Governance Practice	Example Metrics
EDM05.03 Monitor stakeholder engagement. Monitor stakeholder engagement levels and the effectiveness of stakeholder communication. Assess mechanisms for ensuring accuracy, reliability and effectiveness, and ascertain whether the requirements of different stakeholders in terms of reporting and communication are met.	a. Level of stakeholder engagement with enterprise I&T b. Percent of reports containing inaccuracies c. Percent of reports delivered on time

Activities	Capability Level
1. Periodically assess the effectiveness of the mechanisms for ensuring the accuracy and reliability of mandatory reporting.	4
2. Periodically assess the effectiveness of the mechanisms for, and outcomes from, involvement of and communication with external and internal stakeholders.	
3. Determine whether the requirements of different stakeholders are met and assess stakeholder engagement levels.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	SR.MC Monitor Stakeholder Communication

B. Component: Organizational Structures					
Key Governance Practice	**Board**	**Executive Committee**	**Chief Executive Officer**	**Chief Risk Officer**	**Chief Information Officer**
EDM05.01 Evaluate stakeholder engagement and reporting requirements.	A	R	R	R	R
EDM05.02 Direct stakeholder engagement communication and reporting.	A	R	R	R	R
EDM05.03 Monitor stakeholder engagement.	A	R	R	R	R

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
King IV Report on Corporate Governance for South Africa, 2016	Part 2: Fundamental concepts—Definition of corporate governance

C. Component: Information Flows and Items (see also Section 3.6)				
Governance Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
EDM05.01 Evaluate stakeholder engagement and reporting requirements.	EDM02.04	Actions to improve value delivery	Reporting and communications principles	MEA01.01
	EDM03.03	Risk management issues for the board	Evaluation of enterprise reporting requirements	MEA01.01
	EDM04.03	Feedback on allocation and effectiveness of resources and capabilities		
EDM05.02 Direct stakeholder engagement, communication and reporting.	APO12.04	Risk analysis and risk profile reports for stakeholders	Rules for validating and approving mandatory reports	MEA01.01; MEA03.04
			Escalation guidelines	MEA01.05
EDM05.03 Monitor stakeholder engagement.	MEA04.08	• Assurance review results • Assurance review report	Assessment of reporting effectiveness	MEA01.01; MEA03.04

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Relationship management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.4. Relationship Management

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Transparency policy	Addresses the importance of frequent, open communication with all stakeholders to ensure that they understand the strategic importance of I&T to enterprise success. Ensures that transparency supports appropriate risk mitigation, linking transparency and effective risk management to I&T value and enterprise growth.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Create a culture in which open and structured communication is provided to key stakeholders, in line with their requirements.		

G. Component: Services, Infrastructure and Applications
• Communication tools and channels • IT dashboarding • Stakeholder survey tools

Page intentionally left blank

4.2 Align, Plan and Organize (APO)

01 Managed I&T Management Framework

02 Managed Strategy

03 Managed Enterprise Architecture

04 Managed Innovation

05 Managed Portfolio

06 Managed Budget and Costs

07 Managed Human Resources

08 Managed Relationships

09 Managed Service Agreements

10 Managed Vendors

11 Managed Quality

12 Managed Risk

13 Managed Security

14 Managed Data

Page intentionally left blank

Domain: Align, Plan and Organize Management Objective: APO01 — Managed I&T Management Framework	Focus Area: COBIT Core Model

Description

Design the management system for enterprise I&T based on enterprise goals and other design factors. Based on this design, implement all required components of the management system.

Purpose

Implement a consistent management approach for enterprise governance requirements to be met, covering governance components such as management processes; organizational structures; roles and responsibilities; reliable and repeatable activities; information items; policies and procedures; skills and competencies; culture and behavior; and services, infrastructure and applications.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG03 Compliance with external laws and regulations • EG08 Optimization of internal business process functionality • EG11 Compliance with internal policies • EG12 Managed digital transformation programs	• AG03 Realized benefits from I&T-enabled investments and services portfolio • AG11 I&T compliance with internal policies

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG03	a. Cost of regulatory noncompliance, including settlements and fines b. Number of regulatory noncompliance issues causing public comment or negative publicity c. Number of noncompliance matters noted by regulators d. Number of regulatory noncompliance issues relating to contractual agreements with business partners	AG03	a. Percent of I&T-enabled investments for which claimed benefits in the business case are met or exceeded b. Percent of I&T services for which expected benefits (as stated in service level agreements) are realized
EG08	a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities	AG11	a. Number of incidents related to noncompliance with I&T-related policies. b. Number of exceptions to internal policies c. Frequency of policy review and update
EG11	a. Number of incidents related to noncompliance to policy b. Percent of stakeholders who understand policies c. Percent of policies supported by effective standards and working practices		
EG12	a. Number of programs on time and within budget b. Percent of stakeholders satisfied with program delivery c. Percent of business transformation programs stopped d. Percent of business transformation programs with regular reported status updates		

A. Component: Process	
Management Practice	**Example Metrics**
APO01.01 Design the management system for enterprise I&T. Design a management system tailored to the needs of the enterprise. Management needs of the enterprise are defined through the use of the goals cascade and by application of design factors. Ensure the governance components are integrated and aligned with the enterprise's governance and management philosophy and operating style.	a. Number of formal sign-offs by applicable governance structures of the priority objectives for the I&T management system b. Percent of governance components integrated and aligned with the enterprise's governance and management philosophy and operating style

Activities	Capability Level
1. Obtain an understanding of the enterprise vision, direction and strategy as well as the current enterprise context and challenges.	2
2. Consider the enterprise's internal environment, including management culture and philosophy, risk tolerance, security and privacy policy, ethical values, code of conduct, accountability, and requirements for management integrity.	
3. Apply the COBIT goals cascade and design factors to the enterprise strategy and context to decide on priorities for the management system and, thus, for implementation of management objective priorities.	
4. Validate selected priorities for implementation of management objectives with industry-specific good practices or requirements (e.g., industry-specific regulations) and with appropriate governance structures.	3

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
COSO Enterprise Risk Management, June 2017	7. Strategy and Objective-Setting—Principle 9
ISO/IEC 27001:2013/Cor.2:2015(E)	International standard for establishing, implementing and maintaining a management system (all chapters)
ITIL V3, 2011	Service Strategy, 2.3 Governance and management systems

Management Practice	Example Metrics
APO01.02 Communicate management objectives, direction and decisions made. Communicate awareness and promote understanding of alignment and I&T objectives to stakeholders throughout the enterprise. Communicate at regular intervals on important I&T-related decisions and their impact for the organization.	a. Frequency of communication on management objectives and direction for I&T b. Assigned responsibility for sending out regular communications

Activities	Capability Level
1. Provide sufficient and skilled resources to support the communication process.	2
2. Define ground rules for communication by identifying communication needs and implementing plans based on those needs, considering top-down, bottom-up and horizontal communication.	3
3. Continuously communicate I&T objectives and direction. Ensure that communication is supported by executive management in actions and words, using all available channels.	
4. Ensure the information communicated encompasses a clearly articulated mission, service objectives, internal controls, quality, code of ethics/conduct, policies and procedures, roles and responsibilities, etc. Communicate the information at the appropriate level of detail for respective audiences within the enterprise.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO01.03 Implement management processes (to support the achievement of governance and management objectives). Define target process capability levels and implementation priority based on the management system design.	a. Number of priority processes to be implemented or improved to meet the target capability level b. Number of metrics defined for follow-up of successful process implementation

Activities	Capability Level
1. Develop the I&T governance target process model specific to the organization, based on the selection of priority management objectives (output of goals cascade and design factors exercise).	2
2. Analyze the gap between the target process model for the organization and current practices and activities.	3
3. Draft a road map for implementation of missing process practices and activities. Use practice metrics to follow up on successful implementation.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
APO01.04 Define and implement the organizational structures. Put in place the required internal and extended organizational structures (e.g., committees) per the management system design, enabling effective and efficient decision making. Ensure that required technology and information knowledge is included in the composition of management structures.	a. Level of executive satisfaction with management decision making b. Number of decisions that could not be resolved within management structures and were escalated to governance structures

Activities	Capability Level
1. Identify decisions required for the achievement of enterprise outcomes and the I&T strategy and for the management and execution of I&T services.	2
2. Involve stakeholders who are critical to decision making (accountable, responsible, consulted or informed).	
3. Define the scope, focus, mandate and responsibilities of each function within the I&T-related organization, in line with governance direction.	
4. Define the scope of internal and external functions, internal and external roles, and capabilities and decision rights required to cover all practices, including those performed by third parties.	3
5. Align the I&T-related organization with enterprise architecture organizational models.	
6. Establish an I&T steering committee (or equivalent) composed of executive, business and I&T management to track status of projects, resolve resource conflicts, and monitor service levels and service improvements.	
7. 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.	
8. Regularly verify the adequacy and effectiveness of the organizational structures.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO01.05 Establish roles and responsibilities. Define and communicate roles and responsibilities for enterprise I&T, including authority levels, responsibilities and accountability.	a. Number of I&T-related roles assigned to individuals b. Number of completed role descriptions

Activities	Capability Level
1. Establish, agree on and communicate I&T-related roles and responsibilities for all personnel in the enterprise, in alignment with business needs and objectives. Clearly delineate responsibilities and accountabilities, especially for decision making and approvals.	2
2. Consider requirements from enterprise and I&T service continuity when defining roles, including staff back-up and cross-training requirements.	
3. Provide input to the I&T service continuity process by maintaining up-to-date contact information and role descriptions in the enterprise.	
4. Include specific requirements in role and responsibility descriptions regarding adherence to management policies and procedures, the code of ethics, and professional practices.	
5. Ensure that accountability is defined through roles and responsibilities.	
6. Structure roles and responsibilities to reduce the possibility for a single role to compromise a critical process.	
7. Implement adequate supervisory practices to ensure that roles and responsibilities are properly exercised, to assess whether all personnel have sufficient authority and resources to execute their roles and responsibilities, and generally to review performance. The level of supervision should be aligned with the sensitivity of the position and extent of assigned responsibilities.	3

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
APO01.06 Optimize the placement of the IT function. Position the IT capabilities in the overall organizational structure to reflect the strategic importance and operational dependency of IT within the enterprise. The reporting line of the CIO and representation of IT within senior management should be commensurate with the importance of I&T within the enterprise.	a. Number of key stakeholders that have signed off on the placement of the IT function b. Percent of stakeholders with a favorable opinion of the placement of the IT function

Activities	Capability Level
1. Understand context for the placement of the IT function, including assessment of enterprise strategy and operating model (centralized, federated, decentralized, hybrid), importance of I&T, and sourcing situation and options.	3
2. Identify, evaluate and prioritize options for organizational placement, sourcing and operating models.	
3. Define placement of the IT function and obtain agreement.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISO/IEC 27002:2013/Cor.2:2015(E)	8.2 Information classification

Management Practice	Example Metrics
APO01.07 Define information (data) and system ownership. Define and maintain responsibilities for ownership of information (data) and information systems. Ensure that owners classify information and systems and protect them in line with their classification.	a. Percent of data assets with clearly defined owners b. Percent of information systems with clearly defined owners c. Percent of information items classified according to the agreed classification levels

Activities	Capability Level
1. Provide guidelines to ensure appropriate and consistent enterprisewide classification of information items.	3
2. Create and maintain an inventory of information (systems and data) that includes a listing of owners, custodians and classifications. Include systems that are outsourced and those for which ownership should stay within the enterprise.	
3. Assess and distinguish between critical (high value) and noncritical data, information and systems. Ensure appropriate protection for each category.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO01.08 Define target skills and competencies. Define the required skills and competencies to achieve relevant management objectives.	a. Number of staff who have attended training or awareness sessions for selected skills, competencies, desired behaviors b. Percent of staff with required skills and competencies aligned to selected management objectives

Activities	Capability Level
1. Identify the required skills and competencies to achieve selected management objectives.	2
2. Analyze the gap between target skills and capabilities for the enterprise and current skills of the workforce. Refer to APO07—Managed Human Resources for skills development and management practices.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
APO01.09 Define and communicate policies and procedures. Put in place procedures to maintain compliance with and performance measurement of policies and other components of the control framework. Enforce the consequences of noncompliance or inadequate performance. Track trends and performance and consider these in the future design and improvement of the control framework.	a. Percent of active policies and procedures that are documented and up to date b. Number of staff aware and able to demonstrate competency with respect to policies and procedures

Activities	Capability Level
1. Create a set of policies to drive IT control expectations on relevant key topics such as quality, security, privacy, internal controls, usage of I&T assets, ethics and intellectual property (IP) rights.	3
2. Roll out and enforce I&T policies uniformly for all relevant staff so they are built into, and become integral parts of, enterprise operations.	
3. Evaluate and update the policies at least yearly to accommodate changing operating or business environments.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
APO01.10 Define and implement infrastructure, services and applications to support the governance and management system. Define and implement infrastructure, services and applications to support the governance and management system (e.g., architecture repositories, risk management system, project management tools, cost-tracking tools and incident monitoring tools).	a. Number of tools selected to support priority processes b. Adequacy/coverage by the tools of key I&T processes c. Satisfaction of recipients with the accuracy, completeness and timeliness of information d. Percent of stakeholder satisfaction with tools selected to support their needs

Activities	Capability Level
1. Identify priority management objectives that may be achieved by automating services, applications or infrastructure.	2
2. Select and implement the most appropriate tools and communicate to stakeholders.	
3. Provide training on selected tools, as required.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO01.11 Manage continual improvement of the I&T management system. Continually improve processes and other management system components to ensure that they can deliver against governance and management objectives. Consider COBIT implementation guidance, emerging standards, compliance requirements, automation opportunities and the feedback of stakeholders.	a. Date of last updates to the framework and components b. Number of I&T-related loss exposures due to inadequacies in the design of the control environment

Activities	Capability Level
1. Regularly assess performance of framework components and take appropriate action.	4
2. Identify business-critical processes based on performance and conformance drivers and related risk. Assess capability and identify improvement targets. Analyze gaps in capability and control. Identify options for improving or redesigning the process.	
3. Prioritize initiatives for improvement based on potential benefits and costs. Implement agreed improvements, operate as normal business practice, and set performance goals and metrics to enable monitoring of improvements.	5
4. Consider ways to improve efficiency and effectiveness (e.g., through training, documentation, standardization and/or process automation).	
5. Apply quality management practices to update the process.	
6. Retire outdated governance components (processes, information items, policies, etc.).	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ITIL V3, 2011	Continual Service Improvement, 4.1 The 7-Step Improvement Process

B. Component: Organizational Structures

Key Management Practice	Executive Committee	Chief Risk Officer	Chief Information Officer	Chief Technology Officer	Chief Digital Officer	I&T Governance Board	Architecture Board	Enterprise Risk Committee	Chief Information Security Officer	Business Process Owners	Data Management Function	Head Human Resources	Relationship Manager	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO01.01 Design the management system for enterprise I&T.	A		R	R	R	R															
APO01.02 Communicate management objectives, direction and decisions made.	A	R	R	R	R	R			R				R								
APO01.03 Implement management processes (to support the achievement of governance and management objectives).	A	R	R	R	R	R			R												
APO01.04 Define and implement the organizational structures.	A		R	R	R	R						R									
APO01.05 Establish roles and responsibilities.	A		R	R	R	R															
APO01.06 Optimize the placement of the IT function.	A		R	R	R	R		R													
APO01.07 Define information (data) and system ownership.	A		R	R	R	R		R		R	R			R							
APO01.08 Define target skills and competencies.	A		R	R	R	R								R	R	R	R				
APO01.09 Define and communicate policies and procedures.	A		R	R	R	R	R	R		R	R	R		R	R	R	R	R	R	R	R
APO01.10 Define and implement infrastructure, services and applications to support the governance and management system.	A		R	R	R	R					R			R	R	R	R	R	R	R	R
APO01.11 Manage continual improvement of the I&T management system.	A		R	R	R	R				R	R			R	R	R	R	R	R	R	R

B. Component: Organizational Structures *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
COSO Enterprise Risk Management, June 2017	6. Governance and Culture—Principle 2
ISO/IEC 27001:2013/Cor.2:2015(E)	5.3 Organizational roles, responsibilities and authorities

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
APO01.01 Design the management system for enterprise I&T.	APO02.05	Strategic road map	Priority governance and management objectives	All APO; All BAI; All DSS; All MEA
	APO12.01	Emerging risk issues and factors	Management system design	All APO; All BAI; All DSS; All MEA
	APO12.02	Risk analysis results		
	EDM01.01	• Enterprise governance guiding principles • Decision-making model		
APO01.02 Communicate management objectives, direction and decisions made.	APO12.06	Risk impact communication	Communication ground rules	All APO; All BAI; All DSS; All MEA
	DSS04.01	Policy and objectives for business continuity	Communication on I&T objectives	All APO; All BAI; All DSS; All MEA
	DSS05.01	Malicious software prevention policy		
	DSS05.02	Connectivity security policy		
	DSS05.03	Security policies for endpoint devices		
	EDM01.02	Enterprise governance communication		
	EDM04.02	Principles for safeguarding resources		
APO01.03 Implement management processes (to support the achievement of governance and management objectives).	APO02.04	Gaps and changes required to realize target capability	Target model gap analysis	All APO; All BAI; All DSS; All MEA
	EDM01.01	Enterprise governance guiding principles	Process capability levels	APO01.11
APO01.04 Define and implement the organizational structures.	APO03.02	Process architecture model	Enterprise operational guidelines	APO03.02
	EDM01.01	Enterprise governance guiding principles	Definition of organizational structure and functions	APO03.02

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO01.05 Establish roles and responsibilities.	**From**	**Description**	**Description**	**To**
	APO07.03	• Skills and competencies matrix • Skill development plans	Definition of supervisory practices	APO07.01
	APO11.01	Quality management system (QMS) roles, responsibilities and decision rights	Definition of I&T-related roles and responsibilities	DSS05.04
	APO13.01	Information security management system (ISMS) scope statement		
	DSS06.03	• Allocated roles and responsibilities • Allocated levels of authority		
	EDM01.01	Authority levels		
	EDM04.02	Assigned responsibilities for resource management		
APO01.06 Optimize the placement of the IT function.	Outside COBIT	• Enterprise strategy • Enterprise operating model	Defined operational placement of IT function	APO03.02
			Evaluation of options for IT organization	APO03.02
APO01.07 Define information (data) and system ownership.			Data classification guidelines	APO03.02; APO14.01; BAI02.01; DSS05.02; DSS06.01
			Data security and control guidelines	APO14.04; APO14.10; BAI02.01
			Data integrity procedures	APO14.04; BAI02.01; DSS06.01
APO01.08 Define target skills and competencies.			Target skills and competencies matrix	APO07.03
APO01.09 Define and communicate policies and procedures.	DSS01.04	Environmental policies	Noncompliance remedial actions	MEA01.05
	MEA03.02	Updated policies, principles, procedures and standards		
APO01.10 Define and implement infrastructure, services and applications to support the governance and management system.	APO09.01	Identified gaps in I&T services to the business	Plan of right-size I&T landscape including missing I&T capabilities, services and applications	APO02.02; APO02.03
	Outside COBIT	I&T landscape assessment including services, applications and infrastructure		

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO01.11 Manage continual improvement of the I&T management system.	**From**	**Description**	**Description**	**To**
	APO01.03	Process capability levels	Process improvement opportunities	All APO; All BAI; All DSS; All MEA
	EDM01.03	Feedback on governance effectiveness and performance	Performance goals and metrics for process improvement tracking	MEA01.02
	MEA03.02	Updated policies, principles, procedures and standards	Process capability assessments	MEA01.03
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
No related guidance for this component				

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
IT governance	Skills Framework for the Information Age V6, 2015	GOVN
IT management	Skills Framework for the Information Age V6, 2015	ITMG

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
I&T management framework	Establishes management system for enterprise I&T based on enterprise goals and other design factors. Considers detailed policies and principles for I&T management across all components.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Set an internal culture of alignment between business and IT, establishing the necessary management objectives, structures, processes, and roles and responsibilities that enable decision making and value creation in the most effective and efficient manner.		

G. Component: Services, Infrastructure and Applications
• COBIT and related products/tools • Equivalent frameworks and standards

Page intentionally left blank

Domain: Align, Plan and Organize Management Objective: APO02 — Managed Strategy	Focus Area: COBIT Core Model

Description

Provide a holistic view of the current business and I&T environment, the future direction, and the initiatives required to migrate to the desired future environment. Ensure that the desired level of digitization is integral to the future direction and the I&T strategy. Assess the organization's current digital maturity and develop a road map to close the gaps. With the business, rethink internal operations as well as customer-facing activities. Ensure focus on the transformation journey across the organization. Leverage enterprise architecture building blocks, governance components and the organization's ecosystem, including externally provided services and related capabilities, to enable reliable but agile and efficient response to strategic objectives.

Purpose

Support the digital transformation strategy of the organization and deliver the desired value through a road map of incremental changes. Use a holistic I&T approach, ensuring that each initiative is clearly connected to an overarching strategy. Enable change in all different aspects of the organization, from channels and processes to data, culture, skills, operating model and incentives.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG05 Customer-oriented service culture • EG08 Optimization of internal business process functionality • EG12 Managed digital transformation programs	AG08 Enabling and supporting business processes by integrating applications and technology

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG01	a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG08	a. Time to execute business services or processes b. Number of I&T-enabled business programs delayed or incurring additional cost due to technology-integration issues c. Number of business process changes that need to be delayed or reworked because of technology-integration issues d. Number of applications or critical infrastructures operating in silos and not integrated
EG05	a. Number of customer service disruptions b. Percent of business stakeholders satisfied that customer service delivery meets agreed levels c. Number of customer complaints d. Trend of customer satisfaction survey results		
EG08	a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities		
EG12	a. Number of programs on time and within budget b. Percent of stakeholders satisfied with program delivery c. Percent of business transformation programs stopped d. Percent of business transformation programs with regular reported status updates		

A. Component: Process	
Management Practice	**Example Metrics**
APO02.01 Understand enterprise context and direction. Understand the enterprise context (industry drivers, relevant regulations, basis for competition), its current way of working and its ambition level in terms of digitization.	a. Level of understanding within I&T management of current enterprise organization and context b. Level of knowledge within I&T management of enterprise goals and direction c. Level of understanding of key stakeholders for I&T and their detailed requirements

Activities	Capability Level
1. Develop and maintain an understanding of the external environment of the enterprise.	2
2. Develop and maintain an understanding of the current way of working, including the operational environment, enterprise architecture (business, information, data, applications and technology domains), enterprise culture and current challenges.	
3. Develop and maintain an understanding of future enterprise direction, including enterprise strategy, goals and objectives. Understand the ambition level of the enterprise in terms of digitization, which may include a range of increasingly aspirational goals, from cutting costs, increasing customer centricity, or getting to market faster by digitizing internal operations, to creating entirely new revenue streams from new business models (e.g., platform business).	
4. Identify key stakeholders and obtain insight on their requirements.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
COSO Enterprise Risk Management, June 2017	7. Strategy and Objective-Setting—Principle 6

Management Practice	Example Metrics
APO02.02 Assess current capabilities, performance and digital maturity of the enterprise. Assess the performance of current I&T services and develop an understanding of current business and I&T capabilities (both internal and external). Assess current digital maturity of the enterprise and its appetite for change.	a. Percent of staff satisfied with current capabilities b. Percent of business owner satisfaction with investment in and utilization of the internal and external asset base to meet critical success factors

Activities	Capability Level
1. Develop a baseline of current business and I&T capabilities and services. Include assessment of externally provisioned services, governance of I&T, and enterprisewide I&T-related skills and competencies.	2
2. Assess digital maturity across different dimensions (e.g., ability of leadership to leverage technology, level of accepted technology risk, approach to innovation, culture and knowledge level of users). Assess appetite for change.	3

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
COSO Enterprise Risk Management, June 2017	7. Strategy and Objective-Setting—Principle 6; 9. Review and Revision—Principle 15

Management Practice	Example Metrics
APO02.03 Define target digital capabilities. Based on the understanding of enterprise context and direction, define the target I&T products and services and required capabilities. Consider reference standards, best practices and validated emerging technologies.	a. Percent of enterprise objectives addressed by the I&T goals/objectives b. Percent of I&T objectives that support the enterprise strategy

Activities	Capability Level
1. Summarize enterprise context and direction and identify specific I&T aspects of enterprise strategy (e.g., digitizing processes, implementing new technology, supporting legacy architecture, applying new digital business models, developing digital product portfolio, etc.).	2
2. Define high-level I&T objectives and goals and specify their contribution to enterprise objectives.	
3. Detail required I&T services and products to realize enterprise objectives. Consider validated emerging technology or innovation ideas, reference standards, competitor business and I&T capabilities, comparative benchmarks of good practice, and emerging I&T service provision.	3
4. Determine I&T capabilities, methodologies and organizational approaches required to realize the defined I&T product and service portfolio. Consider different development methodologies (Agile, scrum, waterfall, bimodal IT), depending on business requirements. Consider how each could help realize I&T objectives.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO02.04 Conduct a gap analysis. Identify gaps between current and target environments and describe the high-level changes in the enterprise architecture.	a. Number of high-impact changes required in the different enterprise architecture domains b. Number of significant gaps between current environment and good practices

Activities	Capability Level
1. Identify all gaps and changes required to realize the target environment.	3
2. Describe high-level changes in enterprise architecture (business, information, data, applications and technology domains).	
3. Consider the high-level implications of all gaps. Assess the impact of potential changes on business and I&T operating models, I&T research and development capabilities, and I&T investment programs.	
4. Consider the value of potential changes to business and IT capabilities, I&T services and enterprise architecture, and the implications if no changes are realized.	4
5. Refine the target environment definition and prepare a value statement outlining benefits of the target environment.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
APO02.05 Define the strategic plan and road map. Develop a holistic digital strategy, in cooperation with relevant stakeholders, and detail a road map that defines the incremental steps required to achieve the goals and objectives. Ensure focus on the transformation journey through the appointment of a person who helps spearhead the digital transformation and drives alignment between business and I&T.	a. Level of stakeholder support for the digital transformation plan b. Percent of initiatives in the I&T strategy that are self-funding (with financial benefits exceeding costs) c. Degree of correspondence between enterprise strategy and I&T strategy and objectives

Activities	Capability Level
1. Define initiatives required to close gaps between current and target environments. Integrate initiatives into a coherent I&T strategy that aligns I&T with all aspects of the business.	3
2. Detail a road map that defines the incremental steps required to achieve the goals and objectives of the I&T strategy. Ensure actions are included to train people with new skills, support adoption of new technology, sustain change throughout the organization, etc.	
3. Consider the external ecosystem (enterprise partners, suppliers, start-ups, etc.) to help support execution of the road map.	
4. Group actions into programs and/or projects with a clear goal or deliverable. For each project, identify high-level resource requirements, schedule, investment/operational budget, risk, change impact, etc.	
5. Determine dependencies, overlaps, synergies and impacts among projects, and prioritize.	
6. Finalize road map, indicating relative scheduling and interdependencies of projects.	
7. Ensure focus on the transformation journey. Appoint a champion of digital transformation and alignment between business and I&T (chief digital officer [CDO] or other traditional C-suite role).	
8. Obtain support and formal approval of plan from stakeholders.	
9. Translate objectives into measurable outcomes represented by metrics (what) and targets (how much). Ensure that outcomes and measures correlate to enterprise benefits.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISF, The Standard of Good Practice for Information Security 2016	SG2.1 Information Security Strategy
ITIL V3, 2011	Service Strategy, 4.1 Strategy management for IT services

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO02.06 Communicate the I&T strategy and direction. Create awareness and understanding of the business and I&T objectives and direction, as captured in the I&T strategy, through communication to appropriate stakeholders and users throughout the enterprise.	a. Frequency of updates to the I&T strategy communication plan b. Percent of stakeholders aware of I&T strategy and direction

Activities	Capability Level
1. Develop a communication plan covering the required messages, target audiences, communication mechanisms/channels and schedules.	3
2. Prepare a communication package that delivers the plan effectively, using available media and technologies.	
3. Develop and maintain a network for endorsing, supporting and driving the I&T strategy.	
4. Obtain feedback and update the communication plan and delivery as required.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

B. Component: Organizational Structures

Key Management Practice	Chief Executive Officer	Chief Information Officer	Chief Technology Officer	Chief Digital Officer	I&T Governance Board	Business Process Owners	Project Management Office	Data Management Function	Relationship Manager	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO02.01 Understand enterprise context and direction.		A	R	R				R	R	R	R	R	R	R	R	R	R
APO02.02 Assess current capabilities, performance and digital maturity of the enterprise.		A	R	R				R		R	R	R	R	R	R	R	R
APO02.03 Define target digital capabilities.		R	R	A		R		R	R	R	R	R	R	R	R	R	R
APO02.04 Conduct a gap analysis.		R	R	R	A	R		R		R	R	R	R	R	R	R	R
APO02.05 Define the strategic plan and road map.		R	R	R	A	R	R	R		R	R	R	R	R	R	R	R
APO02.06 Communicate the I&T strategy and direction.	R	R	R	R	A												

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISO/IEC 38502:2017(E)	5.4 Responsibilities of managers

C. Component: Information Flows and Items (see also Section 3.6)

Management Practice	Inputs		Outputs	
APO02.01 Understand enterprise context and direction.	**From**	**Description**	**Description**	**To**
	APO04.02	Innovation opportunities linked to business drivers	Sources and priorities for change	Internal
	EDM04.01	Guiding principles for allocating resources and capabilities		
	Outside COBIT	Enterprise strategy and strengths, weaknesses, opportunities, threats (SWOT) analysis		

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO02.02 Assess current capabilities, performance and digital maturity of the enterprise.	**From**	**Description**	**Description**	**To**
	APO06.05	Cost optimization opportunities	Gaps and risk related to current capabilities	APO12.01
	APO08.05	Definition of potential improvement projects	Capability SWOT analysis	Internal
	APO09.01	Identified gaps in IT services to the business	Baseline of current capabilities	Internal
	APO09.04	Improvement action plans and remediations		
	APO12.01	Emerging risk issues and factors		
	APO12.02	Risk analysis results		
	APO12.03	Aggregated risk profile, including status of risk management actions		
	APO12.05	Project proposals for reducing risk		
	BAI04.03	• Prioritized improvements • Performance and capacity plans		
	BAI04.05	Corrective actions		
	BAI09.01	Results of fit-for-purpose reviews		
	BAI09.04	• Results of cost optimization reviews • Opportunities to reduce asset costs or increase value		
	EDM04.03	Feedback on allocation and effectiveness of resources and capabilities		
APO02.03 Define target digital capabilities.	APO04.05	• Results and recommendations from proof-of-concept initiatives • Analysis of rejected initiatives	Proposed enterprise architecture changes	APO03.03
			Required business and IT capabilities	Internal
			High-level I&T-related goals	Internal
APO02.04 Conduct a gap analysis.	APO04.06	Assessments of using innovative approaches	Gaps and changes required to realize target capability	APO01.03; APO13.02; BAI03.11; EDM04.01
	APO05.01	Investment return expectations	Value benefit statement for target environment	BAI03.11
	BAI01.05	Results of program goal achievement monitoring		
	BAI01.06	Stage-gate review results		
	BAI11.09	Post-implementation review results		
	EDM02.02	Evaluation of strategic alignment		

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
APO02.05 Define the strategic plan and road map.	APO03.01	• Defined scope of architecture • Architecture concept business case and value proposition	I&T strategy and objectives	All APO; All BAI; All DSS; All MEA
	APO03.02	Information architecture model	Strategic road map	APO01.01; APO03.01; APO08.01; EDM02.01; EDM02.02
	APO03.03	Transition architectures	Definition of strategic initiatives	EDM02.01
	APO05.01	Funding options	Risk assessment initiatives	EDM02.01, APO12.01
	APO06.02	Budget allocations		
	APO06.03	I&T budget		
	BAI09.05	Action plan to adjust license numbers and allocations		
	DSS04.02	Approved strategic options		
	EDM02.01	Feedback on strategy and goals		
	EDM04.01	Approved resources plan		
	EDM04.03	Remedial actions to address resource management deviations		
APO02.06 Communicate the I&T strategy and direction.	EDM04.02	Communication of resourcing strategies	Communication package	All APO; All BAI; All DSS; All MEA
			Communication plan	Internal

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ITIL V3, 2011	Service strategy, 3.9 Service strategy inputs and outputs

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Business plan development	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.3. Business Plan Development
Emerging technology monitoring	Skills Framework for the Information Age V6, 2015	EMRG
I&T strategy and planning	Skills Framework for the Information Age V6, 2015	ITSP
Strategy alignment	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.1. IS and Business Strategy Alignment

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
I&T service strategy principles	For details, refer to related guidance.	ITIL V3, 2011	Service Strategy, 3. Service strategy principles
I&T strategy policy and principles	Provides holistic view of current business and I&T environment, strategic direction and initiatives required to transition to the desired future environment. Ensures that business and I&T strategy reflect target level of digitization.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Establish a culture and underlying values that fit the overall business strategy (i.e., customer oriented, innovation driven, product based). Find ways to inject speed into processes and introduce the supporting culture and behavior that allow moving at a faster pace. This could start with changing basic habits such as having more frequent strategy leadership meetings or automating certain activities. In the current context of digital business models, ecosystems and disruption, it is vital for many organizations to prioritize digital transformation in their strategy. Build a culture that challenges the status quo and explores new ways of working (e.g., invest in automation to respond rapidly to customers, develop sophisticated reporting and analytics to interpret customer needs, build innovative interfaces to gather customer data, create mechanisms to deliver content and offers across all relevant channels).	The Scaled Agile Framework for Lean Enterprises	Configurable framework that helps organizations deliver new products and solutions in the shortest sustainable lead time (all chapters)

G. Component: Services, Infrastructure and Applications
• Customer analytics • Industry benchmarks • Performance measurement system (e.g., balanced scorecard, skills management tools) • Technology watch services and tools

Page intentionally left blank

Domain: Align, Plan and Organize Management Objective: APO03 — Managed Enterprise Architecture	Focus Area: COBIT Core Model

Description

Establish a common architecture consisting of business process, information, data, application and technology architecture layers. Create key models and practices that describe the baseline and target architectures, in line with the enterprise and I&T strategy. Define requirements for taxonomy, standards, guidelines, procedures, templates and tools, and provide a linkage for these components. Improve alignment, increase agility, improve quality of information and generate potential cost savings through initiatives such as re-use of building block components.

Purpose

Represent the different building blocks that make up the enterprise and its interrelationships as well as the principles guiding their design and evolution over time, to enable a standard, responsive and efficient delivery of operational and strategic objectives.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG05 Customer-oriented service culture • EG08 Optimization of internal business process functionality • EG12 Managed digital transformation programs	• AG06 Agility to turn business requirements into operational solutions • AG08 Enabling and supporting business processes by integrating applications and technology

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG01	a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG06	a. Level of satisfaction of business executives with I&T responsiveness to new requirements b. Average time to market for new I&T-related services and applications c. Average time to turn strategic I&T objectives into agreed and approved initiatives d. Number of critical business processes supported by up-to-date infrastructure and applications
EG05	a. Number of customer service disruptions b. Percent of business stakeholders satisfied that customer service delivery meets agreed levels c. Number of customer complaints d. Trend of customer satisfaction survey results	AG08	a. Time to execute business services or processes b. Number of I&T-enabled business programs delayed or incurring additional cost due to technology-integration issues c. Number of business process changes that need to be delayed or reworked because of technology-integration issues d. Number of applications or critical infrastructures operating in silos and not integrated
EG08	a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities		
EG12	a. Number of programs on time and within budget b. Percent of stakeholders satisfied with program delivery c. Percent of business transformation programs stopped d. Percent of business transformation programs with regular reported status updates		

A. Component: Process

Management Practice	Example Metrics
APO03.01 Develop the enterprise architecture vision. The architecture vision provides a first-cut, high-level description of the baseline and target architectures, covering the business, information, data, application and technology domains. The architecture vision provides the sponsor with a key tool to sell the benefits of the proposed capabilities to stakeholders within the enterprise. The architecture vision describes how the new capabilities (in line with I&T strategy and objectives) will meet enterprise goals and strategic objectives and address stakeholder concerns when implemented.	a. Level of architecture customer feedback b. Degree to which the baseline and target architectures cover the business, information, data, application and technology domains and frequency of updates

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Identify key stakeholders and their concerns/objectives. Define key enterprise requirements to be addressed as well as architecture views to be developed to satisfy stakeholder requirements.	2
2. Identify enterprise goals and strategic drivers. Define constraints that must addressed, including both enterprisewide and project-specific constraints (e.g., time, schedule, resources, etc.).	
3. Align architecture objectives with strategic program priorities.	
4. Understand enterprise capabilities and goals, then identify options to realize those goals.	
5. Assess the enterprise's readiness for change.	
6. Define scope of baseline architecture and target architecture. Enumerate items that are in scope as well as those out of scope. (Baseline and target architecture need not be described at the same level of detail.)	
7. Understand current enterprise strategic goals and objectives. Work within the strategic planning process to ensure that I&T-related enterprise architecture opportunities are leveraged in the development of the strategic plan.	
8. Based on stakeholder concerns, business capability requirements, scope, constraints and principles, create the architecture vision (i.e., the high-level view of baseline and target architectures).	
9. Confirm and elaborate architecture principles, including enterprise principles. Ensure that any existing definitions are current. Clarify any areas of ambiguity.	3
10. Identify enterprise change risk associated with the architecture vision. Assess the initial level of risk (e.g., critical, marginal or negligible). Develop a mitigation strategy for each significant risk.	
11. Develop an enterprise architecture concept business case and outline plans and statement of architecture work. Secure approval to initiate a project aligned and integrated with the enterprise strategy.	
12. Define the target architecture value propositions, goals and metrics.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.15 Program management (PM-7)
The Open Group Standard TOGAF version 9.2, 2018	6. Phase A: Architecture Vision

Management Practice	Example Metrics
APO03.02 Define reference architecture. The reference architecture describes the current and target architectures for the business, information, data, application and technology domains.	a. Date of last update to domain and/or federated architectures b. Number of exceptions to architecture standards and baselines applied for and granted

Activities	Capability Level
1. Maintain an architecture repository containing standards, reusable components, modeling artifacts, relationships, dependencies and views, to enable uniformity of architectural organization and maintenance.	3
2. Select reference viewpoints from the architecture repository that enable the architect to demonstrate how stakeholder concerns are addressed in the architecture.	
3. For each viewpoint, select models needed to support the specific view required. Use selected tools or methods and the appropriate level of decomposition.	
4. Develop baseline architectural domain descriptions, using the scope and level of detail necessary to support the target architecture and, to the extent possible, identifying relevant architecture building blocks from the architecture repository.	
5. Maintain a process architecture model as part of the baseline and target domain descriptions. Standardize the descriptions and documentation of processes. Define the roles and responsibilities of the process decision makers, process owner, process users, process team and any other process stakeholders who should be involved.	
6. Maintain an information architecture model as part of baseline and target domain descriptions, consistent with enterprise strategy to acquire, store and use data optimally in support of decision making.	
7. Verify architecture models for internal consistency and accuracy. Perform a gap analysis between baseline and target. Prioritize gaps and define new or modified components that must be developed for the target architecture. Resolve incompatibilities, inconsistencies or conflicts within the target architecture.	
8. Conduct a formal stakeholder review by vetting proposed architecture against the original intent of the architecture project and the statement of architecture work.	
9. Finalize business, information, data, applications and technology domain architectures. Create an architecture definition document.	

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Platform and Architecture—Architectural Approach; Platform and Architecture—Data Integration
ITIL V3, 2011	Service Strategy, 5.4 IT service strategy and enterprise architecture
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.1 Preparation (Task 9)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.5 Configuration management (CM-8)
The Open Group Standard TOGAF version 9.2, 2018	7. Phase B: Business Architecture; 8. Phase C: Information Systems Architectures; 9. Phase C: Information Systems Architectures Data Architecture; 10. Phase C: Information Systems Architectures Application Architecture; 11. Phase D: Technology Architecture
Management Practice	**Example Metrics**
APO03.03 Select opportunities and solutions. Rationalize the gaps between baseline and target architectures, accounting for both business and technical perspectives, and logically group them into project work packages. Integrate the project with any related I&T-enabled investment programs to ensure that the architectural initiatives are aligned with and enable these initiatives as part of overall enterprise change. Make this a collaborative effort with key enterprise stakeholders from business and IT to assess the enterprise's transformation readiness, and identify opportunities, solutions and all implementation constraints.	a. Number of identified gaps in models across enterprise, information, data, application and technology architecture domains b. Percent of key enterprise stakeholders from business and IT to assess the enterprise's transformation readiness, and identify opportunities, solutions and all implementation constraints
Activities	**Capability Level**
1. Determine and confirm key enterprise change attributes. Consider enterprise culture, the potential impact of culture on implementation of architecture and the enterprise's capabilities for transition.	3
2. Identify any enterprise drivers that would constrain the sequence of implementation. Include a review of enterprise and line-of-business strategic and business plans. Consider current enterprise architecture maturity.	
3. Review and consolidate results of the gap analysis between baseline and target architectures. Assess implications with respect to potential solutions, opportunities, interdependencies and alignment with current I&T-enabled programs.	
4. Assess requirements, gaps, solutions and other factors to identify a minimal set of functional requirements whose integration into work packages would lead to a more efficient and effective implementation of target architecture.	
5. Reconcile the consolidated requirements with potential solutions.	
6. Refine initial dependencies and identify constraints on implementation and migration plans. Compile a dependency analysis report.	
7. Confirm the enterprise's readiness for, and the risk associated with, enterprise transformation.	
8. Formulate high-level strategy for implementation and migration. Implement target architecture (and arrange any transition architecture) according to overall enterprise strategy, objectives and timelines.	
9. Identify and group major work packages into a coherent set of programs and projects, respecting the direction and approach to enterprise strategic implementation.	
10. Develop transition architectures where the scope of change required by the target architecture necessitates an incremental approach.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Platform and Architecture—Architectural Approach; Platform and Architecture—Data Integration
The Open Group Standard TOGAF version 9.2, 2018	12. Phase E: Opportunities and Solutions

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO03.04 Define architecture implementation. Create a viable implementation and migration plan in alignment with the program and project portfolios. Ensure the plan is closely coordinated to deliver value and that the required resources are available to complete the necessary work.	a. Clear definition of architecture implementation governance requirements b. Percent of stakeholders aware of architecture implementation and migration
Activities	**Capability Level**
1. Establish items required in the implementation and migration plan as part of program and project planning. Ensure that the plan aligns with requirements of relevant decision makers.	3
2. Confirm increments and phases of the transition architecture. Update the architecture definition document.	
3. Define and complete the architecture implementation and migration plan, including relevant governance requirements. Integrate the plan, activities and dependencies into program and project planning.	
4. Communicate the defined architectural road map to relevant stakeholders. Inform stakeholders about the target architecture definition, architecture guidelines and principles, service portfolio, etc.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Platform and Architecture—Architectural Approach; Platform and Architecture—Data Integration
The Open Group Standard TOGAF version 9.2, 2018	13. Phase F: Migration Planning
Management Practice	**Example Metrics**
APO03.05 Provide enterprise architecture services. Provide enterprise architecture services within the enterprise that include guidance to and monitoring of implementation projects, formalizing ways of working through architecture contracts, and measuring and communicating architecture's value and compliance monitoring.	a. Level of customer feedback for architecture services b. Percent of projects that utilize the framework and methodology to reuse defined components c. Percent of projects using enterprise architecture services d. Project benefits realized that can be traced back to architecture involvement (e.g., cost reduction through reuse)
Activities	**Capability Level**
1. Confirm scope and priorities and provide guidance for solution development and deployment (e.g., by using service-oriented architecture).	3
2. Manage enterprise architecture requirements and support business and IT with advice and expertise on architectural principles, models and building blocks. Guarantee that new implementations (as well as changes to current architecture) align with enterprise architecture principles and requirements.	
3. Manage portfolio of enterprise architecture services and ensure alignment with strategic objectives and solution development.	
4. Identify enterprise architecture priorities. Align priorities to value drivers. Define and collect value metrics and measure and communicate the value of enterprise architecture.	4
5. Establish a technology forum to provide architectural guidelines, advise projects and guide selection of technology. Measure compliance with standards and guidelines, including compliance with external requirements and internal business relevance.	5
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Platform and Architecture—Architectural Standards
ITIL V3, 2011	Service Design, 3.9 Service Oriented Architecture
The Open Group Standard TOGAF version 9.2, 2018	14. Phase G: Implementation Governance; 15. Phase H: Architecture Change Management

B. Component: Organizational Structures

Key Management Practice	Chief Operating Officer	Chief Information Officer	Chief Technology Officer	Chief Digital Officer	I&T Governance Board	Architecture Board	Data Management Function	Head Architect
APO03.01 Develop the enterprise architecture vision.		R	R	R	R	A	R	R
APO03.02 Define reference architecture.		R	R	R	R	A	R	R
APO03.03 Select opportunities and solutions.		R	R	R	R	A	R	R
APO03.04 Define architecture implementation.	R	R	R	R	R	A	R	R
APO03.05 Provide enterprise architecture services.	R	R	R	R	R	A		R

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
The Open Group Standard TOGAF version 9.2, 2018	41. Architecture Board

C. Component: Information Flows and Items (see also Section 3.6)

Management Practice	Inputs		Outputs	
	From	Description	Description	To
APO03.01 Develop the enterprise APO03.01 architecture vision.	APO02.05	Strategic road map	Defined scope of architecture	APO02.05
	EDM04.01	Guiding principles for enterprise architecture	Architecture concept business case and value proposition	APO02.05; APO05.02
	Outside COBIT	Enterprise strategy	Architecture principles	BAI02.01; BAI03.01; BAI03.02
APO03.02 Define reference architecture.	APO01.04	• Definition of organizational structure and functions • Enterprise operational guidelines	Process architecture model	APO01.04
	APO01.06	• Evaluation of options for IT organization • Defined operational placement of IT function	Information architecture model	APO02.05; APO14.03; BAI02.01; BAI03.02; DSS05.03; DSS05.04; DSS05.06

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO03.02 Define reference architecture. *(cont.)*	**From**	**Description**	**Description**	**To**
	APO01.07	Data classification guidelines	Baseline domain descriptions and architecture definition	APO13.02; BAI02.01; BAI03.01; BAI03.02; BAI03.12
	APO14.01	Data management strategy		
	APO14.03	Metadata documentation		
	Outside COBIT	Enterprise strategy		
APO03.03 Select opportunities and solutions.	APO02.03	Proposed enterprise architecture changes	Transition architectures	APO02.05
	Outside COBIT	• Enterprise drivers • Enterprise strategies		
APO03.04 Define architecture implementation.			Implementation phase descriptions	BAI01.01; BAI01.02; BAI11.01
			Architecture governance requirements	BAI01.01; BAI11.01
			Resource requirements	BAI01.02
APO03.05 Provide enterprise architecture services.			Solution development guidance	BAI02.01; BAI02.02; BAI03.02; BAI03.12

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.1 Preparation (Task 9): Inputs and Outputs
The Open Group Standard TOGAF version 9.2, 2018	6. Phase A: Architecture Vision: Inputs and Outputs; 7. Phase B: Business Architecture: Inputs and Outputs; 9. Phase C: Information Systems Architectures Data Architecture: Inputs and Outputs; 10. Information Systems Architectures Application Architecture: Inputs and Outputs; 11. Phase D: Technology Architecture: Inputs and Outputs; 12. Phase E: Opportunities and Solutions: Inputs and Outputs; 13. Phase F: Migration Planning: Inputs and Outputs; 14. Phase G: Implementation Governance: Inputs and Outputs; 15. Phase H: Architecture Change Management: Inputs and Outputs

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Architecture design	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.5. Architecture Design
Data analysis	Skills Framework for the Information Age V6, 2015	DTAN
Enterprise and business architecture	Skills Framework for the Information Age V6, 2015	STPL
Product / service planning	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.4. Product/Service Planning
Solution architecture	Skills Framework for the Information Age V6, 2015	ARCH

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Architectural principles	Defines general principles to inform rules and 20. Architecture Principles guidelines for architecture processes, procedures, layers, and overall use and interconnection of I&T resources and assets. Outlines architectural principles to enhance decision making. Ensures alignment of current and target architecture with enterprise objectives and strategy.	The Open Group Standard TOGAF version 9.2, 2018	20. Architecture Principles

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Create an environment in which management understands architectural needs relative to business goals and objectives. Drive effective practice of enterprise architecture throughout the organization (not only by enterprise architects). Ensure a holistic approach that links components more seamlessly (e.g., by moving away from dedicated teams of application specialists).		

G. Component: Services, Infrastructure and Applications
Architecture repository

Page intentionally left blank

Domain: Align, Plan and Organize Management Objective: APO04 — Managed Innovation	Focus Area: COBIT Core Model

Description

Maintain an awareness of I&T and related service trends and monitor emerging technology trends. Proactively identify innovation opportunities and plan how to benefit from innovation in relation to business needs and the defined I&T strategy. Analyze what opportunities for business innovation or improvement can be created by emerging technologies, services or I&T-enabled business innovation; through existing established technologies; and by business and IT process innovation. Influence strategic planning and enterprise architecture decisions.

Purpose

Achieve competitive advantage, business innovation, improved customer experience, and improved operational effectiveness and efficiency by exploiting I&T developments and emerging technologies.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG13 Product and business innovation	• AG06 Agility to turn business requirements into operational solutions • AG13 Knowledge, expertise and initiatives for business innovation
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG01 a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG06 a. Level of satisfaction of business executives with I&T responsiveness to new requirements b. Average time to market for new I&T-related services and applications c. Average time to turn strategic I&T objectives into agreed and approved initiatives d. Number of critical business processes supported by up-to-date infrastructure and applications
EG13 a. Level of awareness and understanding of business innovation opportunities b. Stakeholder satisfaction with levels of product and innovation expertise and ideas c. Number of approved product and service initiatives resulting from innovative ideas	AG13 a. Level of business executive awareness and understanding of I&T innovation possibilities b. Number of approved initiatives resulting from innovative I&T ideas c. Number of innovation champions recognized/awarded

A. Component: Process

Management Practice	Example Metrics
APO04.01 Create an environment conducive to innovation. Create an environment that is conducive to innovation, considering methods such as culture, reward, collaboration, technology forums, and mechanisms to promote and capture employee ideas.	a. Enterprise stakeholder perception and feedback on I&T innovation b. Inclusion of innovation or emerging technology-related objectives in performance goals for relevant staff

Activities	Capability Level
1. Create an innovation plan that includes risk appetite, a proposed budget for innovation initiatives and innovation objectives.	2
2. Provide infrastructure that can be a governance component for innovation (e.g., collaboration tools for enhancing work between geographic locations and/or divisions).	
3. Maintain a program-enabling staff to submit innovation ideas and create an appropriate decision-making structure to assess and move ideas forward.	3
4. Encourage innovation ideas from customers, suppliers and business partners.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO04.02 Maintain an understanding of the enterprise environment. Work with relevant stakeholders to understand their challenges. Maintain an adequate understanding of enterprise strategy, competitive environment and other constraints, so that opportunities enabled by new technologies can be identified.	a. Percent of implemented initiatives with a clear linkage to an enterprise objective b. Percent of opportunities enabled by new technologies identified

Activities	Capability Level
1. Maintain an understanding of industry and business drivers, enterprise and I&T strategy, and enterprise operations and current challenges. Apply the understanding to identify potential value-add technology and innovate I&T.	2
2. Conduct regular meetings with business units, divisions and/or other stakeholder entities to understand current business problems, process bottlenecks or other constraints where emerging technologies or I&T innovation can create opportunities.	3
3. Understand enterprise investment parameters for innovation and new technology so appropriate strategies are developed.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
APO04.03 Monitor and scan the technology environment. Set up a technology watch process to perform systematic monitoring and scanning of the enterprise's external environment to identify emerging technologies that have the potential to create value (e.g., by realizing the enterprise strategy, optimizing costs, avoiding obsolescence, and better enabling enterprise and I&T processes). Monitor the marketplace, competitive landscape, industry sectors, and legal and regulatory trends to be able to analyze emerging technologies or innovation ideas in the enterprise context.	a. Frequency of environment research and scans performed for identifying innovative ideas and trends b. Percent of stakeholders satisfied with efforts to monitor marketplace, competitive landscape, industry sectors, and legal and regulatory trends to analyze emerging technologies or innovation ideas in the enterprise context

Activities	Capability Level
1. Understand enterprise appetite and potential for technology innovation. Focus awareness efforts on the most opportune technology innovations.	2
2. Set up a technology watch process and perform research and scanning of the external environment, including appropriate websites, journals and conferences, to identify emerging technologies and their potential value to the enterprise.	
3. Consult third-party experts as necessary to confirm research or supply information on emerging technologies.	
4. Capture I&T-innovation ideas from staff and review for potential implementation.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
APO04.04 Assess the potential of emerging technologies and innovative ideas. Analyze identified emerging technologies and/or other I&T innovative suggestions to understand their business potential. Work with stakeholders to validate assumptions on the potential of new technologies and innovation.	a. Percent of implemented initiatives that realize the envisioned benefits b. Percent of successful proof-of-concept initiatives to test emerging technologies or other innovation ideas

Activities	Capability Level
1. Evaluate identified technologies, considering aspects such as time to reach maturity, inherent risk (including potential legal implications), fit with enterprise architecture and value potential, in line with enterprise and I&T strategy.	2
2. Identify issues that may need to be resolved or validated through a proof-of-concept initiative.	3
3. Scope the proof-of-concept initiative, including desired outcomes, required budget, time frames and responsibilities.	
4. Obtain approval for the proof-of-concept initiative.	
5. Conduct proof-of-concept initiatives to test emerging technologies or other innovation ideas. Identify issues and determine whether implementation or rollout should be considered based on feasibility and potential ROI.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO04.05 Recommend appropriate further initiatives. Evaluate and monitor the results of proof-of-concept initiatives and, if favorable, generate recommendations for further initiatives. Gain stakeholder support.	a. Number of proof-of-concept initiatives evaluated and approved for further rollout b. Number of proof-of-concept initiatives that have been leveraged in actual investment

Activities	Capability Level
1. Document proof-of-concept results, including guidance and recommendations for trends and innovation programs.	3
2. Communicate viable innovation opportunities into the I&T strategy and enterprise architecture processes.	
3. Analyze and communicate reasons for rejected proof-of-concept initiatives.	
4. Follow up on proof-of-concept initiatives to measure actual investment.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
APO04.06 Monitor the implementation and use of innovation. Monitor the implementation and use of emerging technologies and innovations during adoption, integration and for the full economic life cycle to ensure that the promised benefits are realized and to identify lessons learned.	a. Increase in market share or competitiveness due to innovations b. Number of lessons learned and opportunities for improvement captured for future use

Activities	Capability Level
1. Capture lessons learned and opportunities for improvement.	3
2. Ensure that innovation initiatives align with enterprise and I&T strategy. Monitor alignment continuously. Adjust innovation plan, if required.	
3. Assess new technology or I&T innovations implemented as part of I&T strategy and enterprise architecture development. Evaluate level of adoption during program management of initiatives.	4
4. Identify and assess potential value of innovation.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

B. Component: Organizational Structures													
Key Management Practice	**Executive Committee**	**Chief Information Officer**	**Chief Technology Officer**	**Chief Digital Officer**	**Business Process Owners**	**Data Management Function**	**Head Human Resources**	**Relationship Manager**	**Head Architect**	**Head Development**	**Head IT Operations**	**Service Manager**	**Information Security Manager**
APO04.01 Create an environment conducive to innovation.	A	R	R	R	R	R	R		R	R	R	R	R
APO04.02 Maintain an understanding of the enterprise environment.	A	R	R	R	R	R		R	R	R	R	R	R
APO04.03 Monitor and scan the technology environment.	A	R	R	R	R	R			R	R	R	R	R
APO04.04 Assess the potential of emerging technologies and innovative ideas.	A	R	R	R	R	R			R	R	R	R	R
APO04.05 Recommend appropriate further initiatives.	A	R	R	R	R	R			R	R	R	R	R
APO04.06 Monitor the implementation and use of innovation.	A	R	R	R	R	R			R	R	R	R	R

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
APO04.01 Create an environment conducive to innovation.	**From**	**Description**	**Description**	**To**
	EDM03.01	Risk appetite guidance	Recognition and reward program	APO07.04
			Innovation plan	Internal
APO04.02 Maintain an understanding of the enterprise environment.	Outside COBIT	Enterprise strategy and strengths, weaknesses, opportunities, threats (SWOT) analysis	Innovation opportunities linked to business drivers	APO02.01
APO04.03 Monitor and scan the technology environment.	Outside COBIT	Emerging technologies	Research analyses of innovation possibilities	BAI03.01
APO04.04 Assess the potential of emerging technologies and innovative ideas.			Proof-of-concept scope and outline business case	APO05.02; APO06.02
			Evaluations of innovation ideas	BAI03.01
			Test results from proof-of-concept initiatives	Internal
APO04.05 Recommend appropriate further initiatives.			Analysis of rejected initiatives	APO02.03; BAI03.08
			Results and recommendations from proof-of-concept initiatives	APO02.03; BAI03.09
APO04.06 Monitor the implementation and use of innovation.			Assessments of using innovative approaches	APO02.04; BAI03.02
			Evaluation of innovation benefits	APO05.03
			Adjusted innovation plans	Internal
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
No related guidance for this component				

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Business plan development	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.3. Business Plan Development
Emerging technology monitoring	Skills Framework for the Information Age V6, 2015	EMRG
Innovating	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.9. Innovating
Innovation	Skills Framework for the Information Age V6, 2015	INOV
Research	Skills Framework for the Information Age V6, 2015	RSCH
Technology trend monitoring	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.7. Technology Trend Monitoring

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Innovation principles	Defines general principles ensuring that new/innovative ideas are fully assessed when defining new strategic goals and decisions.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Create an environment that is conducive to innovation by maintaining relevant HR initiatives, such as innovation recognition and reward programs, appropriate job rotation, and discretionary time for experimentation. Ensure close collaboration and coordination of initiatives across the organization.		

G. Component: Services, Infrastructure and Applications
• Collaboration platforms • Industry benchmarks • Technology watch services and tools

Page intentionally left blank

Domain: Align, Plan and Organize Management Objective: APO05 — Managed Portfolio	Focus Area: COBIT Core Model

Description

Execute the strategic direction set for investments in line with the enterprise architecture vision and I&T road map. Consider the different categories of investments and the resources and funding constraints. Evaluate, prioritize and balance programs and services, managing demand within resource and funding constraints, based on their alignment with strategic objectives, enterprise worth and risk. Move selected programs into the active products or services portfolio for execution. Monitor the performance of the overall portfolio of products and services and programs, proposing adjustments as necessary in response to program, product or service performance or changing enterprise priorities.

Purpose

Optimize the performance of the overall portfolio of programs in response to individual program, product and service performance and changing enterprise priorities and demand.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG08 Optimization of internal business process functionality • EG12 Managed digital transformation programs	• AG03 Realized benefits from I&T-enabled investments and services portfolio • AG05 Delivery of I&T services in line with business requirements
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG01 a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG03 a. Percent of I&T-enabled investments for which claimed benefits in the business case are met or exceeded b. Percent of I&T services for which expected benefits (as stated in service level agreements) are realized
EG08 a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities	AG05 a. Percent of business stakeholders satisfied that I&T service delivery meets agreed service levels b. Number of business disruptions due to I&T service incidents c. Percent of users satisfied with the quality of I&T service delivery
EG12 a. Number of programs on time and within budget b. Percent of stakeholders satisfied with program delivery c. Percent of business transformation programs stopped d. Percent of business transformation programs with regular reported status updates	

A. Component: Process

Management Practice	Example Metrics
APO05.01 Determine the availability and sources of funds. Determine potential sources of funds, different funding options and the implications of the funding source on the investment return expectations.	a. Ratio between funds allocated and funds used b. Ratio between retained earnings and funds allocated

Activities	Capability Level
1. Understand current availability and commitment of funds, current approved spend and actual spend to date.	2
2. Identify options for additional funding of I&T-enabled investments, considering both internal and external sources.	
3. Determine the implications of the funding source on the investment return expectations.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO05.02 Evaluate and select programs to fund. Based on requirements for the overall investment portfolio mix and the I&T strategic plan and road map, evaluate and prioritize program business cases and decide on investment proposals. Allocate funds and initiate programs.	a. Percent of projects in the I&T project portfolio that can be directly traced back to the I&T strategy b. Percent of business units involved in the evaluation and prioritization process

Activities	Capability Level
1. Identify and classify investment opportunities in line with investment portfolio categories. Specify expected enterprise outcome(s), initiatives required to achieve expected outcome(s), high-level costs, dependencies and risk. Specify methodology for measuring outcomes, cost and risk.	2
2. Perform detailed assessment of all program business cases. Evaluate strategic alignment, enterprise benefit, risk and availability of resources.	3
3. Assess impact of adding potential programs on overall investment portfolio, including changes that might be required to other programs.	
4. Decide which candidate programs should be moved to the active investment portfolio. Decide whether rejected programs should be held for future consideration or provided with seed funding to determine if business case can be improved or discarded.	
5. Determine required milestones for each selected program's full economic life cycle. Allocate and reserve total program funding per milestone. Move the program into the active investment portfolio.	
6. Establish procedures to communicate the cost, benefit and risk-related aspects of portfolios for consideration in budget prioritization, cost management and benefit management processes.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PMBOK Guide Sixth Edition, 2017	Part 1: 1.2.3 Relationship of project, program, portfolio and operations management

Management Practice	Example Metrics
APO05.03 Monitor, optimize and report on investment portfolio performance. On a regular basis, monitor and optimize the performance of the investment portfolio and individual programs throughout the entire investment life cycle. Ensure continuous follow-up on the alignment of the portfolio with I&T strategy.	a. Trends in ROI of initiatives included in the I&T strategy b. Level of satisfaction with the portfolio monitoring reports c. Percent of programs aligned with enterprise business requirements

Activities	Capability Level
1. Review portfolio regularly to identify and exploit synergies, eliminate duplication among programs, and identify and mitigate risk.	3
2. When changes occur, reevaluate and reprioritize portfolio to ensure alignment with business and I&T strategy. Maintain target mix of investments so that the portfolio optimizes overall value. Programs may be changed, deferred or retired, and new programs may be initiated, to rebalance and optimize portfolio.	
3. Adjust enterprise targets, forecasts, budgets and, if required, degree of monitoring to reflect expenditures and enterprise benefits attributable to programs in the active investment portfolio. Charge back program expenditures. Establish flexible budgeting processes so that promising projects get resources to scale quickly.	
4. Develop metrics to measure I&T contribution to the enterprise. Establish appropriate performance targets reflecting required I&T and enterprise capability targets. Use guidance from external experts and benchmark data to develop metrics.	4
5. Provide an accurate view of the performance of the investment portfolio to all stakeholders.	
6. Provide reports for senior management's review of enterprise progress towards identified goals, stating what still needs to be spent and accomplished over given time frames.	
7. In regular performance monitoring, include information on the extent to which planned objectives have been achieved, risk mitigated, capabilities created, deliverables obtained and performance targets met.	
8. Identify deviations for budget vs. actual spend and expected ROI on investments.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO05.04 Maintain portfolios. Maintain portfolios of investment programs and projects, I&T products and services, and I&T assets.	a. Number of completed programs and projects b. Time since last update of services portfolio

Activities	Capability Level
1. Create and maintain portfolios of I&T-enabled investment programs, I&T services and I&T assets, which form the basis for the current I&T budget and support the I&T tactical and strategic plans.	3
2. Work with service delivery managers to maintain the service portfolios. Work with operations managers, product managers and architects to maintain the asset portfolios. Prioritize portfolios to support investment decisions.	
3. Remove a program from the active investment portfolio when the desired enterprise benefits have been achieved or when it is clear that benefits will not be achieved within the value criteria set for the program.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ITIL V3, 2011	Service Strategy, 4.2 Service portfolio management

Management Practice	Example Metrics
APO05.05 Manage benefits achievement. Monitor the benefits of providing and maintaining appropriate I&T products, services and capabilities, based on the agreed and current business case.	a. Percent of changes from the investment program reflected in the relevant I&T portfolios b. Percent of stakeholders satisfied with efforts to monitor the benefits of providing and maintaining appropriate I&T services and capabilities, based on the agreed and current business case

Activities	Capability Level
1. Use the agreed metrics and track how benefits are achieved, how they evolve throughout the life cycle of programs and projects, how they are being delivered from I&T products and services, and how they compare to internal and industry benchmarks. Communicate results to stakeholders.	4
2. Implement corrective action when achieved benefits significantly deviate from expected benefits. Update the business case for new initiatives and implement business process and service improvements as required.	5
3. Consider obtaining guidance from external experts, industry leaders and comparative benchmarking data to test and improve the metrics and targets.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

B. Component: Organizational Structures

Key Management Practice	Chief Financial Officer	Chief Information Officer	Chief Technology Officer	Chief Digital Officer	I&T Governance Board	Business Process Owners	Portfolio Manager	Program Manager	Project Management Office
APO05.01 Determine the availability and sources of funds.	R	R			A		R		
APO05.02 Evaluate and select programs to fund.	R	R	R	R	A		R	R	
APO05.03 Monitor, optimize and report on investment portfolio performance.		R	R	R	A		R	R	
APO05.04 Maintain portfolios.		R	R	R	A		R	R	R
APO05.05 Manage benefits achievement.	R	R	R	R	A	R	R	R	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)

Management Practice	Inputs		Outputs	
	From	Description	Description	To
APO05.01 Determine the availability and sources of funds.			Investment return expectations	APO02.04; APO06.02; BAI01.06; EDM02.02
			Funding options	APO02.05

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO05.02 Evaluate and select programs to fund.	**From**	**Description**	**Description**	**To**
	APO03.01	Architecture concept business case and value proposition	Program business case	APO06.02; BAI01.02
	APO04.04	Proof-of-concept scope and outline business case	Business case assessments	APO06.02; BAI01.06
	APO06.02	• Budget allocations • Prioritization and ranking of I&T initiatives	Selected programs with ROI milestones	BAI01.04; EDM02.02
	APO06.03	• IT budget • Budget communications		
	APO09.01	Identified gaps in IT services to the business		
	APO09.03	Service level agreements (SLAs)		
	APO13.02	Information security business cases		
	BAI01.02	• Program benefit realization plan • Program concept business case • Program mandate and brief		
	EDM02.02	• Evaluation of strategic alignment • Evaluation of investment and services portfolios		
	EDM02.03	Investment types and criteria		
APO05.03 Monitor, optimize and report on investment portfolio performance.	APO04.06	Evaluation of innovation benefits	Investment portfolio performance reports	APO09.04; BAI01.06; EDM02.03; EDM02.04; MEA01.03
	BAI01.06	Stage-gate review results		
	EDM02.02	Evaluation of investment and services portfolios		
	EDM02.04	• Feedback on portfolio and program performance • Actions to improve delivery of value		
APO05.04 Maintain portfolios.	BAI01.09	Communication of program retirement and ongoing accountabilities	Updated portfolios of programs, services and assets	APO09.02; BAI01.01
	BAI03.11	Updated service portfolio		
APO05.05 Manage benefits achievement.	BAI01.04	Program budget and benefits register	Corrective actions to improve benefit realization	APO09.04; BAI01.06
	BAI01.05	Results of benefit realization monitoring	Benefit results and related communications	APO09.04; BAI01.06; EDM02.02
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
No related guidance for this component				

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Benefits management	Skills Framework for the Information Age V6, 2015	BENM
Portfolio management	Skills Framework for the Information Age V6, 2015	POMG
Product / service planning	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.4. Product/Service Planning

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Portfolio principles	Defines general principles that ensure correct and diverse selection of programs and projects to achieve I&T strategy; considers alignment with business strategy, appropriate investment mix, etc.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Promote systematic management of I&T investments; measure and evaluate investment scenarios objectively.		
To support speed and agility, ensure that leaders evaluate the active investment portfolio decisively. If a prototype does not work, leadership must end the project decisively, incorporate lessons learned and move on. Quickly devote additional resources to successful projects in order to appropriately scale.		

G. Component: Services, Infrastructure and Applications
Portfolio/investment management tools

Domain: Align, Plan and Organize Management Objective: APO06 — Managed Budget and Costs	Focus Area: COBIT Core Model

Description

Manage the I&T-related financial activities in both the business and IT functions, covering budget, cost and benefit management and prioritization of spending through the use of formal budgeting practices and a fair and equitable system of allocating costs to the enterprise. Consult stakeholders to identify and control the total costs and benefits within the context of the I&T strategic and tactical plans. Initiate corrective action where needed.

Purpose

Foster a partnership between IT and enterprise stakeholders to enable the effective and efficient use of I&T-related resources and provide transparency and accountability of the cost and business value of solutions and services. Enable the enterprise to make informed decisions regarding the use of I&T solutions and services.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG04 Quality of financial information • EG07 Quality of management information • EG08 Optimization of internal business process functionality • EG09 Optimization of business process costs • EG12 Managed digital transformation programs	• AG04 Quality of technology-related financial information • AG09 Delivering programs on time, on budget and meeting requirements and quality standards

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG01	a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG04	a. Satisfaction of key stakeholders regarding the level of transparency, understanding and accuracy of I&T financial information b. Percent of I&T services with defined and approved operational costs and expected benefits
EG04	a. Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of enterprise financial information b. Cost of noncompliance with finance-related regulations	AG09	a. Number of programs/projects on time and within budget b. Number of programs needing significant rework due to quality defects c. Percent of stakeholders satisfied with program/project quality
EG07	a. Degree of board and executive management satisfaction with decision-making information b. Number of incidents caused by incorrect business decisions based on inaccurate information c. Time to provide information supporting effective business decisions d. Timeliness of management information		
EG08	a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities		
EG09	a. Ratio of cost vs. achieved service levels b. Satisfaction levels of board and executive management with business processing costs		
EG12	a. Number of programs on time and within budget b. Percent of stakeholders satisfied with program delivery c. Percent of business transformation programs stopped d. Percent of business transformation programs with regular reported status updates		

A. Component: Process	
Management Practice	**Example Metrics**
APO06.01 Manage finance and accounting. Establish and maintain a method to manage and account for all I&T-related costs, investments and depreciation as an integral part of enterprise financial systems and accounts. Report using the enterprise's financial measurement systems.	a. Numbers of deviations between expected and actual budget categories b. Usefulness of financial information as input to business cases for new investment in I&T assets and services

Activities	Capability Level
1. Define processes, inputs, outputs and responsibilities for the financial management and accounting of I&T in alignment with the enterprise budgeting and cost accounting policies and approach. Define how to analyze and report (to whom and how) on the I&T budget control process.	2
2. Define a classification scheme to identify all I&T-related cost elements (capital expenditures [capex] vs. operational expenses [opex], hardware, software, people, etc.). Identify how they are captured.	
3. Use financial information to provide input to business cases for new investments in I&T assets and services.	3
4. Ensure that costs are maintained in the I&T assets and services portfolios.	
5. Establish and maintain practices for financial planning and the optimization of recurring operational costs to deliver maximum value to the enterprise for the least expenditure.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ITIL V3, 2011	Service Strategy, 4.3 Financial management for IT services

Management Practice	Example Metrics
APO06.02 Prioritize resource allocation. Implement a decision-making process to prioritize the allocation of resources and establish rules for discretionary investments by individual business units. Include the potential use of external service providers and consider the buy, develop and rent options.	a. Number of resource-allocation issues escalated b. Percent of alignment of I&T resources with high-priority initiatives

Activities	Capability Level
1. Rank all I&T initiatives and budget requests based on business cases and strategic and tactical priorities. Establish procedures to determine budget allocations and cutoff.	2
2. Allocate business and IT resources (including external service providers) within the high-level budget allocations for I&T-enabled programs, services and assets. Consider the options for buying or developing capitalized assets and services vs. externally utilized assets and services on a pay-for-use basis.	
3. Establish a procedure to communicate budget decisions and review them with the business unit budget holders.	
4. Identify, communicate and resolve significant impacts of budget decisions on business cases, portfolios and strategy plans. For example, this may include when budgets require revision due to changing enterprise circumstances or when they are not sufficient to support strategic objectives or business case objectives).	
5. Obtain ratification from the executive committee for the I&T budget implications that negatively impact the entity's strategic or tactical plans. Suggest actions to resolve these impacts.	3

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
APO06.03 Create and maintain budgets. Prepare a budget reflecting investment priorities based on the portfolio of I&T-enabled programs and I&T services.	a. Number of budget changes due to omissions and errors b. Usefulness of I&T budget in identifying all expected I&T costs of I&T-enabled programs, services and assets

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Implement a formal I&T budget, including all expected I&T costs of I&T-enabled programs, services and assets.	2
2. When creating the budget, consider the following components: alignment with the business; alignment with the sourcing strategy; authorized sources of funding; internal resource costs, including personnel, information assets and accommodations; third-party costs, including outsourcing contracts, consultants and service providers; capital and operational expenses; and cost elements that depend on the workload.	
3. Document the rationale to justify contingencies and review them regularly.	
4. Instruct process, service and program owners, as well as project and asset managers, to plan budgets.	
5. Review the budget plans and make decisions about budget allocations. Compile and adjust the budget based on changing enterprise needs and financial considerations.	3
6. Record, maintain and communicate the current I&T budget, including committed expenditures and current expenditures, considering I&T projects recorded in the I&T-enabled investment portfolios and operation and maintenance of asset and service portfolios.	
7. Monitor the effectiveness of the different aspects of budgeting.	4
8. Use the monitoring results to implement improvements and ensure that future budgets are more accurate, reliable and cost-effective.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISO/IEC 20000-1:2011(E)	6.4 Budgeting and accounting for services
PMBOK Guide Sixth Edition, 2017	Part 1: 7. Project cost management

Management Practice	Example Metrics
APO06.04 Model and allocate costs. Establish and use an I&T costing model based, for example, on the service definition. This approach ensures that allocation of costs for services is identifiable, measurable and predictable, and encourages the responsible use of resources, including those provided by service providers. Regularly review and benchmark the cost/chargeback model to maintain its relevance and appropriateness for evolving business and IT activities.	a. Percent of overall I&T costs that are allocated according to the agreed cost models b. Number of reviews and benchmarks of the cost/chargeback model and its appropriateness to evolving business and I&T activities

Activities	Capability Level
1. Decide on a cost allocation model that enables fair, transparent, repeatable and comparable allocation of I&T-related costs to users. A basic allocation model example is the even spread of shared I&T-related costs. This is a very simple allocation model that is easy to apply; however, depending on the context of the enterprise, it is often viewed as unfair and it does not encourage responsible use of resources. An activity-based costing scheme, in which costs are allocated to IT services and charged to users of these services, enables a more transparent and comparable allocation of cost.	3
2. Inspect service definition catalogs to identify services subject to user chargeback and those that are shared services.	
3. Design the cost model to be transparent enough to allow users to identify their actual usage and charges by using categories and cost drivers that make sense for the user (e.g., cost per help desk call, cost per software license) and to better enable predictability of I&T costs and efficient and effective utilization of I&T resources. Analyze cost drivers (time spent per activity, expenses, portion of fixed vs. variable costs, etc.). Decide on appropriate differentiation (e.g., different categories of users with different weights) and use cost approximations or averages when actual costs are highly variable in nature.	
4. Explain the cost model principles and outcome to key stakeholders. Obtain their feedback for further fine-tuning toward a transparent and comprehensive model.	
5. Obtain approval of key stakeholders and communicate the I&T costing model to the management of user departments.	
6. Communicate important changes in the cost/chargeback model principles to key stakeholders and management of user departments.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO06.05 Manage costs. Implement a cost management process that compares actual costs against budget. Costs should be monitored and reported. Deviations from budget should be identified in a timely manner and their impact on enterprise processes and services assessed.	a. Percent of variance among budgets, forecasts and actual costs b. Timeliness of monitoring and reporting in the case of deviations and the impact of deviations on enterprise processes and services assessed

Activities	Capability Level
1. Obtain approval of key stakeholders and communicate the I&T costing model to the management of user departments.	2
2. Establish time scales for the operation of the cost management process in line with budgeting and accounting requirements and timeline.	
3. Define a method for the collection of relevant data to identify deviations in budget vs. actuals, investment ROI, service cost trends, etc.	
4. Define how costs are consolidated for the appropriate levels in the enterprise (central IT vs. IT budget within business departments) and how they will be presented to the stakeholders. The reports provide information on costs per cost category, budget vs. actuals status, top spending, etc., to enable the timely identification of required corrective actions.	3
5. Instruct those responsible for cost management to capture, collect and consolidate the data, and present and report the data to the appropriate budget owners. Budget analysts and owners jointly analyze deviations and compare performance to internal and industry benchmarks. They should establish and maintain the overheads allocation method. The result of the analysis provides an explanation of significant deviations and the suggested corrective actions.	
6. Ensure that the appropriate levels of management review the results of the analysis and approve suggested corrective actions.	
7. Ensure that changes in cost structures and enterprise needs are identified and budgets and forecasts are revised as required.	4
8. At regular intervals, and especially when budgets are cut due to financial constraints, identify ways to optimize costs and introduce efficiencies without jeopardizing services.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

B. Component: Organizational Structures							
Key Management Practice	**Chief Financial Officer**	**Chief Information Officer**	**Chief Technology Officer**	**Chief Digital Officer**	**Portfolio Manager**	**Head IT Administration**
APO06.01 Manage finance and accounting.	A				R	R
APO06.02 Prioritize resource allocation.	R	A	R	R	R	R
APO06.03 Create and maintain budgets.	R	A	R	R		R
APO06.04 Model and allocate costs.	R	A				R
APO06.05 Manage costs.	R	A	R	R		R

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Management Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
APO06.01 Manage finance and accounting.	**From**	**Description**	**Description**	**To**
	BAI09.01	Asset register	Financial planning practices	Internal
			I&T costs classification scheme	Internal
			Accounting processes	Internal
APO06.02 Prioritize resource allocation.	APO04.04	Proof-of-concept scope and outline business case	Budget allocations	APO02.05; APO05.02; APO07.05; BAI03.11
	APO05.01	Investment return expectations	Prioritization and ranking of I&T initiatives	APO05.02
	APO05.02	• Program business case • Business case assessments		
	EDM02.02	Evaluation of investment and services portfolios		
	EDM02.04	Actions to improve value delivery		
APO06.03 Create and maintain budgets.			I&T budget	APO02.05; APO05.02; APO07.01; BAI03.11
			Budget communications	APO05.02; APO07.01; BAI03.11
APO06.04 Model and allocate costs.			Operational procedures	Internal
			Cost allocation communications	Internal
			Cost allocation model	Internal
			Categorized I&T costs	Internal
APO06.05 Manage costs.	BAI01.02	Program benefit realization plan	Cost optimization opportunities	APO02.02
	BAI01.04	Program budget and benefits register	Cost consolidation method	Internal
	BAI01.05	Results of benefit realization monitoring	Cost data collection method	Internal
	EDM02.04	Feedback on portfolio and program performance		

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PMBOK Guide Sixth Edition, 2017	Part 1: 7. Project cost management: Inputs and Outputs

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Financial management	Skills Framework for the Information Age V6, 2015	FMIT

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Budgeting policy	Addresses preparation and timeline for the annual budget and forecasting of the annual financial position. Outlines required management reporting processes. Establishes accountability and responsibility for budget plan and other financial documents.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Effective and efficient management of I&T is supported by a culture of transparency on budget, costs and benefits throughout the organization. Management should enable a culture of fact-based decision-making through, for example, comparable estimations of business and IT costs and benefits for input to portfolio management, fair cost allocation of IT assets and resources, and repeatable budgeting of IT budgets.		

G. Component: Services, Infrastructure and Applications
Cost accounting system

Domain: Align, Plan and Organize Management Objective: APO07 — Managed Human Resources	Focus Area: COBIT Core Model

Description

Provide a structured approach to ensure optimal recruitment/acquisition, planning, evaluation and development of human resources (both internal and external).

Purpose

Optimize human resources capabilities to meet enterprise objectives.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG10 Staff skills, motivation and productivity • EG13 Product and business innovation	• AG12 Competent and motivated staff with mutual understanding of technology and business • AG13 Knowledge, expertise and initiatives for business innovation
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG01 a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG12 a. Percent of I&T-savvy business people (i.e., those having the required knowledge and understanding of I&T to guide, direct, innovate and see I&T opportunities in their domain of business expertise) b. Percent of business-savvy I&T people (i.e., those having the required knowledge and understanding of relevant business domains to guide, direct, innovate and see I&T opportunities for the business domain) c. Number or percentage of business people with technology management experience
EG10 a. Staff productivity compared to benchmarks b. Level of stakeholder satisfaction with staff expertise and skills c. Percent of staff whose skills are insufficient for competency in their role d. Percent of satisfied staff	AG13 a. Level of business executive awareness and understanding of I&T innovation possibilities b. Number of approved initiatives resulting from innovative I&T ideas c. Number of innovation champions recognized/awarded
EG13 a. Level of awareness and understanding of business innovation opportunities b. Stakeholder satisfaction with levels of product and innovation expertise and ideas c. Number of approved product and service initiatives resulting from innovative ideas	

A. Component: Process

Management Practice	Example Metrics
APO07.01 Acquire and maintain adequate and appropriate staffing. Establish and maintain a method to manage and account for all I&T-related costs, investments and depreciation as an integral part of the enterprise financial systems and accounts. Report using the enterprise's financial measurement systems.	a. Average duration of vacancies b. Percent of IT posts vacant c. Percent of staff turnover

Activities	Capability Level
1. Evaluate staffing requirements on a regular basis or upon major changes. Ensure that both the enterprise and the IT function have sufficient resources to support enterprise goals and objectives, business processes and controls, and I&T-enabled initiatives adequately and appropriately.	2
2. Maintain business and IT personnel recruitment and retention processes in line with the overall enterprise's personnel policies and procedures.	
3. Establish flexible resource arrangements, such as the use of transfers, external contractors and third-party service arrangements, to support changing business needs.	
4. Include background checks in the IT recruitment process for employees, contractors and vendors. The extent and frequency of these checks should depend on the sensitivity and/or criticality of the function.	3

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
COSO Enterprise Risk Management, June 2017	6. Governance and Culture—Principle 5
Skills Framework for the Information Age V6, 2015	SFIA and skills management—Acquire
Management Practice	**Example Metrics**
APO07.02 Identify key IT personnel. Identify key IT personnel. Use knowledge capture (documentation), knowledge sharing, succession planning and staff backup to minimize reliance on a single individual performing a critical job function.	a. Percent of critical jobs where the enterprise relies on a single individual b. Number of staff backup plans performed

Activities	Capability Level
1. As a security precaution, provide guidelines on a minimum time of annual vacation to be taken by key individuals.	2
2. Take appropriate actions regarding job changes, especially job terminations.	
3. Use knowledge capture (documentation), knowledge sharing, succession planning, staff backup, cross-training and job rotation initiatives to minimize reliance on a single individual performing a critical job function.	
4. Regularly test staff backup plans.	3

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	RI.RR Identification of Roles and Responsibilities
Skills Framework for the Information Age V6, 2015	SFIA and skills management—Acquire
Management Practice	**Example Metrics**
APO07.03 Maintain the skills and competencies of personnel. Define and manage the skills and competencies required of personnel. Regularly verify that personnel have the competencies to fulfill their roles on the basis of their education, training and/or experience. Verify that these competencies are being maintained, using qualification and certification programs where appropriate. Provide employees with ongoing learning and opportunities to maintain their knowledge, skills and competencies at a level required to achieve enterprise goals.	a. Identified key skills and competencies missing in the resource matrix b. Number of identified gaps between required and available skills c. Number of training programs provided

Activities	Capability Level
1. Identify currently available skills and competencies of internal and external resources.	2
2. Identify gaps between required and available skills. Develop action plans, such as training (technical and behavioral skills), recruitment, redeployment and changed sourcing strategies, to address the gaps on an individual and collective basis.	
3. Review training materials and programs on a regular basis. Ensure adequacy with respect to changing enterprise requirements and their impact on necessary knowledge, skills and abilities.	3
4. Provide access to knowledge repositories to support the development of skills and competencies.	
5. Develop and deliver training programs based on organizational and process requirements, including requirements for enterprise knowledge, internal control, ethical conduct, security and privacy.	
6. Conduct regular reviews to assess the evolution of the skills and competencies of the internal and external resources. Review succession planning.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISF, The Standard of Good Practice for Information Security 2016	PM2.3 Security Education/Training
ISO/IEC 27001:2013/Cor.2:2015(E)	7.2 Competence
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity V1.1, April 2018	PR.AT Awareness and Training
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.2 Awareness and training (AT-3, AT-4)
Skills Framework for the Information Age V6, 2015	SFIA and skills management—Deploy
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO07.04 Assess and recognize/reward employee job performance. Conduct timely, regular performance evaluations against individual objectives derived from enterprise goals, established standards, specific job responsibilities, and the skills and competency framework. Implement a remuneration/recognition process that rewards successful attainment of performance goals.	a. Number of official feedback moments and 360-degree evaluations performed b. Number and value of rewards given to staff

Activities	Capability Level
1. Consider functional/enterprise goals as the context for setting individual goals.	2
2. Set individual goals aligned with the relevant I&T and enterprise goals. Base goals on specific, measurable, achievable, relevant and time-bound (SMART) objectives that reflect core competencies, enterprise values and skills required for the role(s).	
3. Provide timely feedback regarding performance against the individual's goals.	
4. Provide specific instructions for the use and storage of personal information in the evaluation process, in compliance with applicable personal data and employment legislation.	
5. Compile 360-degree performance evaluation results.	3
6. Provide formal career planning and professional development plans based on the results of the evaluation process to encourage competency development and opportunities for personal advancement and to reduce dependence on key individuals. Provide employee coaching on performance and conduct whenever appropriate.	
7. Implement a remuneration/recognition process that rewards appropriate commitment, competency development and successful attainment of performance goals. Ensure that the process is applied consistently and in line with organizational policies.	
8. Implement and communicate a disciplinary process.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
Skills Framework for the Information Age V6, 2015	SFIA and skills management—Develop

Management Practice	Example Metrics
APO07.05 Plan and track the usage of IT and business human resources. Understand and track the current and future demand for business and IT human resources with responsibilities for enterprise I&T. Identify shortfalls and provide input into sourcing plans, enterprise and IT recruitment processes, and business and IT recruitment processes.	a. Number of identified shortfalls and missing skills in planning for staffing b. Time spent per full-time equivalent (FTE) on assignments and projects

Activities	Capability Level
1. Create and maintain an inventory of business and IT human resources.	2
2. Understand the current and future demand for human resources to support the achievement of I&T objectives and to deliver services and solutions based on the portfolio of current I&T-related initiatives, the future investment portfolio and day-to-day operational needs.	3
3. Identify shortfalls and provide input into sourcing plans as well as enterprise and IT recruitment processes. Create and review the staffing plan, keeping track of actual usage.	
4. Maintain adequate information on the time spent on different tasks, assignments, services or projects.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
Skills Framework for the Information Age V6, 2015	SFIA and skills management—Assess; Reward

Management Practice	Example Metrics
APO07.06 Manage contract staff. Ensure that consultants and contract personnel who support the enterprise with I&T skills know and comply with the organization's policies and meet agreed contractual requirements.	a. Percent of contractors signing off on the enterprise control framework b. Frequency of periodic reviews conducted to ensure correctness and compliance of contractor's staff

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Implement contract staff policies and procedures.	2
2. At the commencement of the contract, obtain formal agreement from contractors that they are required to comply with the enterprise's I&T control framework, such as policies for security clearance, physical and logical access control, use of facilities, information confidentiality requirements, and nondisclosure agreements.	
3. Advise contractors that management reserves the right to monitor and inspect all usage of IT resources, including email, voice communications, and all programs and data files.	
4. As part of their contracts, provide contractors with a clear definition of their roles and responsibilities, including explicit requirements to document their work to agreed standards and formats.	
5. Review contractors' work and base the approval of payments on the results.	
6. In formal and unambiguous contracts, define all work performed by external parties.	3
7. Conduct periodic reviews to ensure that contract staff have signed and agreed on all necessary agreements.	4
8. Conduct periodic reviews to ensure that contractors' roles and access rights are appropriate and in line with agreements.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
Skills Framework for the Information Age V6, 2015	SFIA and skills management—Deploy

B. Component: Organizational Structures																	
Key Management Practice	**Chief Financial Officer**	**Chief Operating Officer**	**Chief Information Officer**	**Chief Technology Officer**	**Chief Digital Officer**	**Project Management Office**	**Head Human Resources**	**Head Architect**	**Head Development**	**Head IT Operations**	**Head IT Administration**	**Service Manager**	**Information Security Manager**	**Business Continuity Manager**	**Privacy Officer**	**Legal Counsel**
APO07.01 Acquire and maintain adequate and appropriate staffing.			A	R	R	R	R	R	R	R	R	R	R	R		
APO07.02 Identify key IT personnel.			A	R	R	R	R	R	R	R	R	R	R	R	R	R
APO07.03 Maintain the skills and competencies of personnel.			A	R	R	R	R	R	R	R	R	R	R	R		
APO07.04 Assess and recognize/reward employee job performance.			A			R	R	R	R	R	R	R	R	R		
APO07.05 Plan and track the usage of IT and business human resources.	R	A	R	R	R	R	R	R	R	R	R	R	R	R		
APO07.06 Manage contract staff.			A	R	R	R	R	R	R	R	R	R	R	R		R
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**																
No related guidance for this component																	

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
APO07.01 Acquire and maintain adequate and appropriate staffing.	APO01.05	Definition of supervisory practices	Job descriptions and personnel sourcing plans	Internal
	APO06.03	• IT budget • Budget communications	Staffing requirement evaluations	Internal
	EDM04.01	• Guiding principles for allocating resources and capabilities • Approved resources plan	Competency and career development plans	Internal; APO07.02
	EDM04.03	Remedial actions to address resource management deviations		
	Outside COBIT	• Enterprise HR policies and procedures • Enterprise goals and objectives		
APO07.02 Identify key IT personnel.	APO07.01	Competency and career development plans	Job termination action plans	Internal
			Minimal amount of vacation guidance	Internal
APO07.03 Maintain the skills and competencies of personnel.	APO01.08	Target skills and competencies matrix	Skills and competencies matrix	APO01.05; APO14.01 BAI01.02; BAI01.04; BAI03.12
	BAI08.02	Published knowledge repositories	Skill development plans	APO01.05; EDM04.01
	BAI08.03	Knowledge awareness and training schemes	Review reports	Internal
	DSS04.06	• Training requirements • Monitoring results of skills and competencies		
	EDM01.02	Reward system approach		
	EDM04.03	Remedial actions to address resource management deviations		
	Outside COBIT	Enterprise goals and objectives		

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO07.04 Assess and recognize/reward employee job performance.	**From**	**Description**	**Description**	**To**
	APO04.01	Recognition and reward program	Improvement plans	Internal
	BAI05.04	Aligned HR performance objectives	Performance evaluations	Internal
	BAI05.06	HR performance review results	Personnel goals	Internal
	DSS06.03	Allocated access rights		
	EDM01.02	Reward system approach		
	Outside COBIT	Enterprise goals and objectives		
APO07.05 Plan and track the usage of IT and business human resources.	APO06.02	Budget allocations	Inventory of business and IT human resources	BAI01.04
	BAI01.04	Resource requirements and roles	Resource utilization records	BAI01.06
	BAI11.08	Project resource requirements	Resourcing shortfall analyses	BAI01.06
	EDM04.02	Communication of resourcing strategies		
	EDM04.03	Feedback on allocation and effectiveness of resources and capabilities		
	Enterprise organization	Current and future portfolios		
	Outside COBIT	Enterprise organization structure		
APO07.06 Manage contract staff.	BAI01.04	Resource requirements and roles	Contract agreement reviews	Internal
	BAI01.09	Communication of program retirement and ongoing accountabilities	Contract agreements	Internal
	BAI11.08	Project resource requirements	Contract staff policies	Internal
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
PMBOK Guide Sixth Edition, 2017		Part 1: 9. Project resource management: Inputs and Outputs		

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Education and training provision	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	D. Enable—D.3. Education and Training Provision
Learning and development management	Skills Framework for the Information Age V6, 2015	ETMG
Performance management	Skills Framework for the Information Age V6, 2015	PEMT
Personnel development	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework, 2016	D. Enable—D.9. Personnel Development
Professional development	Skills Framework for the Information Age V6, 2015	PDSV
Resourcing	Skills Framework for the Information Age V6, 2015	RESC

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Contract staff policy	Enumerates criteria for augmenting staff with third-party consultants and/or contractors in accordance with enterprise IT procurement policy and the I&T control framework. Specifies what type of work can be performed or augmented by third parties, under what conditions, and when.	National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.16 Personnel security (PS-1)
Human resources (HR) policies	Outlines mutual expectations of the enterprise and its employees. Enumerates acceptable and unacceptable employee behaviors in a code of conduct to help manage risk related to human behavior.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Describe the roles and responsibilities of users toward information, media and network usage, security, and privacy. Encourage and communicate a common culture that prescribes expected behaviors for all individuals in the enterprise and establishes zero tolerance for unethical behaviors.	National Institute of Standards and Technology Special Publication 800- 53, Revision 5, August 2017	3.14 Planning (PL-4)

G. Component: Services, Infrastructure and Applications
• HR management system • Performance measurement system (e.g., balanced scorecard, skills management tools) • Resource planning tools

Page intentionally left blank

Domain: Align, Plan and Organize Management Objective: APO08 — Managed Relationships	Focus Area: COBIT Core Model

Description

Manage relationships with business stakeholders in a formalized and transparent way that ensures mutual trust and a combined focus on achieving the strategic goals within the constraints of budgets and risk tolerance. Base relationships on open and transparent communication, a common language, and the willingness to take ownership and accountability for key decisions on both sides. Business and IT must work together to create successful enterprise outcomes in support of the enterprise objectives.

Purpose

Enable the right knowledge, skills and behaviors to create improved outcomes, increased confidence, mutual trust and effective use of resources that stimulate a productive relationship with business stakeholders.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG08 Optimization of internal business process functionality • EG10 Staff skills, motivation and productivity • EG13 Product and business innovation	• AG05 Delivery of I&T services in line with business requirements • AG06 Agility to turn business requirements into operational solutions • AG12 Competent and motivated staff with mutual understanding of technology and business • AG13 Knowledge, expertise and initiatives for business innovation

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG01	a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG05	a. Percent of business stakeholders satisfied that I&T service delivery meets agreed service levels b. Number of business disruptions due to I&T service incidents c. Percent of users satisfied with the quality of I&T service delivery
EG08	a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities	AG06	a. Level of satisfaction of business executives with I&T responsiveness to new requirements b. Average time to market for new I&T-related services and applications c. Average time to turn strategic I&T objectives into agreed and approved initiatives d. Number of critical business processes supported by up-to-date infrastructure and applications
EG10	a. Staff productivity compared to benchmarks b. Level of stakeholder satisfaction with staff expertise and skills c. Percent of staff whose skills are insufficient for competency in their role d. Percent of satisfied staff	AG12	a. Percent of I&T-savvy business people (i.e., those having the required knowledge and understanding of I&T to guide, direct, innovate and see I&T opportunities in their domain of business expertise) b. Percent of business-savvy I&T people (i.e., those having the required knowledge and understanding of relevant business domains to guide, direct, innovate and see I&T opportunities for the business domain) c. Number or percentage of business people with technology management experience
EG13	a. Level of awareness and understanding of business innovation opportunities b. Stakeholder satisfaction with levels of product and innovation expertise and ideas c. Number of approved product and service initiatives resulting from innovative ideas	AG13	a. Level of business executive awareness and understanding of I&T innovation possibilities b. Number of approved initiatives resulting from innovative I&T ideas c. Number of innovation champions recognized/awarded

A. Component: Process	
Management Practice	**Example Metrics**
APO08.01 Understand business expectations. Understand current business issues, objectives and expectations for I&T. Ensure that requirements are understood, managed and communicated, and their status agreed and approved.	a. Number of identified current business issues b. Number of defined business requirements for I&T-enabled services

Activities	Capability Level
1. Identify business stakeholders, their interests and their areas of responsibilities.	2
2. Review current enterprise direction, issues, strategic objectives, and alignment with enterprise architecture.	
3. Understand the current business environment, process constraints or issues, geographical expansion or contraction, and industry/regulatory drivers.	
4. Maintain an awareness of business processes and associated activities. Understand demand patterns that relate to service volumes and use.	
5. Manage expectations by ensuring that business units understand priorities, dependencies, financial constraints and the need to schedule requests.	3
6. Clarify business expectations for I&T-enabled services and solutions. Ensure that requirements are defined with associated business acceptance criteria and metrics.	4
7. Confirm that there is agreement between IT and all business departments on expectations and how they will be measured. Ensure that this agreement is confirmed by all stakeholders.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
APO08.02 Align I&T strategy with business expectations and identify opportunities for IT to enhance the business. Align I&T strategies with current business objectives and expectations to enable IT to be a value-add partner for the business and a governance component for enhanced enterprise performance.	a. Inclusion rate of technology opportunities in investment proposals b. Survey of business stakeholders regarding their level of technological awareness

Activities	Capability Level
1. Position IT as a partner to the business. Play a proactive role in identifying and communicating with key stakeholders on opportunities, risk and constraints. This includes current and emerging technologies, services and business process models.	3
2. Collaborate on major new initiatives with portfolio, program and project management. Ensure the involvement of the IT organization from the start of a new initiative by providing value-add advice and recommendations (e.g., for business case development, requirements definition, solution design) and by taking ownership for I&T work streams.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ITIL V3, 2011	Service Strategy, 4.4 Demand management

Management Practice	Example Metrics
APO08.03 Manage the business relationship. Manage the relationship between the IT service organization and its business partners. Ensure that relationship roles and responsibilities are defined and assigned, and communication is facilitated.	a. Ratings of user and IT personnel satisfaction surveys b. Percent of relationship roles and responsibilities defined, assigned, and communicated

Activities	Capability Level
1. Assign a relationship manager as a single point of contact for each significant business unit. Ensure that a single counterpart is identified in the business organization and the counterpart has business understanding, sufficient technology awareness and the appropriate level of authority.	3
2. Manage the relationship in a formalized and transparent way that ensures a focus on achieving a common and shared goal of successful enterprise outcomes in support of strategic goals and within the constraint of budgets and risk tolerance.	
3. Define and communicate a complaints and escalation procedure to resolve any relationship issues.	
4. Ensure that key decisions are agreed and approved by relevant accountable stakeholders.	
5. Plan specific interactions and schedules based on mutually agreed objectives and common language (service and performance review meetings, review of new strategies or plans, etc.).	4

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISO/IEC 20000-1:2011(E)	7.1 Business relationship management
ITIL V3, 2011	Service Strategy, 4.5 Business relationship management
Management Practice	**Example Metrics**
APO08.04 Coordinate and communicate. Work with all relevant stakeholders and coordinate the end-to-end delivery of I&T services and solutions provided to the business.	a. Time since last update of end-to-end communication plan to business b. Percent of business owner satisfaction with coordination of the end to end delivery of I&T services and solutions
Activities	**Capability Level**
1. Coordinate and communicate changes and transition activities such as project or change plans, schedules, release policies, release known errors, and training awareness.	2
2. Coordinate and communicate operational activities, roles and responsibilities, including the definition of request types, hierarchical escalation, major outages (planned and unplanned), and content and frequency of service reports.	
3. Take ownership of the response to the business for major events that may influence the relationship with the business. Provide direct support if required.	
4. Maintain an end-to-end communication plan that defines the content, frequency and recipients of service delivery information, including status of value delivered and any risk identified.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
APO08.05 Provide input to the continual improvement of services. Continually improve and evolve I&T-enabled services and service delivery to the enterprise to align with changing enterprise objectives and technology	a. Percent of alignment of I&T services with enterprise business requirements b. Percent of root causes identified and resolved for any issues
Activities	**Capability Level**
1. Perform customer and provider satisfaction analysis. Ensure that issues are addressed; report results and status.	4
2. Work together to identify, communicate and implement improvement initiatives.	5
3. Work with service management and process owners to ensure that I&T-enabled services and service management processes are continually improved and the root causes of any issues are identified and resolved.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

B. Component: Organizational Structures

Key Management Practice	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Chief Information Officer	Chief Technology Officer	Chief Digital Officer	I&T Governance Board	Business Process Owners	Relationship Manager	Head Architect	Head Development	Head IT Operations	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO08.01 Understand business expectations.				A	R	R		R	R		R	R	R	R	R	R
APO08.02 Align I&T strategy with business expectations and identify opportunities for IT to enhance the business.				A	R	R	R	R	R	R	R	R	R			
APO08.03 Manage the business relationship.	R	R	R	A	R	R		R	R		R	R	R			
APO08.04 Coordinate and communicate.	R	R	R	A	R	R		R	R		R	R	R			
APO08.05 Provide input to the continual improvement of services.				A	R	R		R	R		R	R	R			

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)

Management Practice	Inputs		Outputs	
	From	Description	Description	To
APO08.01 Understand business expectations.	APO02.05	Strategic road map	Clarified and agreed business expectations	Internal
APO08.02 Align I&T strategy with business expectations and identify opportunities for IT to enhance the business.	APO09.01	Identified gaps in IT services to the business	Agreed next steps and action plans	Internal
	APO09.04	• Service level performance reports • Improvement action plans and remediations		
	APO11.03	Root causes of failure to deliver quality		
APO08.03 Manage the business relationship.	DSS02.02	Classified and prioritized incidents and service requests	Complaint and escalation status	Internal
	DSS02.06	• Closed service requests and incidents • User confirmation of satisfactory fulfilment or resolution	Agreed key decisions	Internal
	DSS02.07	• Incident status and trends report • Request fulfilment status and trends report		

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO08.04 Coordinate and communicate.	**From**	**Description**	**Description**	**To**
	APO09.03	Service level agreements (SLAs)	Customer responses	Internal
	APO12.06	Risk impact communication	Communication packages	Internal
	BAI05.05	Operation and use plan	Communication plan	Internal
	BAI07.07	Supplemental support plan		
	BAI09.02	Communications of planned maintenance downtime		
	DSS03.04	Communication of knowledge learned		
APO08.05 Provide input to the continual improvement of services.	APO09.02	Service catalogs	Definition of potential improvement projects	APO02.02; BAI03.11
	APO11.02	• Customer requirements for quality management • Results of quality of service, including customer feedback	Satisfaction analyses	APO09.04
	APO11.03	Results of quality monitoring for solution and service delivery		
	APO11.04	Results of quality reviews and audits		
	BAI03.10	Maintenance plan		
	BAI05.05	Success measures and results		
	BAI07.07	Supplemental support plan		
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
No related guidance for this component				

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Relationship management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.4. Relationship Management
Relationship management	Skills Framework for the Information Age V6, 2015	RLMT

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Business—IT relationship management policy	Provides guidelines to establish and maintain relations between the business and IT. Fosters transparency, mutual trust and a common focus on achieving strategic goals within the context of budget and risk tolerance.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Establish a culture based on mutual trust, transparent communication, open and understandable terms, a common language, ownership, and accountability. Good relationships must exist between the business and IT within the enterprise to achieve a shared goal.		

G. Component: Services, Infrastructure and Applications
• Collaboration platforms • Internal training and awareness building services

Domain: Align, Plan and Organize Management Objective: APO09 — Managed Service Agreements	Focus Area: COBIT Core Model

Description

Align I&T-enabled products and services and service levels with enterprise needs and expectations, including identification, specification, design, publishing, agreement, and monitoring of I&T products and services, service levels and performance indicators.

Purpose

Ensure that I&T products, services and service levels meet current and future enterprise needs.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG08 Optimization of internal business process functionality	AG05 Delivery of I&T services in line with business requirements
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG01 a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG05 a. Percent of business stakeholders satisfied that I&T service delivery meets agreed service levels b. Number of business disruptions due to I&T service incidents c. Percent of users satisfied with the quality of I&T service delivery
EG08 a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities	

A. Component: Process

Management Practice	Example Metrics
APO09.01 Identify I&T services. Analyze business requirements and the degree to which I&T-enabled services and service levels support business processes. Discuss and agree with the business on potential services and service levels. Compare potential service levels against the current service portfolio; identify new or changed services or service level options.	a. Number of business activities that are not supported by any I&T service b. Number of obsolete services identified

Activities	Capability Level
1. Assess current I&T services and service levels to identify gaps between existing services and the business activities they support. Identify areas for improvement of existing services and service level options.	2
2. Analyze, study and estimate future demand and confirm capacity of existing I&T-enabled services.	
3. Analyze business process activities to identify the need for new or redesigned I&T services.	3
4. Compare identified requirements to existing service components in the portfolio. If possible, package existing service components (I&T services, service level options and service packages) into new service packages to meet identified business requirements.	
5. Regularly review the portfolio of I&T services with portfolio management and business relationship management to identify obsolete services. Agree on retirement and propose change.	
6. Where possible, match demands to service packages and create standardized services to obtain overall efficiencies.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ITIL V3, 2011	Service Strategy, 4.4 Demand management

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO09.02 Catalog I&T-enabled services. Define and maintain one or more service catalogues for relevant target groups. Publish and maintain live I&T-enabled services in the service catalogs.	a. Percent of live I&T-enabled services and service packages offered in comparison to the portfolio b. Time since last service portfolio update
Activities	**Capability Level**
1. Publish in catalogues relevant live I&T-enabled services, service packages and service level options from the portfolio.	2
2. Continually ensure that the service components in the portfolio and the related service catalogues are complete and up to date.	3
3. Inform business relationship management of any updates to the service catalogues.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ITIL V3, 2011	Service Design, 4.2 Service Catalogue Management
Management Practice	**Example Metrics**
APO09.03 Define and prepare service agreements. Define and prepare service agreements based on options in the service catalogues. Include internal operational agreements.	a. Number of business processes with undefined service agreements b. Percent of live IT services covered by service agreements
Activities	**Capability Level**
1. Analyze requirements for new or changed service agreements received from business relationship management to ensure that the requirements can be matched. Consider aspects such as service times, availability, performance, capacity, security, privacy, continuity, compliance and regulatory issues, usability, demand constraints, and data quality.	2
2. Draft customer service agreements based on the services, service packages and service level options in the relevant service catalogues.	
3. Finalize customer service agreements with business relationship management.	
4. Determine, agree on and document internal operational agreements to underpin the customer service agreements, if applicable.	3
5. Liaise with supplier management to ensure that appropriate commercial contracts with external service providers underpin the customer service agreements, if applicable.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	SY2.1 Service Level Agreements
ISO/IEC 20000-1:2011(E)	4.5 Establish and improve the SMS; 6.1 Service level management
ITIL V3, 2011	Service Design, 4.3 Service Level Management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.18 System and services acquisition (SA-9)
Management Practice	**Example Metrics**
APO09.04 Monitor and report service levels. Monitor service levels, report on achievements and identify trends. Provide the appropriate management information to aid performance management.	a. Number and severity of service breaches b. Percent of customers satisfied that service delivery meets agreed levels c. Percent of service targets being met d. Percent of services being monitored to service levels
Activities	**Capability Level**
1. Establish and maintain measures to monitor and collect service level data.	4
2. Evaluate performance and provide regular and formal reporting of service agreement performance, including deviations from the agreed values. Distribute this report to business relationship management.	
3. Perform regular reviews to forecast and identify trends in service level performance. Incorporate quality management practices in the service monitoring.	
4. Provide the appropriate management information to aid performance management.	
5. Agree on action plans and remediations for any performance issues or negative trends.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
HITRUST CSF version 9, September 2017	09.02 Control Third Party Service Delivery
ISO/IEC 20000-1:2011(E)	6.2 Service reporting

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO09.05 Review service agreements and contracts. Conduct periodic reviews of the service agreements and revise when needed.	a. Number of reviews of the service agreements performed b. Percent of service targets being met c. Percent of stakeholders satisfied with the quality of service agreements d. Number of service agreements revised, as needed

Activities	Capability Level
1. Regularly review service agreements according to the agreed terms to ensure that they are effective and up to date. When appropriate, take into account changes in requirements, I&T-enabled services, service packages or service level options.	3
2. When needed, revise the existing service agreement with the service provider. Agree on and update the internal operational agreements.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

B. Component: Organizational Structures												
Key Management Practice	**Chief Operating Officer**	**Chief Information Officer**	**Chief Technology Officer**	**Enterprise Risk Committee**	**Business Process Owners**	**Head IT Operations**	**Head IT Administration**	**Service Manager**	**Information Security Manager**	**Privacy Officer**	**Legal Counsel**
APO09.01 Identify I&T services.	R	R	A		R			R			
APO09.02 Catalog I&T-enabled services.		R	A	R				R			
APO09.03 Define and prepare service agreements.		R	A			R	R	R	R	R	R
APO09.04 Monitor and report service levels.		R	A		R			R			R
APO09.05 Review service agreements and contracts.	R	A	R			R	R	R			

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISO/IEC 20000-1:2011(E)	4.1.1 Management commitment

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
APO09.01 Identify I&T services.	**From**	**Description**	**Description**	**To**
			Identified gaps in I&T services to the business	APO01.10; APO02.02; APO05.02; APO08.02
			Definitions of standard services	EDM02.01
APO09.02 Catalog I&T-enabled services.	APO05.04	Updated portfolios of programs, services and assets	Service catalogs	APO08.05
	EDM04.01	Approved resources plan		
	EDM04.02	Communication of resourcing strategies		
APO09.03 Define and prepare service agreements.	APO11.02	Customer requirements for quality management	Service level agreements (SLAs)	APO05.02; APO08.04; DSS01.02; DSS02.01; DSS02.02; DSS04.01; DSS05.02; DSS05.03
	APO14.07	Data quality requirements	Operational level agreements (OLAs)	DSS01.02; DSS02.07; DSS04.03; DSS05.03
APO09.04 Monitor and report service levels.	APO05.03	Investment portfolio performance reports	Improvement action plans and remediations	APO02.02; APO08.02
	APO05.05	• Benefit results and related communications • Corrective actions to improve benefit realization	Service level performance reports	APO08.02; MEA01.03
	APO08.05	Satisfaction analyses		
	APO11.03	• Results of quality monitoring for solution and service delivery • Root causes of quality delivery failures		
	APO11.04	Results of quality reviews and audits		
	DSS02.02	Classified and prioritized incidents and service requests		
	DSS02.06	Closed service requests and incidents		
	DSS02.07	• Incident status and trends report • Status of request fulfilment and trends report		
	EDM04.03	Remedial actions to address resource management deviations		

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO09.05 Review service agreements and contracts.	**From**	**Description**	**Description**	**To**
	APO11.02	Results of quality of service, including customer feedback	Updated SLAs	Internal
	APO11.04	Results of quality reviews and audits		
	BAI04.01	Evaluations against SLAs		
	EDM04.03	Feedback on allocation and effectiveness of resources and capabilities		

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PMBOK Guide Sixth Edition, 2017	Part 1: 12. Project procurement management: Inputs and Outputs

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Service level management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.2. Service Level Management
Service level management	Skills Framework for the Information Age V6, 2015	SLMO

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Service level agreement (SLA) policy	Describes general standards and criteria to inform specific requirements and terms for delivery of services, whether between entities within the enterprise or between the enterprise and a third party.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Establish a contract between a service provider (internal or external) and the end user that defines expected level of service. Make sure this service level is based on output, specifically defining what the customer will receive in SMART objectives (specific, measurable, achievable, realistic and time-phased). Establish a culture in which service levels are respected. Discourage noncompliance through a penalty system.		

G. Component: Services, Infrastructure and Applications
• Contract management system • Service level monitoring tools

Page intentionally left blank

Domain: Align, Plan and Organize Management Objective: APO10 — Managed Vendors	Focus Area: COBIT Core Model

Description

Manage I&T-related products and services provided by all types of vendors to meet enterprise requirements. This includes the search for and selection of vendors, management of relationships, management of contracts, and reviewing and monitoring of vendor performance and vendor ecosystem (including upstream supply chain) for effectiveness and compliance.

Purpose

Optimize available I&T capabilities to support the I&T strategy and road map, minimize the risk associated with nonperforming or noncompliant vendors, and ensure competitive pricing.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG08 Optimization of internal business process functionality	AG05 Delivery of I&T services in line with business requirements
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG01 a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG05 a. Percent of business stakeholders satisfied that I&T service delivery meets agreed service levels b. Number of business disruptions due to I&T service incidents c. Percent of users satisfied with the quality of I&T service delivery
EG08 a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities	

A. Component: Process

Management Practice	Example Metrics
APO10.01 Identify and evaluate vendor relationships and contracts. Continuously search for and identify vendors and categorize them into type, significance and criticality. Establish criteria to evaluate vendors and contracts. Review the overall portfolio of existing and alternative vendors and contracts.	a. Percent of defined evaluation criteria achieved for existing suppliers and contracts b. Percent of alternative suppliers providing equivalent services of existing supplier contracts

Activities	Capability Level
1. Continuously scan the enterprise landscape in search for new partners and vendors that can provide complementary capabilities and support the realization of the I&T strategy, road map and enterprise objectives.	3
2. Establish and maintain criteria relating to type, significance and criticality of vendors and vendor contracts, enabling a focus on preferred and important vendors.	
3. Identify, record and categorize existing vendors and contracts according to defined criteria to maintain a detailed register of preferred vendors that need to be managed carefully.	
4. Establish and maintain vendor and contract evaluation criteria to enable overall review and comparison of vendor performance in a consistent way.	4
5. Periodically evaluate and compare the performance of existing and alternative vendors to identify opportunities or a compelling need to reconsider current vendor contracts.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO10.02 Select vendors. Select suppliers according to a fair and formal practice to ensure a viable best fit based on specified requirements. Requirements should be optimized with input from potential suppliers.	a. Number of identified gaps between the selected supplier's offerings and the needs specified in the request for proposal (RFP) b. Percent of stakeholders satisfied with suppliers

Activities	Capability Level
1. Review all requests for information (RFIs) and requests for proposals (RFPs) to ensure that they clearly define requirements (e.g., enterprise requirements for security and privacy of information, operational business and I&T processing requirements, priorities for service delivery) and include a procedure to clarify requirements. The RFIs and RFPs should allow vendors sufficient time to prepare their proposals and should clearly define award criteria and the decision process.	2
2. Evaluate RFIs and RFPs in accordance with the approved evaluation process/criteria and maintain documentary evidence of the evaluations. Verify the references of candidate vendors.	
3. Select the vendor that best fits the RFP. Document and communicate the decision, and sign the contract.	
4. In the specific case of software acquisition, include and enforce the rights and obligations of all parties in the contractual terms. These rights and obligations may include ownership and licensing of IP; maintenance; warranties; arbitration procedures; upgrade terms; and fit for purpose, including security, privacy, escrow and access rights.	3
5. In the specific case of acquisition of development resources, include and enforce the rights and obligations of all parties in the contractual terms. These rights and obligations may include ownership and licensing of IP; fit for purpose, including development methodologies; testing; quality management processes, including required performance criteria; performance reviews; basis for payment; warranties; arbitration procedures; human resource management; and compliance with the enterprise's policies.	
6. Obtain legal advice on resource development acquisition agreements regarding ownership and licensing of IP.	
7. In the specific case of acquisition of infrastructure, facilities and related services, include and enforce the rights and obligations of all parties in the contractual terms. These rights and obligations may include service levels, maintenance procedures, access controls, security, privacy, performance review, basis for payment and arbitration procedures.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
APO10.03 Manage vendor relationships and contracts. Formalize and manage the supplier relationship for each supplier. Manage, maintain and monitor contracts and service delivery. Ensure that new or changed contracts conform to enterprise standards and legal and regulatory requirements. Deal with contractual disputes.	a. Percent of third-party suppliers who have contracts defining control requirements b. Number of formal disputes with suppliers c. Number of supplier review meetings d. Percent of disputes resolved amicably in a reasonable time frame

Activities	Capability Level
1. Assign relationship owners for all vendors and make them accountable for the quality of service(s) provided.	3
2. Specify a formal communication and review process, including vendor interactions and schedules.	
3. Agree on, manage, maintain and renew formal contracts with the vendor. Ensure that contracts conform to enterprise standards and legal and regulatory requirements.	
4. Include provisions in contracts with key service vendors for review of the vendor site and internal practices and controls by management or independent third parties. Agree on independent audit and assurance controls of the operational environments of vendors providing outsourced services to confirm that agreed requirements are being adequately addressed.	
5. Use established procedures to deal with contract disputes. Whenever possible, first use effective relationships and communications to overcome service problems.	
6. Define and formalize roles and responsibilities for each service vendor. Where several vendors combine to provide a service, consider allocating a lead contractor role to one of the vendors to take responsibility for an overall contract.	
7. Evaluate the effectiveness of the relationship and identify necessary improvements.	4
8. Define, communicate and agree on ways to implement required improvements to the relationship.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISO/IEC 20000-1:2011(E)	7.2 Supplier management
ITIL V3, 2011	Service Design, 4.8 Supplier Management

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO10.04 Manage vendor risk. Identify and manage risk relating to vendors' ability to continually provide secure, efficient and effective service delivery. This also includes the subcontractors or upstream vendors that are relevant in the service delivery of the direct vendor.	a. Frequency of risk management sessions with supplier b. Number of risk-related events leading to service incidents c. Percent of risk-related incidents resolved acceptably (time and cost)

Activities	Capability Level
1. When preparing the contract, provide for potential service risk by clearly defining service requirements, including software escrow agreements, alternative vendors or standby agreements to mitigate possible vendor failure; security and protection of IP; privacy; and any legal or regulatory requirements.	3
2. Identify, monitor and, where appropriate, manage risk relating to the vendor's ability to deliver service efficiently, effectively, securely, confidentially, reliably and continually. Integrate critical internal IT management processes with those of the outsourced service providers, covering, for example, performance and capacity planning, change management, and configuration management.	4
3. Assess the larger ecosystem of the vendor and identify, monitor, and, where appropriate, manage risk related to the subcontractors and upstream vendors influencing the vendor's ability to deliver service efficiently, effectively, securely, reliably and continually.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	RM.MP Manage External Participation
ISF, The Standard of Good Practice for Information Security 2016	SC1.1 External Supplier Management Process
ISO/IEC 27002:2013/Cor.2:2015(E)	15. Supplier relationships
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	D.SC Supply Chain Risk Management

Management Practice	Example Metrics
APO10.05 Monitor vendor performance and compliance. Periodically review overall vendor performance, compliance to contract requirements and value for money. Address identified issues.	a. Number of service breaches to I&T-related services caused by suppliers b. Percent of suppliers meeting agreed requirements

Activities	Capability Level
1. Request independent reviews of vendor internal practices and controls, if necessary.	3
2. Define and document criteria to monitor vendor performance aligned with service level agreements. Ensure that the vendor regularly and transparently reports on agreed criteria.	4
3. Monitor and review service delivery to ensure that the vendor is providing an acceptable quality of service, meeting requirements and adhering to contract conditions.	
4. Review vendor performance and value for money. Ensure that the vendor is reliable and competitive, compared with alternative vendors and market conditions.	
5. Monitor and evaluate externally available information about the vendor and the vendor's supply chain.	
6. Record and assess review results periodically and discuss them with the vendor to identify needs and opportunities for improvement.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

B. Component: Organizational Structures

Key Management Practice	Chief Risk Officer	Chief Information Officer	Chief Technology Officer	Chief Digital Officer	I&T Governance Board	Enterprise Risk Committee	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Privacy Officer	Legal Counsel
APO10.01 Identify and evaluate vendor relationships and contracts.		R	R	R	A				R				R
APO10.02 Select vendors.		R	R	R	A		R	R	R	R	R	R	
APO10.03 Manage vendor relationships and contracts.		R	R	R	A		R	R	R	R			R
APO10.04 Manage vendor risk.	R	R	R	R	A	R	R	R	R	R	R	R	
APO10.05 Monitor vendor performance and compliance.	R	R	R	R	A	R	R	R	R	R			R

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)

Management Practice	Inputs		Outputs	
	From	Description	Description	To
APO10.01 Identify and evaluate vendor relationships and contracts.	Outside COBIT	Vendor contracts	Vendor catalog	BAI02.02
			Potential revisions to vendor contracts	Internal
			Vendor significance and evaluation criteria	Internal
APO10.02 Select vendors.	BAI02.02	High-level acquisition/ development plan	Vendor RFIs and RFPs	BAI02.01; BAI02.02
			RFI and RFP evaluations	BAI02.02
			Decision results of vendor evaluations	vendor evaluations BAI02.02; EDM04.01
APO10.03 Manage vendor relationships and contracts.	BAI03.04	Approved acquisition plan	Results and suggested improvements	Internal
			Communication and review process	Internal
			Vendor roles and responsibilities	Internal
APO10.04 Manage vendor risk.	APO12.04	• Risk analysis and risk profile reports for stakeholders • Results of third-party risk assessments	Identified vendor delivery risk	APO12.01; APO12.03; BAI01.01; BAI11.01
			Identified contract requirements to minimize risk	Internal
APO10.05 Monitor vendor performance and compliance.			Vendor compliance monitoring criteria	Internal
			Vendor compliance monitoring review results	MEA01.03

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this component	

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Contract management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework, 2016	D. Enable—D.8. Contract Management
Contract management	Skills Framework for the Information Age V6, 2015	ITCM
Purchasing	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	D. Enable—D.4. Purchasing
Sourcing	Skills Framework for the Information Age V6, 2015	SORC

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
IT procurement policy	Outlines principles and procedures for procuring IT hardware, software and hosting solutions. Details standards for operating systems, computer networks, hardware specifications, etc. Provides guidelines for contract management (e.g., terms and conditions, monitoring of contracts).		
Third-party IT service delivery management policy	Sets guidelines for managing risk related to third-party services. Establishes framework of expectations for behavior and enumerates security precautions required of third-party service providers in managing risk related to provided services.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Build and manage an ecosystem of vendors that can assist the organization in its digital transformation and innovation. Continuously scan the landscape in search of new and effective partners.		
Management sets the tone and exemplifies correct behaviors when communicating with vendors to agree on and implement required improvements. Ensure that contracts conform to enterprise standards, and legal and regulatory requirements.		

G. Component: Services, Infrastructure and Applications
• Contract management system • Third-party assurance services

Page intentionally left blank

Domain: Align, Plan and Organize Management Objective: APO11 — Managed Quality	Focus Area: COBIT Core Model

Description

Define and communicate quality requirements in all processes, procedures and related enterprise outcomes. Enable controls, ongoing monitoring, and the use of proven practices and standards in continuous improvement and efficiency efforts.

Purpose

Ensure consistent delivery of technology solutions and services to meet the quality requirements of the enterprise and satisfy stakeholder needs.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG04 Quality of financial information • EG07 Quality of management information • EG08 Optimization of internal business process functionality • EG12 Managed digital transformation programs	• AG09 Delivering programs on time, on budget and meeting requirements and quality standards • AG10 Quality of I&T management information

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG01	a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG09	a. Number of programs/projects on time and within budget b. Number of programs needing significant rework due to quality defects c. Percent of stakeholders satisfied with program/project quality
EG04	a. Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of enterprise financial information b. Cost of noncompliance with finance-related regulations	AG10	a. Level of user satisfaction with quality, timeliness and availability of I&T-related management information, taking into account available resources b. Ratio and extent of erroneous business decisions in which erroneous or unavailable I&T-related information was a key factor c. Percentage of information meeting quality criteria
EG07	a. Degree of board and executive management satisfaction with decision-making information b. Number of incidents caused by incorrect business decisions based on inaccurate information c. Time to provide information supporting effective business decisions d. Timeliness of management information		
EG08	a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities		
EG12	a. Number of programs on time and within budget b. Percent of stakeholders satisfied with program delivery c. Percent of business transformation programs stopped d. Percent of business transformation programs with regular reported status updates		

A. Component: Process	
Management Practice	**Example Metrics**
APO11.01 Establish a quality management system (QMS). Establish and maintain a quality management system (QMS) that provides a standard, formal and continuous approach to quality management of information. The QMS should enable technology and business processes to align with business requirements and enterprise quality management.	a. Percent of effectiveness of quality management reviews b. Percent of key stakeholder satisfaction with quality management review program
Activities	**Capability Level**
1. Ensure that the I&T control framework and the business and IT processes include a standard, formal and continuous approach to quality management that is aligned with enterprise requirements. Within the I&T control framework and the business and IT processes, identify quality requirements and criteria (e.g., based on legal requirements and requirements from customers).	3
2. Define roles, tasks, decision rights and responsibilities for quality management in the organizational structure.	
3. Obtain input from management and external and internal stakeholders on the definition of quality requirements and quality management criteria.	
4. Regularly monitor and review the QMS against agreed acceptance criteria. Include feedback from customers, users and management.	4
5. Respond to discrepancies in review results to continuously improve the QMS.	5
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 8.1 Plan quality management
Management Practice	**Example Metrics**
APO11.02 Focus quality management on customers. Focus quality management on customers by determining their requirements and ensuring integration in quality management practices.	a. Percent of customer satisfaction b. Percent of customer requirements and expectations communicated throughout the business and IT organization
Activities	**Capability Level**
1. Focus quality management on customers by determining internal and external customer requirements and ensuring alignment of the I&T standards and practices. Define and communicate roles and responsibilities concerning conflict resolution between the user/customer and the IT organization.	3
2. Manage the business needs and expectations for each business process, IT operational service and new solutions. Maintain their quality acceptance criteria.	
3. Communicate customer requirements and expectations throughout the business and IT organization.	
4. Periodically obtain customer views on business process and service provisioning and IT solution delivery. Determine the impact on I&T standards and practices and ensure that customer expectations are met and actioned.	4
5. Capture quality acceptance criteria for inclusion in SLAs.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
APO11.03 Manage quality standards, practices and procedures and integrate quality management into key processes and solutions. Identify and maintain standards, procedures and practices for key processes to guide the enterprise in meeting the intent of the agreed quality management standards (QMS). This activity should align with I&T control framework requirements. Consider certification for key processes, organizational units, products or services.	a. Number of processes with defined quality requirements b. Number of defects uncovered prior to production c. Number of services with a formal quality management plan d. Number of SLAs that include quality acceptance criteria

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Define the quality management standards, practices and procedures in line with the I&T control framework's requirements and enterprise quality management criteria and policies.	2
2. Integrate the required quality management practices in key processes and solutions across the organization.	3
3. Consider the benefits and costs of quality certifications.	
4. Effectively communicate the quality management approach (e.g., through regular, formal quality training programs).	
5. Record and monitor quality data. Use industry good practices for reference when improving and tailoring the enterprise's quality practices.	4
6. Regularly review the continued relevance, efficiency and effectiveness of specific quality management processes. Monitor the achievement of quality objectives.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 8.2 Manage quality
Management Practice	**Example Metrics**
APO11.04 Perform quality monitoring, control and reviews. Monitor the quality of processes and services on an ongoing basis, in line with quality management standards. Define, plan and implement measurements to monitor customer satisfaction with quality as well as the value provided by the quality management system (QMS). The information gathered should be used by the process owner to improve quality.	a. Percent of solutions and services delivered with formal certification b. Average stakeholder satisfaction rating of solutions and services c. Number of processes with a formal quality assessment report d. Percent of projects reviewed that meet target quality goals and objectives e. Number, robustness and timeliness of risk analyses
Activities	**Capability Level**
1. Prepare and conduct quality reviews for key organizational processes and solutions.	3
2. For these key organizational processes and solutions, monitor goal-driven quality metrics aligned to overall quality objectives.	4
3. Ensure that management and process owners regularly review quality management performance against defined quality metrics.	
4. Analyze overall quality management performance results.	
5. Report the quality management performance review results and initiate improvements where appropriate.	5
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 8.3 Control quality
Management Practice	**Example Metrics**
APO11.05 Maintain continuous improvement. Maintain and regularly communicate an overall quality plan that promotes continuous improvement. The plan should define the need for, and benefits of, continuous improvement. Collect and analyze data about the quality management system (QMS) and improve its effectiveness. Correct nonconformities to prevent recurrence.	a. Number of root cause analyses performed b. Percent of on-time and complete services and products
Activities	**Capability Level**
1. Establish a platform to share good practices and capture information on defects and mistakes to enable learning from them.	2
2. Identify examples of excellent quality delivery processes that can benefit other services or projects. Share these with the service and project delivery teams to encourage improvement.	3
3. Identify recurring examples of quality defects. Determine their root cause, evaluate their impact and result, and agree on improvement actions with the service and/or project delivery teams.	
4. Provide employees with training in the methods and tools of continual improvement.	
5. Benchmark the results of the quality reviews against internal historical data, industry guidelines, standards and data from similar types of enterprises.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	DE.DP Detection Processes

B. Component: Organizational Structures

Key Management Practice	Chief Operating Officer	Chief Risk Officer	Chief Information Officer	Chief Technology Officer	Chief Digital Officer	I&T Governance Board	Business Process Owners	Portfolio Manager	Program Manager	Project Manager	Project Management Office	Data Management Function	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager
APO11.01 Establish a quality management system (QMS).	A		R		R											R	R		
APO11.02 Focus quality management on customers.			A		R		R										R		
APO11.03 Manage quality standards, practices and procedures and integrate quality management into key processes and solutions.			A	R	R		R	R	R	R	R	R	R	R	R	R	R	R	R
APO11.04 Perform quality monitoring, control and reviews.		R	A		R	R	R										R		
APO11.05 Maintain continuous improvement.			A				R	R	R	R	R		R	R	R	R	R	R	R

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)

Management Practice	Inputs		Outputs	
	From	Description	Description	To
APO11.01 Establish a quality management system (QMS).	Outside COBIT	Enterprisewide quality system	Quality management system (QMS) roles, responsibilities and decision rights	APO01.05; DSS06.03
			Quality management plans	APO14.04; APO14.06; BAI01.07; BAI11.05
			Results of QMS effectiveness reviews	BAI03.06
APO11.02 Focus quality management on customers.	Outside COBIT	Business and customer quality requirements	Customer requirements for quality management	APO08.05; APO09.03; BAI01.07; BAI11.06
			Results of quality of service, including customer feedback	APO08.05; APO09.05; BAI05.01; BAI07.07
			Acceptance criteria	BAI02.01; BAI02.02

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
APO11.03 Manage quality standards, practices and procedures and integrate quality management into key processes and solutions.	BAI02.04	Approved quality reviews	Quality management standards	All APO; All BAI; All DSS; All MEA
	Outside COBIT	• Available quality certifications • Industry good practices	Root causes of quality delivery failures	APO08.02; APO09.04; BAI07.08; MEA02.04; MEA04.04
			Results of quality monitoring	APO08.05; APO09.04; BAI07.08
APO11.04 Perform quality monitoring, control and reviews.	BAI03.06	• Quality assurance plan • Quality review results, exceptions and corrections	Process quality of service goals and metrics	All APO; All BAI; All DSS; All MEA
	DSS02.07	• Incident status and trends report • Status of request fulfilment and trends report	Results of quality reviews and audits	APO08.05; APO09.04; APO09.05; BAI07.08
APO11.05 Maintain continuous improvement.			Quality review benchmark results	All APO; All BAI; All DSS; All MEA
			Examples of good practice to be shared	All APO; All BAI; All DSS; All MEA
			Communications on continual improvement and best practices	All APO; All BAI; All DSS; All MEA

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PMBOK Guide Sixth Edition, 2017	Part 1: 8. Project quality management: Inputs and Outputs

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
ICT quality strategy development	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	D. Enable—D.2. ICT Quality Strategy Development
Quality assurance	Skills Framework for the Information Age V6, 2015	QUAS
Quality management	Skills Framework for the Information Age V6, 2015	QUMG
Quality standards	Skills Framework for the Information Age V6, 2015	QUST

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Quality management policy	Captures management's vision of enterprise quality objectives, acceptable level of quality, and duties of specific teams and entities to ensure quality.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Promote a culture of quality and continual improvement. Maintain and regularly communicate the need for, and benefits of, quality and continuous improvement.		

G. Component: Services, Infrastructure and Applications
• QMS • Third-party quality assurance services

Domain: Align, Plan and Organize Management Objective: APO12 — Managed Risk	Focus Area: COBIT Core Model

Description

Continually identify, assess and reduce I&T-related risk within tolerance levels set by enterprise executive management.

Purpose

Integrate the management of I&T-related enterprise risk with overall enterprise risk management (ERM) and balance the costs and benefits of managing I&T-related enterprise risk.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG02 Managed business risk • EG06 Business service continuity and availability	• AG02 Managed I&T-related risk • AG07 Security of information, processing infrastructure and applications, and privacy
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG02 a. Percent of critical business objectives and services covered by risk assessment b. Ratio of significant incidents that were not identified in risk assessments vs. total incidents c. Frequency of updating risk profile	AG02 a. Frequency of updating risk profile b. Percent of enterprise risk assessments including I&T-related risk c. Number of significant I&T-related incidents that were not identified in a risk assessment
EG06 a. Number of customer service or business process interruptions causing significant incidents b. Business cost of incidents c. Number of business processing hours lost due to unplanned service interruptions d. Percent of complaints as a function of committed service availability targets	AG07 a. Number of confidentiality incidents causing financial loss, business disruption or public embarrassment b. Number of availability incidents causing financial loss, business disruption or public embarrassment c. Number of integrity incidents causing financial loss, business disruption or public embarrassment

A. Component: Process

Management Practice	Example Metrics
APO12.01 Collect data. Identify and collect relevant data to enable effective I&T-related risk identification, analysis and reporting.	a. Number of loss events with key characteristics captured in repositories b. Percent of audits, events and trends captured in repositories c. Percent of critical systems with known issues

Activities	Capability Level
1. Establish and maintain a method for the collection, classification and analysis of I&T risk-related data.	2
2. Record relevant and significant I&T risk-related data on the enterprise's internal and external operating environment.	
3. Adopt or define a risk taxonomy for consistent definitions of risk scenarios and impact and likelihood categories.	3
4. Record data on risk events that have caused or may cause business impacts as per the impact categories defined in the risk taxonomy. Capture relevant data from related issues, incidents, problems and investigations.	
5. Survey and analyze the historical I&T risk data and loss experience from externally available data and trends, industry peers through industry-based event logs, databases, and industry agreements for common event disclosure.	4
6. For similar classes of events, organize the collected data and highlight contributing factors. Determine common contributing factors across multiple events.	
7. Determine the specific conditions that existed or were absent when risk events occurred and the way the conditions affected event frequency and loss magnitude.	
8. Perform periodic event and risk factor analysis to identify new or emerging risk issues and to gain an understanding of the associated internal and external risk factors.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Data Management Maturity Model, 2014	Supporting Processes - Risk Management
COSO Enterprise Risk Management, June 2017	8. Performance—Principle 10
ISO/IEC 27005:2011(E)	8.2 Risk identification; 12. Information security risk monitoring and review
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.1 Preparation (Task 7)

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO12.02 Analyze risk. Develop a substantiated view on actual I&T risk, in support of risk decisions.	a. Number of identified I&T risk scenarios b. Time since last update of I&T risk scenarios

Activities	Capability Level
1. Define the appropriate scope of risk analysis efforts, considering all risk factors and/or the business criticality of assets.	3
2. Build and regularly update I&T risk scenarios; I&T-related loss exposures; and scenarios regarding reputational risk, including compound scenarios of cascading and/or coincidental threat types and events. Develop expectations for specific control activities and capabilities to detect.	
3. Estimate the frequency (or likelihood) and magnitude of loss or gain associated with I&T risk scenarios. Take into account all applicable risk factors and evaluate known operational controls.	
4. Compare current risk (I&T-related loss exposure) to risk appetite and acceptable risk tolerance. Identify unacceptable or elevated risk.	
5. Propose risk responses for risk exceeding risk appetite and tolerance levels.	
6. Specify high-level requirements for projects or programs that will implement the selected risk responses. Identify requirements and expectations for appropriate key controls for risk mitigation responses.	
7. Validate the risk analysis and business impact analysis (BIA) results before using them in decision making. Confirm that the analysis aligns with enterprise requirements and verify that estimations were properly calibrated and scrutinized for bias.	4
8. Analyze cost/benefit of potential risk response options such as avoid, reduce/mitigate, transfer/share, and accept and exploit/seize. Confirm the optimal risk response.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Data Management Maturity Model, 2014	Supporting Processes—Risk Management
COSO Enterprise Risk Management, June 2017	8. Performance—Principle 11
ISF, The Standard of Good Practice for Information Security 2016	IR2.1 Risk Assessment Scope; IR2.2 Business Impact Assessment
ISO/IEC 27001:2013/Cor.2:2015(E)	8.2 Information security risk assessment
ISO/IEC 27005:2011(E)	8.3 Risk analysis
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	ID.RA Risk Assessment
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.6 Authorization (Task 3)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.17 Risk assessment (RA-3)

Management Practice	Example Metrics
APO12.03 Maintain a risk profile. Maintain an inventory of known risk and risk attributes, including expected frequency, potential impact and responses. Document related resources, capabilities and current control activities related to risk items.	a. Completeness of attributes and values in the risk profile b. Percent of key business processes included in the risk profile

Activities	Capability Level
1. Inventory business processes and document their dependency on I&T service management processes and IT infrastructure resources. Identify supporting personnel, applications, infrastructure, facilities, critical manual records, vendors, suppliers and outsourcers.	2
2. Determine and agree on which I&T services and IT infrastructure resources are essential to sustain the operation of business processes. Analyze dependencies and identify weak links.	
3. Aggregate current risk scenarios by category, business line and functional area.	
4. Regularly capture all risk profile information and consolidate it into an aggregated risk profile.	3
5. Capture information on the status of the risk action plan for inclusion in the I&T risk profile of the enterprise.	
6. Based on all risk profile data, define a set of risk indicators that allow the quick identification and monitoring of current risk and risk trends.	4
7. Capture information on I&T risk events that have materialized for inclusion in the IT risk profile of the enterprise.	

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	RS.DT Define Organizational Risk Tolerance
COSO Enterprise Risk Management, June 2017	8. Performance—Principle 12
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.17 Risk assessment (RA-7)
Management Practice	**Example Metrics**
APO12.04 Articulate risk. Communicate information on the current state of I&T-related exposures and opportunities in a timely manner to all required stakeholders for appropriate response.	a. Level of stakeholder satisfaction with provided risk reporting b. Completeness of risk profile reporting (including information in line with stakeholder requirements) c. Use of risk reporting in management decision making
Activities	**Capability Level**
1. Report the results of risk analysis to all affected stakeholders in terms and formats useful to support enterprise decisions. Whenever possible, include probabilities and ranges of loss or gain along with confidence levels, to enable management to balance risk-return.	3
2. Provide decision makers with an understanding of worst-case and most-probable scenarios, I&T-related loss exposures and significant reputation, legal and regulatory considerations, or any other impact category as per the risk taxonomy.	
3. Report the current risk profile to all stakeholders. Include information on the effectiveness of the risk management process, control effectiveness, gaps, inconsistencies, redundancies, remediation status and their impacts on the risk profile.	
4. On a periodic basis, for areas with relative risk and risk capacity parity, identify I&T-related opportunities that would allow the acceptance of greater risk and enhanced growth and return.	
5. Review the results of objective third-party assessments and internal audit and quality assurance reviews. Include them in the risk profile. Review identified gaps and I&T-related loss exposures to determine the need for additional risk analysis.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	RS.CR Determine Critical Infrastructure Requirements
COSO Enterprise Risk Management, June 2017	10. Information, Communication, and Reporting—Principle 19
ISO/IEC 27005:2011(E)	11. Information security risk communication and consultation
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	ID.RM Risk Management Strategy
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.15 Program management (PM-32)
Management Practice	**Example Metrics**
APO12.05 Define a risk management action portfolio. Manage opportunities to reduce risk to an acceptable level as a portfolio.	a. Number of significant incidents not identified and included in the risk management portfolio b. Percent of risk management project proposals rejected due to lack of consideration of other related risk
Activities	**Capability Level**
1. Maintain an inventory of control activities that are in place to mitigate risk and that enable risk to be taken in line with the risk appetite and tolerance. Classify control activities and map them to specific I&T risk scenarios and aggregations of I&T risk scenarios.	2
2. Determine whether each organizational entity monitors risk and accepts accountability for operating within its individual and portfolio tolerance levels.	3
3. Define a balanced set of project proposals designed to reduce risk and/or projects that enable strategic enterprise opportunities, considering costs, benefits, effect on current risk profile and regulations.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Supporting Processes—Risk Management
COSO Enterprise Risk Management, June 2017	8. Performance—Principle 14
HITRUST CSF version 9, September 2017	03.01 Risk Management Program

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO12.06 Respond to risk. Respond in a timely manner to materialized risk events with effective measures to limit the magnitude of loss.	a. Number of measures not reducing residual risk b. Percent of I&T risk action plans executed as designed

Activities	Capability Level
1. Prepare, maintain and test plans that document the specific steps to take when a risk event may cause a significant operational or development incident with serious business impact. Ensure that plans include pathways of escalation across the enterprise.	3
2. Apply the appropriate response plan to minimize the impact when risk incidents occur.	
3. Categorize incidents and compare I&T-related loss exposures against risk tolerance thresholds. Communicate business impacts to decision makers as part of reporting and update the risk profile.	4
4. Examine past adverse events/losses and missed opportunities and determine root causes.	
5. Communicate root cause, additional risk response requirements and process improvements to appropriate decision makers. Ensure that the cause, response requirements and process improvement are included in risk governance processes.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
COSO Enterprise Risk Management, June 2017	8. Performance—Principle 13
ISF, The Standard of Good Practice for Information Security 2016	IR2.9 Risk Treatment
ISO/IEC 27001:2013/Cor.2:2015(E)	6.1 Action to address risk and opportunities
ISO/IEC 27005:2011(E)	9. Information security risk treatment
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.6 Authorization (Task 4)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.15 Program management (PM-9, PM-31)

B. Component: Organizational Structures

Key Management Practice	Chief Risk Officer	Chief Information Officer	Chief Technology Officer	Chief Digital Officer	Enterprise Risk Committee	Chief Information Security Officer	Business Process Owners	Project Management Office	Data Management Function	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO12.01 Collect data.	A	R	R	R		R	R	R	R	R	R	R	R	R	R	R	R
APO12.02 Analyze risk.	A	R			R		R										
APO12.03 Maintain a risk profile.	A	R			R		R										
APO12.04 Articulate risk.	A	R			R		R										
APO12.05 Define a risk management action portfolio.	A	R			R		R										
APO12.06 Respond to risk.	R	A	R	R		R	R	R		R	R	R	R	R	R	R	R

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.1 Preparation (Task 1); Appendix A: Roles and Responsibilities

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
APO12.01 Collect data.	**From**	**Description**	**Description**	**To**
	APO02.02	Gaps and risk related to current capabilities	Emerging risk issues and factors	APO01.01; APO02.02; EDM03.01
	APO02.05	Risk assessment initiatives	Data on risk events and contributing factors	Internal
	APO10.04	Identified vendor delivery risk	Data on the operating environment relating to risk	Internal
	DSS02.07	Incident status and trends report		
	EDM03.01	Evaluation of risk management activities		
	EDM03.02	• Risk management policies • Key objectives to be monitored for risk management • Approved process for measuring risk management		
APO12.02 Analyze risk.	DSS04.02	Business impact analyses (BIAs)	Risk analysis results	APO01.01; APO02.02; EDM03.03; BAI01.08; BAI11.06
	DSS05.01	Evaluations of potential threats	I&T risk scenarios	Internal
	Outside COBIT	Threat advisories	Scope of risk analysis efforts	Internal
APO12.03 Maintain a risk profile.	APO10.04	Identified vendor delivery risk	Aggregated risk profile, including status of risk management actions	APO02.02; EDM03.02
	DSS05.01	Evaluations of potential threats	Documented risk scenarios by line of business and function	Internal
	EDM03.01	• Risk appetite guidance • Approved risk tolerance levels		
APO12.04 Articulate risk.			Risk analysis and risk profile reports for stakeholders	APO10.04; EDM03.03; EDM05.02; MEA04.05
			Results of third-party risk assessments	APO10.04; EDM03.03; MEA02.01
			Opportunities for acceptance of greater risk	EDM03.03

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO12.05 Define a risk management action portfolio.	**From**	**Description**	**Description**	**To**
			Project proposals for reducing risk	APO02.02; APO13.02
APO12.06 Respond to risk.	EDM03.03	Remedial actions to address risk management deviations	Risk impact communication	APO01.02; APO08.04; DSS04.02
			Risk-related root causes	DSS02.03; DSS03.01; DSS03.02; DSS03.03; DSS03.05; DSS04.02; MEA02.04; MEA04.04; MEA04.06
			Risk-related incident response plans	DSS02.05

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
COSO Enterprise Risk Management, June 2017	10. Information, Communication, and Reporting—Principle 20
SF, The Standard of Good Practice for Information Security 2016	IR1.3 Information Risk Assessment—Supporting Material
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.1 Preparation (Task 7): Inputs and Outputs; 3.6 Authorization (Task 3, 4): Inputs and Outputs
PMBOK Guide Sixth Edition, 2017	Part 1: 11. Project risk management: Inputs and Outputs

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Business risk management	Skills Framework for the Information Age V6, 2015	BURM
Information assurance	Skills Framework for the Information Age V6, 2015	INAS
Risk management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.3. Risk Management

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Enterprise risk policy	Defines governance and management of enterprise risk at strategic, tactical and operational levels, pursuant to business objectives. Translates enterprise governance into risk governance principles and policy and elaborates risk management activities.	National Institute of Standards and Technology Special Publication 800- 53, Revision 5 (Draft), August 2017	3.17 Risk assessment (RA-1)
Fraud risk policy	Informs protection of enterprise brand, reputation and assets in the event of loss or damage resulting from fraud or misconduct. Guides employees in reporting suspicious activity and handling sensitive information and evidence. Encourages antifraud culture and cultivates awareness of risk.	National Institute of Standards and Technology Special Publication 800- 37, Revision 2 (Draft), May 2018	

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
To support a transparent and participatory risk culture, senior management should set direction and demonstrate visible and genuine support for incorporation of risk practices throughout the enterprise. Management should encourage open communication and business ownership for I&T-related business risk. Desirable behaviors include aligning policies to the defined risk appetite, reporting risk trends to senior management and risk governing bodies, rewarding effective risk management, and proactively monitoring risk and progress on the risk action plan.	ISF, The Standard of Good Practice for Information Security 2016	IR1.2 Information Risk Assessment

G. Component: Services, Infrastructure and Applications
• Crisis management services • Governance, risk and compliance (GRC) tools • Risk analysis tools • Risk intelligence services

Page intentionally left blank

Domain: Align, Plan and Organize Management Objective: APO13 — Managed Security	Focus Area: COBIT Core Model

Description

Define, operate and monitor an information security management system.

Purpose

Keep the impact and occurrence of information security incidents within the enterprise's risk appetite levels.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG02 Managed business risk • EG06 Business service continuity and availability	AG07 Security of information, processing infrastructure and applications, and privacy

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG02	a. Percent of critical business objectives and services covered by risk assessment b. Ratio of significant incidents that were not identified in risk assessments vs. total incidents c. Frequency of updating risk profile	AG07	a. Number of confidentiality incidents causing financial loss, business disruption or public embarrassment b. Number of availability incidents causing financial loss, business disruption or public embarrassment c. Number of integrity incidents causing financial loss, business disruption or public embarrassment
EG06	a. Number of customer service or business process interruptions causing significant incidents b. Business cost of incidents c. Number of business processing hours lost due to unplanned service interruptions d. Percent of complaints as a function of committed service availability targets		

A. Component: Process

Management Practice	Example Metrics
APO13.01 Establish and maintain an information security management system (ISMS). Establish and maintain an information security management system (ISMS) that provides a standard, formal and continuous approach to information security management, enabling secure technology and business processes that are aligned with business requirements.	a. Level of stakeholder satisfaction with the security plan throughout the enterprise

Activities	Capability Level
1. Define the scope and boundaries of the information security management system (ISMS) in terms of the characteristics of the enterprise, the organization, its location, assets and technology. Include details of, and justification for, any exclusions from the scope.	2
2. Define an ISMS in accordance with enterprise policy and the context in which the enterprise operates.	
3. Align the ISMS with the overall enterprise approach to the management of security.	
4. Obtain management authorization to implement and operate or change the ISMS.	
5. Prepare and maintain a statement of applicability that describes the scope of the ISMS.	
6. Define and communicate Information security management roles and responsibilities.	
7. Communicate the ISMS approach.	

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
HITRUST CSF version 9, September 2017	0.01 Information Security Management program
ISO/IEC 20000-1:2011(E)	6.6 Information security management
ITIL V3, 2011	Service Design, 4.7 Information Security Management
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.3 Selection (Task 1); 3.4 Implementation (Task 1)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.17 Risk assessment (RA-2)
Management Practice	**Example Metrics**
APO13.02 Define and manage an information security and privacy risk treatment plan. Maintain an information security plan that describes how information security risk is to be managed and aligned with enterprise strategy and enterprise architecture. Ensure that recommendations for implementing security improvements are based on approved business cases, implemented as an integral part of services and solutions development, and operated as an integral part of business operation.	a. Percentage of successful security risk scenario simulations b. Number of employees who have successfully completed information security awareness training

Activities	Capability Level
1. Formulate and maintain an information security risk treatment plan aligned with strategic objectives and the enterprise architecture. Ensure that the plan identifies the appropriate and optimal management practices and security solutions, with associated resources, responsibilities and priorities for managing identified information security risk.	3
2. Maintain as part of the enterprise architecture an inventory of solution components that are in place to manage security-related risk.	
3. Develop proposals to implement the information security risk treatment plan, supported by suitable business cases that include consideration of funding and allocation of roles and responsibilities.	
4. Provide input to the design and development of management practices and solutions selected from the information security risk treatment plan.	
5. Implement information security and privacy training and awareness programs.	
6. Integrate the planning, design, implementation and monitoring of information security and privacy procedures and other controls capable of enabling prompt prevention, detection of security events, and response to security incidents.	
7. Define how to measure the effectiveness of the selected management practices. Specify how these measurements are to be used to assess effectiveness to produce comparable and reproducible results.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	
Management Practice	**Example Metrics**
APO13.03 Monitor and review the information security management system (ISMS). Maintain and regularly communicate the need for, and benefits of, continuous improvement in information security. Collect and analyze data about the information security management system (ISMS), and improve its effectiveness. Correct nonconformities to prevent recurrence.	a. Frequency of scheduled security reviews b. Number of findings in regularly scheduled security reviews c. Level of stakeholder satisfaction with the security plan d. Number of security-related incidents caused by failure to adhere to the security plan

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Undertake regular reviews of the effectiveness of the ISMS. Include meeting ISMS policy and objectives and reviewing security and privacy practices.	4
2. Conduct ISMS audits at planned intervals.	
3. Undertake a management review of the ISMS on a regular basis to ensure that the scope remains adequate and improvements in the ISMS process are identified.	
4. Record actions and events that could have an impact on the effectiveness or performance of the ISMS.	
5. Provide input to the maintenance of the security plans to take into account the findings of monitoring and reviewing activities.	5
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.3 Selection (Task 3)

B. Component: Organizational Structures															
Key Management Practice	**Chief Information Officer**	**Chief Technology Officer**	**Enterprise Risk Committee**	**Chief Information Security Officer**	**Business Process Owners**	**Project Management Office**	**Head Architect**	**Head Development**	**Head IT Operations**	**Head IT Administration**	**Service Manager**	**Information Security Manager**	**Business Continuity Manager**	**Privacy Officer**
APO13.01 Establish and maintain an information security management system (ISMS).	R		R	A						R		R		
APO13.02 Define and manage an information security and privacy risk treatment plan.	R		R	A						R		R		R
APO13.03 Monitor and review the information security management system (ISMS).	R	R		A	R	R	R	R	R	R	R	R	R	R

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISF, The Standard of Good Practice for Information Security 2016	SG1.2 Security Direction
ISO/IEC 27002:2013/Cor.2:2015(E)	6.1 Internal organization

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
APO13.01 Establish and maintain an information security management system (ISMS).	Outside COBIT	Enterprise security approach	ISMS scope statement	APO01.05; DSS06.03
			ISMS policy	Internal
APO13.02 Define and manage an information security risk treatment plan.	APO02.04	Gaps and changes required to realize target capability	Information security risk treatment plan	All APO; All BAI; All DSS; All MEA; ALL EDM
	APO03.02	Baseline domain descriptions and architecture definition	Information security business cases	APO05.02
	APO12.05	Project proposals for reducing risk		

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO13.03 Monitor and review the information security management system (ISMS).	**From**	**Description**	**Description**	**To**
	DSS02.02	Classified and prioritized incidents and service requests	Recommendations for improving the information security management system (ISMS)	Internal
			Information security management system (ISMS) audit reports	MEA02.01
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017		3.3 Selection (Tasks 1, 3): Inputs and Outputs; 3.4 Implementation (Task 1): Inputs and Outputs		

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Information security	Skills Framework for the Information Age V6, 2015	SCTY
Information security strategy development	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework, 2016	D. Enable—D.1. Information Security Strategy Development

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Information security and privacy policy	Sets behavioral guidelines to protect corporate information, systems and infrastructure. Given that business requirements regarding security and storage are more dynamic than I&T risk management and privacy, their governance should be handled separately from that of I&T risk and privacy. For operational efficiency, synchronize information security policy with I&T risk and privacy policy.	(1) ISO/IEC 27001:2013/ Cor.2:2015(E); (2) ISO/IEC 27002:2013/Cor.2:2015(E); (3) National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017; (4) HITRUST CSF version 9, September 2017; (5) ISF, The Standard of Good Practice for Information Security 2016	(1) 5.2 Policy; (2) 5. Information security policies; (3) 3.2 Awareness and training (AT-1); (4) 04.01 Information Security Policy; (5) SM1.1 Information Security Policy

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Establish a culture of security and privacy awareness that positively influences desirable behavior and actual implementation of security and privacy policy in daily practice. Provide sufficient security and privacy guidance, indicate security and privacy champions (including C-level executives, leaders in HR, and security and/or privacy professionals) and proactively support and communicate security and privacy programs, innovations and challenges.	(1) ISO/IEC 27001:2013/ Cor.2:2015(E); (2) Creating a Culture of Security, ISACA, 2011	1) 7.3 Awareness; (2) Framework to achieve an intentional security aware culture (all chapters)

G. Component: Services, Infrastructure and Applications
• Configuration management tools • Security and privacy awareness services • Third-party security assessment services

Domain: Align, Plan and Organize Management Objective: APO14 — Managed Data	Focus Area: COBIT Core Model

Description

Achieve and sustain effective management of the enterprise data assets across the data life cycle, from creation through delivery, maintenance and archiving.

Purpose

Ensure effective utilization of the critical data assets to achieve enterprise goals and objectives.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG04 Quality of financial information • EG07 Quality of management information	AG10 Quality of I&T management information

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG04	a. Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of enterprise financial information b. Cost of noncompliance with finance-related regulations	AG10	a. Level of user satisfaction with quality, timeliness and availability of I&T-related management information, taking into account available resources b. Ratio and extent of erroneous business decisions in which erroneous or unavailable I&T-related information was a key factor c. Percentage of information meeting quality criteria
EG07	a. Degree of board and executive management satisfaction with decision-making information b. Number of incidents caused by incorrect business decisions based on inaccurate information c. Time to provide information supporting effective business decisions d. Timeliness of management information		

A. Component: Process

Management Practice	Example Metrics
APO14.01 Define and communicate the organization's data management strategy and roles and responsibilities. Define how to manage and improve the organization's data assets, in line with enterprise strategy and objectives. Communicate the data management strategy to all stakeholders. Assign roles and responsibilities to ensure that corporate data are managed as critical assets and the data management strategy is implemented and maintained in an effective and sustainable manner.	a. Number of data management breaches in comparison to the defined strategy b. Percent of roles and responsibilities identified to support the governance of data management and the interaction between governance and the data management function

Activities	Capability Level
1. Establish a data management function with responsibility for managing activities that support data management objectives.	2
2. Specify roles and responsibilities to support the management of data and the interaction between governance and the data management function.	
3. Ensure that business and technology collaboratively develop the organization's data management strategy. Make sure that data management objectives, priorities and scope reflect enterprise objectives, are consistent with data management policies and regulation, and are approved by all stakeholders.	3
4. Communicate data management objectives, priorities and scope and adjust them as needed, based upon feedback.	
5. Use metrics to assess and monitor the achievement of objectives for data management.	4
6. Monitor the sequence plan for implementation of the data management strategy. Update it as needed, based on progress reviews.	
7. Use statistical and other quantitative techniques to evaluate the effectiveness of strategic data management objectives in achieving business objectives. Make modifications as needed, based on metrics.	
8. Ensure that the organization researches innovative business processes and emerging regulatory requirements to ensure that the data management program is compatible with future business needs.	5
9. Make contributions to industry best practices for data management strategy development and implementation.	

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Data Management Strategy - Data Management Strategy; Data Governance—Governance Management
ITIL V3, 2011	Service Design, 5.2 Management of Data and Information
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 13: Data Protection
Management Practice	**Example Metrics**
APO14.02 Define and maintain a consistent business glossary. Create, approve, update and promote consistent business terms and definitions to foster shared data usage across the organization.	a. Level of acceptance and frequency of use of business glossary terms throughout the entire organization b. Number of synonyms for defined business glossary terminology that are used in new development efforts c. Level of granularity of defined business glossary terms

Activities	Capability Level
1. Ensure that standard business terms are readily available and communicated to relevant stakeholders.	2
2. Ensure that each business term added to the business glossary has a unique name and unique definition.	
3. Use standard industry business terms and definitions, as appropriate, in the business glossary.	
4. Establish, document and follow a process to define, manage, use and maintain the business glossary. For example, new initiatives should apply standard business terms as part of the data requirements definition process to ensure consistency of language. This will help achieve comparability of the content and facilitate data sharing across the organization.	3
5. Ensure that new development, data integration and data consolidation efforts apply standard business terms as part of the data requirements definition process.	
6. Integrate the business glossary into the organization's metadata repository, with appropriate access permissions.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Data Management Maturity Model, 2014	Data Governance - Business Glossary
ISF, The Standard of Good Practice for Information Security 2016	IM1.1 Information Classification and Handling
Management Practice	**Example Metrics**
APO14.03 Establish the processes and infrastructure for metadata management. Establish the processes and infrastructure for specifying and extending metadata about the organization's data assets, fostering and supporting data sharing, ensuring compliant use of data, improving responsiveness to business changes and reducing data-related risk.	a. Number of identified inaccuracies in metadata b. Percent of metadata containing measures and metrics to evaluate the accuracy and adoption of metadata

Activities	Capability Level
1. Establish and follow a metadata management process.	2
2. Ensure that metadata documentation captures data interdependencies.	
3. Establish and follow metadata categories, properties and standards.	
4. Develop and use metadata to perform impact analysis on potential data changes.	3
5. Populate the organization's metadata repository with additional categories and classifications of metadata according to a phased implementation plan. Link it to architecture layers.	
6. Validate metadata and any changes to metadata against the existing architecture.	
7. Ensure that the organization has developed an integrated metamodel deployed across all platforms.	
8. Ensure that metadata types and data definitions support consistent import, subscription and consumption practices.	
9. Use measures and metrics to evaluate the accuracy and adoption of metadata.	4
10. Evaluate planned data changes for impact on the metadata repository. Continuously improve metadata capture, change and refinement processes.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Data Management Maturity Model, 2014	Data Governance—Metadata Management
ISO/IEC 27002:2013/Cor.2:2015(E)	8.2 Information classification

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO14.04 Define a data quality strategy. Define an integrated, organizationwide strategy to achieve and maintain the level of data quality (such as complexity, integrity, accuracy, completeness, validity, traceability and timeliness) required to support the business goals and objectives.	a. Number of data quality improvement efforts identified and recorded in a sequence plan b. Percent of stakeholders satisfied with the quality of data
Activities	**Capability Level**
1. Define a data quality strategy in collaboration with business and technology stakeholders, approved by executive management, and managed. The strategy should facilitate moving from the current to the target state. It should also explicitly align with business objectives and the organization's data management strategy.	3
2. Ensure that the data quality strategy is followed across the organization and is accompanied by corresponding policies, processes and guidelines.	
3. Anchor the policies, processes and governance contained in the data quality strategy across the data life cycle. Mandate corresponding processes in the system development life cycle methodology.	
4. Develop, monitor and maintain a sequence plan for data quality improvement efforts across the organization.	
5. To evaluate progress, monitor plans to meet the goals and objectives of the data quality strategy.	4
6. Systematically collect stakeholder reports of data quality issues. Include their expectations for improving data quality in the data quality strategy. Measure and monitor them.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	DP.DR Safeguard Data at Rest; DP.DT Safeguard Data in Transit; DP.IP Integrity and Data Leak Prevention
CMMI Data Management Maturity Model, 2014	Data Quality - Data Quality Strategy
Management Practice	**Example Metrics**
APO14.05 Establish data profiling methodologies, processes and tools. Implement standardized data profiling methodologies, processes, practices, tools and templates that can be applied across multiple data repositories and data stores.	a. Number of defined and implemented data templates and their usage percentage b. Number of shared data sets with a defined data profile
Activities	**Capability Level**
1. Define and standardize data profiling methodologies, processes, practices, tools and results templates. Ensure that profiling processes are reusable and leveraged across multiple data stores and shared data repositories.	3
2. Engage data management to identify core shared data sets that are regularly profiled and monitored.	4
3. In data profiling efforts, include evaluation of the conformity of data content with its approved metadata and standards.	
4. During a data profiling activity, compare actual issues to the statistically predicted issues, based on historical profiling results.	
5. Ensure that results are centrally stored, systematically monitored and analyzed with respect to statistics and metrics. Provide the resulting insight to data quality improvements over time.	
6. Create real-time or near real-time automated profiling reports for all critical data feeds and repositories.	5
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Data Quality—Data Profiling
National Institute of Standards and Technology Special Publication 800-53, Revision 5, August 2017	3.20 System and information integrity (SI-1)
Management Practice	**Example Metrics**
APO14.06 Ensure a data quality assessment approach. Provide a systematic approach to measure and evaluate data quality according to processes and techniques, and against data quality rules.	a. Number of identified issues in data quality assessment results b. Number of data quality assessment results that include recommendations for remediation

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Periodically conduct data quality assessments, according to an approved frequency per the data quality assessment policy. Ensure that data governance determines the key set of attributes by subject area for data quality assessments.	4
2. Include recommendations for remediation, with supporting rationale, in data quality assessment results.	
3. Assess data quality, using established thresholds and targets for each selected quality dimension.	
4. Systematically generate data quality measurement reports, based on criticality of attributes and data volatility.	
5. Continuously review and improve data quality assessment and reporting processes.	5
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Data Quality—Data Quality Assessment
Management Practice	**Example Metrics**
APO14.07 Define the data cleansing approach. Define the mechanisms, rules, processes, and methods to validate and correct data according to predefined business rules.	a. Percent of data cleansed correctly b. Percent of SLAs that include data quality criteria and hold data providers accountable for cleansed data
Activities	**Capability Level**
1. Establish and maintain a data cleansing policy.	2
2. Maintain data change history through cleansing activities.	3
3. Establish methods for correcting the data and define those methods within a plan. Methods may include multiple repository comparison, verification against a valid source, logic checks, referential integrity or range tolerance.	4
4. In service level agreements, include data quality criteria to hold data providers accountable for cleansed data.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Data Quality—Data Cleansing
Management Practice	**Example Metrics**
APO14.08 Manage the life cycle of data assets. Ensure that the organization understands, maps, inventories and controls its data flows through business processes over the data life cycle, from creation or acquisition to retirement.	a. Number of requirements from data consumers that cannot be mapped to a data source b. Number of shared data sets c. Time since last compliance check regarding mappings of business processes to data
Activities	**Capability Level**
1. Map and align the requirements of data consumers and producers.	2
2. Define business process-to-data mappings. Maintain them and periodically review them for compliance.	3
3. Follow a defined process for collaborative agreements with respect to shared data and data usage within business processes.	
4. Implement data flows and full data-to-process life cycle maps for shared data for each major business process at the organizational level.	
5. Ensure that changes to shared data sets or target data sets for a specific business purpose are managed by data governance structures, with relevant stakeholder engagement.	
6. Use metrics to expand approved shared data reuse and eliminate process redundancy.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Data Operations—Data Lifecycle Management

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO14.09 Support data archiving and retention. Ensure that data maintenance satisfies organizational and regulatory requirements for availability of historical data. Ensure that legal and regulatory requirements for data archiving and retention are met.	a. Percent of unsuccessful attempts to transfer data to archive b. Percent of data maintenance that meets organizational and regulatory requirements for historical data availability and legal and regulatory requirements for data archiving and retention
Activities	**Capability Level**
1. Ensure that policies mandate management of data history, including retention, destruction and audit trail requirements.	2
2. Ensure the existence of a defined method that guarantees accessibility to the historical data necessary to support business needs.	
3. Use policy and processes to control access, transmittal and modifications to historical and archived data.	
4. Ensure that the organization has a prescribed data warehouse repository that provides access to historical data for meeting analytics needs supporting business processes.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Platform and Architecture—Historical Data, Retention and Archiving
Management Practice	**Example Metrics**
APO14.10 Manage data backup and restore arrangements. Manage availability of critical data to ensure operational continuity.	a. Percent of unsuccessful attempts to back up data b. Percent of successful attempts to restore backup data
Activities	**Capability Level**
1. Define a schedule to ensure correct backup of all critical data.	2
2. Define requirements for on-site and off-site storage of backup data, taking into account volume, capacity and retention period, in alignment with the business requirements.	
3. Establish a testing schedule for backup data. Ensure that the data can be restored correctly without drastically impacting business.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 10: Data Recovery Capability

B. Component: Organizational Structures

Key Management Practice	Chief Risk Officer	Chief Information Officer	Chief Digital Officer	Enterprise Risk Committee	Chief Information Security Officer	Data Management Function	Legal Counsel
APO14.01 Define and communicate the organization's data management strategy and roles and responsibilities.	R	A	R		R	R	
APO14.02 Define and maintain a consistent business glossary.	R	A	R		R	R	
APO14.03 Establish the processes and infrastructure for metadata management.	R	A	R		R	R	
APO14.04 Define a data quality strategy.	R	A	R		R	R	
APO14.05 Establish data profiling methodologies, processes and tools.	R	A	R		R	R	
APO14.06 Ensure a data quality assessment approach.	R	A	R		R	R	
APO14.07 Define the data cleansing approach.	R	A	R		R	R	
APO14.08 Manage the life cycle of data assets.	R	A	R	R	R	R	R
APO14.09 Support data archiving and retention.	R	A	R	R	R	R	R
APO14.10 Manage data backup and restore arrangements.	R	A	R		R	R	R

B. Component: Organizational Structures *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
APO14.01 Define and communicate the organization's data management strategy and roles and responsibilities.	APO01.06	Data classification guidelines	Data management strategy	APO03.02; APO14.10
	APO07.03	Skills and competencies matrix	Agreed roles and responsibilities for data management and data governance	Internal
	Outside COBIT	• Enterprise strategy • Data management policies and regulation	External publications and presentations about best practices at industry conferences	Internal
			Implementation plan for data management strategy	Internal
APO14.02 Define and maintain a consistent business glossary.			Business glossary	APO14.03; BAI02.01
APO14.03 Establish the processes and infrastructure for metadata management.	APO03.02	Information architecture model	Metadata documentation	APO03.02
	APO14.02	Business glossary		
APO14.04 Define a data quality strategy.	APO01.06	Data integrity procedures	Data quality strategy	APO14.05; APO14.06; APO14.07
	APO01.07	Data security and control guidelines	Data quality issue reports	Internal
	APO11.01	Quality management plans	Data quality improvement plan	Internal
APO14.05 Establish data profiling methodologies, processes and tools.	APO14.04	Data quality strategy	Data profiling methodologies, processes, practices, tools and results templates	Internal
APO14.06 Ensure a data quality assessment approach.	APO11.01	Quality management plans	Data quality assessment results	Internal
	APO14.04	Data quality strategy		
APO14.07 Define the data cleansing approach.	APO14.04	Data quality strategy	Data quality requirements	APO09.03
APO14.08 Manage the life cycle of data assets.	APO01.07	Data security and control guidelines		
	DSS04.07	Backup data		
APO14.09 Support data archiving and retention.	DSS06.05	Retention requirements	Data archive	Internal
APO14.10 Manage data backup and restore arrangements.	APO01.07	Data security and control guidelines	Backup test plan	DSS04.07
	APO14.01	Data management strategy	Backup plan	DSS04.07
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
No related guidance for this component				

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Data analysis	Skills Framework for the Information Age V6, 2015	DTAN
Data management	Skills Framework for the Information Age V6, 2015	DATM
Information assurance	Skills Framework for the Information Age V6, 2015	INAS
Information management	Skills Framework for the Information Age V6, 2015	IRMG

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Data cleansing policy	Outlines management's commitment to data cleansing. Prescribes frequency, guidelines and accountability; documents available methods, solutions and tools.	CMMI Data Management Maturity Model, 2014	Data Cleansing
Data management policy	Describes the organization's commitment to manage data assets across the data life cycle, from creation through delivery, maintenance and archiving.		
Data quality assessment policy	Describes the organization's data quality assurance assessment philosophy for ensuring the integrity of the data being used to make decisions that impact the organization. Assigns the frequency, guidelines and accountability for data quality assessment. Outlines available methods, solutions and tools.	(1) CMMI Data Management Maturity Model, 2014; (2) National Institute of Standards and Technology Special Publication 800- 53, Revision 5 (Draft), August 2017	(1) Data Quality Assessment; (2) 3.20 System and information integrity (SI-1)
Privacy policy	Documents the collection, use, disclosure and management of personal data. Personal data can be any data that may be used to identify an individual, including, but not limited to, name, address, date of birth, marital status, contact information, ID issue and expiry date, financial records, credit information, medical history, travel destination, and intent to acquire goods or services. The privacy policy defines how an enterprise collects, stores and releases personal information; how and when the client is informed of specific information that is collected and whether it is kept confidential, shared with partners, or sold to other firms or enterprises. The policy mandates compliance with relevant legislation related to data protection.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Create a culture of shared responsibility for the organization's data assets; acknowledge the potential value of data assets and ensure that roles and responsibilities are clear for governance and management of data assets.	CMMI Data Management Maturity Model, 2014	Data Governance
Create awareness around data integrity, accuracy, completeness and protection to establish a culture of data quality. Relate data quality to the enterprise's core values. Continuously communicate the impact and risk of data loss. Ensure that employees understand the true cost of failing to implement a data quality culture.	CMMI Data Management Maturity Model, 2014	Data Quality

G. Component: Services, Infrastructure and Applications
• Data modeling tools • Data repositories

4.3 Build, Acquire and Implement (BAI)

01 Managed Programs

02 Managed Requirements Definition

03 Managed Solutions Identification and Build

04 Managed Availability and Capacity

05 Managed Organizational Change

06 Managed IT Changes

07 Managed IT Change Acceptance and Transitioning

08 Managed Knowledge

09 Managed Assets

10 Managed Configuration

11 Managed Projects

Page intentionally left blank

Domain: Build, Acquire and Implement Management Objective: BAI01 — Managed Programs	Focus Area: COBIT Core Model

Description

Manage all programs from the investment portfolio in alignment with enterprise strategy and in a coordinated way, based on a standard program management approach. Initiate, plan, control, and execute programs, and monitor expected value from the program.

Purpose

Realize desired business value and reduce the risk of unexpected delays, costs and value erosion. To do so, improve communications to and involvement of business and end users, ensure the value and quality of program deliverables and follow up of projects within the programs, and maximize program contribution to the investment portfolio.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG08 Optimization of internal business process functionality • EG12 Managed digital transformation programs	• AG03 Realized benefits from I&T-enabled investments and services portfolio • AG09 Delivering programs on time, on budget and meeting requirements and quality standards

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG01	a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG03	a. Percent of I&T-enabled investments for which claimed benefits in the business case are met or exceeded b. Percent of I&T services for which expected benefits (as stated in service level agreements) are realized
EG08	a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities	AG09	a. Number of programs/projects on time and within budget b. Number of programs needing significant rework due to quality defects c. Percent of stakeholders satisfied with program/project quality
EG12	a. Number of programs on time and within budget b. Percent of stakeholders satisfied with program delivery c. Percent of business transformation programs stopped d. Percent of business transformation programs with regular reported status updates		

A. Component: Process

Management Practice	Example Metrics
BAI01.01 Maintain a standard approach for program management. Maintain a standard approach for program management that enables governance and management review, decision-making and delivery-management activities. These activities should focus consistently on business value and goals (i.e., requirements, risk, costs, schedule and quality targets).	a. Percent of successful programs based on the defined standard approach b. Percent of stakeholders satisfied with program management

Activities	Capability Level
1. Maintain and enforce a standard approach to program management, aligned to the enterprise's specific environment and with good practice based on defined process and use of appropriate technology. Ensure that the approach covers the full life cycle and disciplines to be followed, including the management of scope, resources, risk, cost, quality, time, communication, stakeholder involvement, procurement, change control, integration and benefit realization.	2
2. Put in place a program office or project management office (PMO) that maintains the standard approach for program and project management across the organization. The PMO supports all programs and projects by creating and maintaining required project documentation templates, providing training and best practices for program/project managers, tracking metrics on the use of best practices for project management, etc. In some cases the PMO may also report on program/project progress to senior management and/or stakeholders, help prioritize projects, and ensure all projects support the overall business objectives of the enterprise.	3
3. Evaluate lessons learned based on the use of the program management approach and update the approach accordingly.	4

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
BAI01.02 Initiate a program. Initiate a program to confirm expected benefits and obtain authorization to proceed. This includes agreeing on program sponsorship, confirming the program mandate through approval of the conceptual business case, appointing program board or committee members, producing the program brief, reviewing and updating the business case, developing a benefits realization plan, and obtaining approval from sponsors to proceed.	a. Percent of I&T initiatives/projects championed by business owners b. Percent of strategic initiatives with assigned accountability c. Percent of programs undertaken without approved business cases d. Percent of stakeholders approving enterprise need, scope, planned outcome and level of program risk

Activities	Capability Level
1. Agree on program sponsorship. Appoint a program board/committee with members who have strategic interest in the program, responsibility for investment decision making, will be significantly impacted by the program and will be required to enable delivery of the change.	2
2. Appoint a dedicated manager for the program, with the commensurate competencies and skills to manage the program effectively and efficiently.	
3. Confirm the program mandate with sponsors and stakeholders. Articulate the strategic objectives for the program, potential strategies for delivery, improvement and benefits that are expected, and how the program fits with other initiatives.	3
4. Develop a detailed business case for a program. Involve all key stakeholders to develop and document a complete understanding of the expected enterprise outcomes, how they will be measured, the full scope of initiatives required, the risk involved and the impact on all aspects of the enterprise. Identify and assess alternative courses of action to achieve the desired enterprise outcomes.	
5. Develop a benefits realization plan that will be managed throughout the program to ensure that planned benefits always have owners and are achieved, sustained and optimized.	
6. Prepare the initial (conceptual) program business case, providing essential decision-making information regarding purpose, contribution to business objectives, expected value created, time frames, etc. Submit it for approval.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	
Management Practice	**Example Metrics**
BAI01.03 Manage stakeholder engagement. Manage stakeholder engagement to ensure an active exchange of accurate, consistent and timely information for all relevant stakeholders. This includes planning, identifying and engaging stakeholders and managing their expectations.	a. Level of stakeholder satisfaction with involvement b. Percent of stakeholders effectively engaged

Activities	Capability Level
1. Plan how stakeholders inside and outside the enterprise will be identified, analyzed, engaged and managed through the life cycle of the projects.	3
2. Identify, engage and manage stakeholders by establishing and maintaining appropriate levels of coordination, communication and liaison to ensure that they are involved in the program.	
3. Analyze stakeholder interests and requirements.	
4. Follow a defined process for collaborative agreements with respect to shared data and data usage within business processes.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PMBOK Guide Sixth Edition, 2017	Part 1: 10. Project communications management
Management Practice	**Example Metrics**
BAI01.04 Develop and maintain the program plan. Formulate a program to lay the initial groundwork. Position it for successful execution by formalizing the scope of the work and identifying deliverables that will satisfy goals and deliver value. Maintain and update the program plan and business case throughout the full economic life cycle of the program, ensuring alignment with strategic objectives and reflecting the current status and insights gained to date.	a. Frequency of program status reviews that do not meet value criteria b. Percent of active programs undertaken without valid and updated program value maps

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Specify funding, cost, schedule and interdependencies of multiple projects.	2
2. Define and document the program plan covering all projects. Include what is needed to bring about changes to the enterprise; its purpose, mission, vision, values, culture, products and services; business processes; people skills and numbers; relationships with stakeholders, customers, suppliers and others; technology needs; and organizational restructuring required to achieve the program's expected enterprise outcomes.	3
3. Ensure that there is effective communication of program plans and progress reports among all projects and with the overall program. Ensure that any changes made to individual plans are reflected in the other enterprise program plans.	
4. Maintain the program plan to ensure that it is up to date and reflects alignment with current strategic objectives, actual progress and material changes to outcomes, benefits, costs and risk. Have the business drive the objectives and prioritize the work throughout to ensure that the program, as designed, will meet enterprise requirements. Review progress of individual projects and adjust the projects as necessary to meet scheduled milestones and releases.	
5. Throughout the program's economic life, update and maintain the business case and a benefits register to identify and define key benefits arising from undertaking the program.	
6. Prepare a program budget that reflects the full economic life cycle costs and the associated financial and nonfinancial benefits.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
BAI01.05 Launch and execute the program. Launch and execute the program to acquire and direct the resources needed to accomplish the goals and benefits of the program as defined in the program plan. In accordance with stage-gate or release review criteria, prepare for stage-gate, iteration or release reviews to report progress and make the case for funding up to the following stage-gate or release review.	a. Percent of stakeholder sign-offs for stage-gate reviews of active programs b. Number of root cause analysis for deviations from the plan and necessary remedial actions addressed
Activities	**Capability Level**
1. Plan, resource and commission the necessary projects required to achieve the program results, based on funding review and approvals at each stage-gate review.	3
2. Manage each program or project to ensure that decision making and delivery activities are focused on value by achieving benefits for the business and goals in a consistent manner, addressing risk, and achieving stakeholder requirements.	
3. Establish agreed stages of the development process (development checkpoints). At the end of each stage, facilitate formal discussions of approved criteria with the stakeholders. After successful completion of functionality, performance and quality reviews, and before finalizing stage activities, obtain formal approval and sign-off from all stakeholders and the sponsor/ business process owner.	
4. Undertake a benefits realization process throughout the program to ensure that planned benefits always have owners and are likely to be achieved, sustained and optimized. Monitor benefits delivery and report against performance targets at the stage-gate or iteration and release reviews. Perform root cause analysis for deviations from the plan and identify and address any necessary remedial actions.	4
5. Plan audits, quality reviews, phase/stage-gate reviews and reviews of realized benefits.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI01.06 Monitor, control and report on the program outcomes. Monitor and control performance against plan throughout the full economic life cycle of the investment, covering solution delivery at the program level and value/outcome at the enterprise level. Report performance to the program steering committee and the sponsors.	a. Percent of expected program benefits achieved b. Percent of programs for which performance was monitored and timely remedial action taken when required

Activities	Capability Level
1. Update operational I&T portfolios to reflect changes that result from the program in the relevant I&T service, asset or resource portfolios.	3
2. Monitor and control the performance of the overall program and the projects within the program, including contributions of the business and IT to the projects. Report in a timely, complete and accurate fashion. Reporting may include schedule, funding, functionality, user satisfaction, internal controls and acceptance of accountabilities.	4
3. Monitor and control performance against enterprise and I&T strategies and goals. Report to management on enterprise changes implemented, benefits realized against the benefits realization plan and the adequacy of the benefits realization process.	
4. Monitor and control IT services, assets and resources created or changed as a result of the program. Note implementation and in-service dates. Report to management on performance levels, sustained service delivery and contribution to value.	
5. Manage program performance against key criteria (e.g., scope, schedule, quality, benefits realization, costs, risk, velocity), identify deviations from the plan and take timely remedial action when required.	
6. Monitor individual project performance related to delivery of the expected capabilities, schedule, benefits realization, costs, risk or other metric. Identify potential impacts on program performance and take timely remedial action when required.	
7. In accordance with stage-gate, release or iteration review criteria, undertake reviews to report on the progress of the program so that management can make go/no-go or adjustment decisions and approve further funding up to the following stage-gate, release or iteration.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
BAI01.07 Manage program quality. Prepare and execute a quality management plan, processes and practices that align with quality management standards (QMS). Describe the approach to program quality and implementation. The plan should be formally reviewed and agreed on by all parties concerned and incorporated into the integrated program plan.	a. Percent of build-to-packages without errors b. Percent of program deliverables approved at each gate review

Activities	Capability Level
1. Identify assurance tasks and practices required to support the accreditation of new or modified systems during program planning, and include them in the integrated plans. Ensure that the tasks provide assurance that internal controls and security/privacy solutions meet the defined requirements.	3
2. To provide quality assurance for the program deliverables, identify ownership and responsibilities, quality review processes, success criteria and performance metrics.	
3. Define any requirements for independent validation and verification of the quality of deliverables in the plan.	4
4. Perform quality assurance and control activities in accordance with the quality management plan and QMS.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI01.08 Manage program risk. Eliminate or minimize specific risk associated with programs through a systematic process of planning, identifying, analyzing, responding to, monitoring and controlling the areas or events with the potential to cause unwanted change. Define and record any risk faced by program management.	a. Number of programs without a proper risk assessment b. Percent of programs aligned with the enterprise risk management framework
Activities	**Capability Level**
1. Establish a formal risk management approach aligned with the enterprise risk management (ERM) framework. Ensure that the approach includes identifying, analyzing, responding to, mitigating, monitoring and controlling risk.	3
2. Assign to appropriately skilled personnel the responsibility for executing the enterprise's risk management process within a program and ensuring that this is incorporated into the solution development practices. Consider allocating this role to an independent team, especially if an objective viewpoint is required or a program is considered critical.	
3. Perform the risk assessment of identifying and quantifying risk continuously throughout the program. Manage and communicate risk appropriately within the program governance structure.	
4. Identify owners for actions to avoid, accept or mitigate risk.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
BAI01.09 Close a program. Remove the program from the active investment portfolio when there is agreement that the desired value has been achieved or when it is clear it will not be achieved within the value criteria set for the program.	a. Percent of successfully closed programs that achieved desired value b. Time between program launch and detection of achievability of value
Activities	**Capability Level**
1. Bring the program to an orderly closure, including formal approval, disbanding of the program organization and supporting function, validation of deliverables, and communication of retirement.	3
2. Review and document lessons learned. Once the program is retired, remove it from the active investment portfolio. Move any resulting capabilities to an operational asset portfolio to ensure that value continues to be created and sustained.	4
3. Put accountability and processes in place to ensure that the enterprise continues to optimize value from the service, asset or resources. Additional investments may be required at some future time to ensure that this occurs.	5
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	RS.IM Improvements

B. Component: Organizational Structures

Key Management Practice	Chief Executive Officer	Chief Risk Officer	Chief Information Officer	I&T Governance Board	Business Process Owners	Steering (Programs/Projects) Committee	Program Manager	Project Management Office	Head Architect	Head Development	Head IT Operations
BAI01.01 Maintain a standard approach for program management.	A		R	R			R				
BAI01.02 Initiate a program.		R			R	A	R	R			
BAI01.03 Manage stakeholder engagement.					R	A	R	R			
BAI01.04 Develop and maintain the program plan.						A	R	R			
BAI01.05 Launch and execute the program.			R		R	A	R	R			
BAI01.06 Monitor, control and report on the program outcomes.			R			A	R	R	R	R	R
BAI01.07 Manage program quality.					R	A	R	R			
BAI01.08 Manage program risk.		R			R	A	R	R		R	
BAI01.09 Close a program.			R		R	A	R	R		R	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)

Management Practice	Inputs		Outputs	
	From	Description	Description	To
BAI01.01 Maintain a standard approach for program management.	APO03.04	• Implementation phase descriptions • Architecture governance requirements	Updated program management approaches	Internal
	APO05.04	Updated portfolios of programs, services and assets		
	APO10.04	Identified vendor delivery risk		
	EDM02.03	Requirements for stagegate reviews		
	EDM02.04	Actions to improve value delivery		

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI01.02 Initiate a program.	**From**	**Description**	**Description**	**To**
	APO03.04	• Resource requirements • Implementation phase descriptions	Program mandate and brief	APO05.02
	APO05.02	Program business case	Program concept business case	APO05.02
	APO07.03	Skills and competencies matrix	Program benefit realization plan	APO05.02; APO06.05
	BAI05.02	Common vision and goals		
BAI01.03 Manage stakeholder engagement.			Results of stakeholder engagement effectiveness assessments	Internal
			Stakeholder engagement plan	Internal
BAI01.04 Develop and maintain the program plan.	APO05.02	Selected programs with ROI milestones	Program budget and benefits register	APO05.05; APO06.05
	APO07.03	Skills and competencies matrix	Resource requirements and roles	APO07.05; APO07.06
	APO07.05	Inventory of business and IT human resources	Program plan	Internal
	BAI05.02	Implementation team and roles		
	BAI05.03	Vision communication plan		
	BAI05.04	Identified quick wins		
	BAI07.03	Approved acceptance test plan		
	BAI07.05	Approved acceptance and release for production		
BAI01.05 Launch and execute the program.	BAI05.03	Vision communications	Results of program goal achievement monitoring	APO02.04
			Results of benefit realization monitoring	APO05.05; APO06.05
			Program audit plans	MEA04.02

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI01.06 Monitor, control and report on the program outcomes.	**From**	**Description**	**Description**	**To**
	APO05.01	Investment return expectations	Stage-gate review results	APO02.04; APO05.03; EDM02.02
	APO05.02	Business case assessments	Results of program performance reviews	MEA01.03
	APO05.03	Investment portfolio performance reports		
	APO05.05	• Benefit results and related communications • Corrective actions to improve benefit realization		
	APO07.05	• Resourcing shortfall analyses • Resource utilization records		
	BAI05.04	Communication of benefits		
	BAI06.03	Change request status reports		
	BAI07.05	Evaluation of acceptance results		
	EDM02.04	Feedback on portfolio and program performance		
BAI01.07 Manage program quality.	APO11.01	Quality management plans	Quality management plan	BAI02.04; BAI03.06; BAI07.01
	APO11.02	Customer requirements for quality management	Requirements for independent verification of deliverables	BAI07.03
BAI01.08 Manage program risk.	APO12.02	Risk analysis results	Program risk register	Internal
	BAI02.03	• Requirements risk register • Risk mitigation actions	Program risk assessment results	Internal
	Outside COBIT	Enterprise risk management (ERM) framework	Program risk management plan	Internal
BAI01.09 Close a program.	BAI07.08	• Post-implementation review report • Remedial action plan	Communication of program retirement and ongoing accountabilities	APO05.04; APO07.06

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PMBOK Guide Sixth Edition, 2017	Part 1: 4. Project integration management: Inputs and Outputs; Part 1: 6. Project schedule management: Inputs and Outputs; Part 1: 10. Project communications management: Inputs and Outputs; Part 1: 11. Project risk management: Inputs and Outputs

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Benefits management	Skills Framework for the Information Age V6, 2015	BENM
Business plan development	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.3. Business Plan Development
Program management	Skills Framework for the Information Age V6, 2015	PGMG
Project and portfolio management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.2. Project and Portfolio Management

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Program/project management policy	Guides management of risk related to programs and projects. Details management position and expectation regarding program and project management. Treats accountability, goals and objectives regarding performance, budget, risk analysis, reporting and mitigation of adverse events during program/project execution.	PMBOK Guide Sixth edition, 2017	Part 1: 2.3.1 Processes, policies and procedures

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Ensure the organization understands and supports the value of enterprisewide program management. Establish an enterprisewide culture that supports consistent implementation of program management, taking into account organizational structure and business environment. Ensure the program office has a central view of all programs in the enterprise portfolio.		

G. Component: Services, Infrastructure and Applications
Program management tool

Page intentionally left blank

Domain: Build, Acquire and Implement Management Objective: BAI02 — Managed Requirements Definition	Focus Area: COBIT Core Model

Description

Identify solutions and analyze requirements before acquisition or creation to ensure that they align with enterprise strategic requirements covering business processes, applications, information/data, infrastructure and services. Coordinate the review of feasible options with affected stakeholders, including relative costs and benefits, risk analysis, and approval of requirements and proposed solutions.

Purpose

Create optimal solutions that meet enterprise needs while minimizing risk.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG08 Optimization of internal business process functionality • EG12 Managed digital transformation programs	• AG05 Delivery of I&T services in line with business requirements • AG06 Agility to turn business requirements into operational solutions • AG09 Delivering programs on time, on budget and meeting requirements and quality standards

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG01	a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG05	a. Percent of business stakeholders satisfied that I&T service delivery meets agreed service levels b. Number of business disruptions due to I&T service incidents c. Percent of users satisfied with the quality of I&T service delivery
EG08	a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities	AG06	a. Level of satisfaction of business executives with I&T responsiveness to new requirements b. Average time to market for new I&T-related services and applications c. Average time to turn strategic I&T objectives into agreed and approved initiatives d. Number of critical business processes supported by up-to-date infrastructure and applications
EG12	a. Number of programs on time and within budget b. Percent of stakeholders satisfied with program delivery c. Percent of business transformation programs stopped d. Percent of business transformation programs with regular reported status updates	AG09	a. Number of programs/projects on time and within budget b. Number of programs needing significant rework due to quality defects c. Percent of stakeholders satisfied with program/project quality

A. Component: Process	
Management Practice	**Example Metrics**
BAI02.01 Define and maintain business functional and technical requirements. Based on the business case, identify, prioritize, specify and agree on business information, functional, technical and control requirements covering the scope/understanding of all initiatives required to achieve the expected outcomes of the proposed I&T-enabled business solution.	a. Percent of requirements reworked due to misalignment with enterprise needs and expectations b. Percent of requirements validated through approaches such as peer review, model validation or operational prototyping

Activities	Capability Level
1. Ensure that all stakeholder requirements, including relevant acceptance criteria, are considered, captured, prioritized and recorded in a way that is understandable to all stakeholders, recognizing that the requirements may change and will become more detailed as they are implemented.	2
2. Express business requirements in terms of how the gap between current and desired business capabilities need to be addressed and how the user (employee, client, etc.) will interact with and use the solution.	
3. Specify and prioritize information, functional and technical requirements, based on the user experience design and confirmed stakeholder requirements.	
4. Ensure requirements meet enterprise policies and standards, enterprise architecture, strategic and tactical I&T plans, in-house and outsourced business and IT processes, security requirements, regulatory requirements, people competencies, organizational structure, business case, and enabling technology.	3
5. Include information control requirements in the business processes, automated processes and I&T environments to address information risk and to comply with laws, regulations and commercial contracts.	
6. Confirm acceptance of key aspects of the requirements, including enterprise rules, user experience, information controls, business continuity, legal and regulatory compliance, auditability, ergonomics, operability and usability, safety, confidentiality, and supporting documentation.	
7. Track and control scope, requirements and changes through the life cycle of the solution as understanding of the solution evolves.	
8. Define and implement a requirements definition and maintenance procedure and a requirements repository that are appropriate for the size, complexity, objectives and risk of the initiative that the enterprise is considering undertaking.	
9. Validate all requirements through approaches such as peer review, model validation or operational prototyping.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISF, The Standard of Good Practice for Information Security 2016	SD2.1 Specifications of Requirements
ISO/IEC 27002:2013/Cor.2:2015(E)	14.1 Security requirements of information systems
ITIL V3, 2011	Service Design, 5.1 Requirements engineering
PMBOK Guide Sixth Edition, 2017	Part 1: 5. Project scope management

Management Practice	Example Metrics
BAI02.02 Perform a feasibility study and formulate alternative solutions. Perform a feasibility study of potential alternative solutions, assess their viability and select the preferred option. If appropriate, implement the selected option as a pilot to determine possible improvements.	a. Percent of business case objectives met by proposed solution b. Percent of requirements satisfied by proposed solution

Activities	Capability Level
1. Identify required actions for solution acquisition or development based on the enterprise architecture. Take into account scope and/or time and/or budget limitations.	2
2. Review the alternative solutions with all stakeholders. Select the most appropriate one based on feasibility criteria, including risk and cost.	
3. Translate the preferred course of action into a high-level acquisition/development plan that identifies resources to be used and stages requiring a go/no-go decision.	3
4. Define and execute a feasibility study, pilot or basic working solution that clearly and concisely describes the alternative solutions and measures how these would satisfy the business and functional requirements. Include an evaluation of their technological and economic feasibility.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI02.03 Manage requirements risk. Identify, document, prioritize and mitigate functional, technical and information processing-related risk associated with the enterprise requirements, assumptions and proposed solution.	a. Percent of requirements risk not covered by an appropriate risk response b. Level of detail of documented requirements risk c. Completeness of estimated probability and impact of listed requirements risk and risk responses

Activities	Capability Level
1. Identify quality, functional and technical requirements risk (due to, for example, lack of user involvement, unrealistic expectations, developers adding unnecessary functionality, unrealistic assumptions, etc.).	3
2. Determine appropriate risk response to requirements risk.	
3. Analyze the identified risk by estimating probability and impact on budget and schedule. Evaluate budgetary impact of appropriate risk response actions.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
BAI02.04 Obtain approval of requirements and solutions. Coordinate feedback from affected stakeholders. At predetermined key stages, obtain approval and sign-off from the business sponsor or product owner regarding functional and technical requirements, feasibility studies, risk analyses and recommended solutions.	a. Level of stakeholder satisfaction with requirements b. Number of solution exceptions to design noted during stage reviews c. Percent of stakeholders not approving solution in relation to business case

Activities	Capability Level
1. Ensure that the business sponsor or product owner makes the final choice of solution, acquisition approach and high-level design, according to the business case. Obtain necessary approvals from affected stakeholders (e.g., business process owner, enterprise architect, operations manager, security, privacy officer).	3
2. Obtain quality reviews throughout, and at the end of, each key project stage, iteration or release. Assess the results against the original acceptance criteria. Have business sponsors and other stakeholders sign off on each successful quality review.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

B. Component: Organizational Structures														
Key Management Practice	**Chief Risk Officer**	**Chief Information Officer**	**Business Process Owners**	**Steering (Programs/Projects) Committee**	**Program Manager**	**Project Manager**	**Project Management Office**	**Relationship Manager**	**Head Architect**	**Head Development**	**Head IT Operations**	**Information Security Manager**	**Privacy Officer**
BAI02.01 Define and maintain business functional and technical requirements.			R	A	R	R	R	R	R	R		R	R
BAI02.02 Perform a feasibility study and formulate alternative solutions.			R	A	R	R	R			R			
BAI02.03 Manage requirements risk.	R	R	R	A	R	R	R			R	R	R	R
BAI02.04 Obtain approval of requirements and solutions.			R	A	R	R	R					R	R

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
BAI02.01 Define and maintain business functional and technical requirements.	**From**	**Description**	**Description**	**To**
	APO01.07	• Data classification guidelines • Data security and control guidelines • Data integrity procedures	Requirements definition repository	BAI03.01; BAI03.02; BAI03.12; BAI04.01; BAI05.01
	APO03.01	Architecture principles	Confirmed acceptance criteria from stakeholders	BAI03.01; BAI03.02; BAI03.12; BAI04.03; BAI05.01; BAI05.02
	APO03.02	• Baseline domain descriptions and architecture definition • Information architecture model	Record of requirement change requests	BAI03.09
	APO03.05	Solution development guidance		
	APO10.02	Vendor requests for information (RFIs) and requests for proposals (RFPs)		
	APO11.02	Acceptance criteria		
	APO14.02	Business glossary		
BAI02.02 Perform a feasibility study and formulate alternative solutions.	APO03.05	Solution development guidance	High-level acquisition/ development plan	APO10.02; BAI03.01
	APO10.01	Vendor catalog	Feasibility study report	BAI03.02; BAI03.03; BAI03.12
	APO10.02	• Vendor requests for information (RFIs) and requests for proposals (RFPs) • RFI and RFP evaluations • Decision results of vendor evaluations		
	APO11.02	Acceptance criteria		
BAI02.03 Manage requirements risk.			Requirements risk register	BAI01.08; BAI03.02; BAI04.01; BAI05.01; BAI11.06
			Risk mitigation actions	BAI01.08; BAI03.02; BAI05.01
BAI02.04 Obtain approval of requirements and solutions.	BAI01.07	Quality management plan	Approved quality reviews	APO11.03
	BAI11.05	Project quality management plan	Sponsor approvals of requirements and proposed solutions	BAI03.02; BAI03.03; BAI03.04

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PMBOK Guide Sixth Edition, 2017	Part 1: 5. Project management scope: Inputs and Outputs

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Application design	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.6. Application Design
Business analysis	Skills Framework for the Information Age V6, 2015	BUAN
Business process improvement	Skills Framework for the Information Age V6, 2015	BPRE
Needs identification	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	D. Enable—D.11. Needs Identification
Requirements definition and management	Skills Framework for the Information Age V6, 2015	REQM
User experience analysis	Skills Framework for the Information Age V6, 2015	UNAN

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Software development policy	Standardizes software development across the organization by listing all protocols and standards to be followed.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Establish a culture that ensures consistent and robust processes for defining requirements. Ensure that the processes clearly align development requirements with enterprise strategic requirements.		

G. Component: Services, Infrastructure and Applications
Requirements definition and documentation tools

Page intentionally left blank

Domain: Build, Acquire and Implement Management Objective: BAI03 — Managed Solutions Identification and Build	Focus Area: COBIT Core Model

Description

Establish and maintain identified products and services (technology, business processes and workflows) in line with enterprise requirements covering design, development, procurement/sourcing and partnering with vendors. Manage configuration, test preparation, testing, requirements management and maintenance of business processes, applications, information/data, infrastructure and services.

Purpose

Ensure agile and scalable delivery of digital products and services. Establish timely and cost-effective solutions (technology, business processes and workflows) capable of supporting enterprise strategic and operational objectives.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG08 Optimization of internal business process functionality • EG12 Managed digital transformation programs	• AG05 Delivery of I&T services in line with business requirements • AG06 Agility to turn business requirements into operational solutions • AG09 Delivering programs on time, on budget and meeting requirements and quality standards

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG01	a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG05	a. Percent of business stakeholders satisfied that I&T service delivery meets agreed service levels b. Number of business disruptions due to I&T service incidents c. Percent of users satisfied with the quality of I&T service delivery
EG08	a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities	AG06	a. Level of satisfaction of business executives with I&T responsiveness to new requirements b. Average time to market for new I&T-related services and applications c. Average time to turn strategic I&T objectives into agreed and approved initiatives d. Number of critical business processes supported by up-to-date infrastructure and applications
EG12	a. Number of programs on time and within budget b. Percent of stakeholders satisfied with program delivery c. Percent of business transformation programs stopped d. Percent of business transformation programs with regular reported status updates	AG09	a. Number of programs/projects on time and within budget b. Number of programs needing significant rework due to quality defects c. Percent of stakeholders satisfied with program/project quality

A. Component: Process

Management Practice	Example Metrics
BAI03.01 Design high-level solutions. Develop and document high-level designs for the solution in terms of technology, business processes and workflows. Use agreed and appropriate phased or rapid Agile development techniques. Ensure alignment with the I&T strategy and enterprise architecture. Reassess and update the designs when significant issues occur during detailed design or building phases, or as the solution evolves. Apply a user-centric approach; ensure that stakeholders actively participate in the design and approve each version.	a. Number of design review deficiencies b. Percent of stakeholder participation in the design and approval signoff of each version

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Establish a high-level design specification that translates the proposed solution into a high-level design for business processes, supporting services, workflows, applications, infrastructure, and information repositories capable of meeting business and enterprise architecture requirements.	2
2. Involve appropriately qualified and experienced user experience designers and IT specialists in the design process to make sure that the design provides a solution that optimally uses the proposed I&T capabilities to enhance the business process.	
3. Create a design that complies with the organization's design standards. Ensure that it maintains a level of detail that is appropriate for the solution and development method and consistent with business, enterprise and I&T strategies, the enterprise architecture, security/privacy plan and applicable laws, regulations and contracts.	
4. After quality assurance approval, submit the final high-level design to the project stakeholders and the sponsor/business process owner for approval based on agreed criteria. This design will evolve throughout the project as understanding grows.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	SD2.2 System Design
Management Practice	**Example Metrics**
BAI03.02 Design detailed solution components. Develop, document and elaborate detailed designs progressively. Use agreed and appropriate phased or rapid Agile development techniques, addressing all components (business processes and related automated and manual controls, supporting I&T applications, infrastructure services and technology products, and partners/suppliers). Ensure that the detailed design includes internal and external service level agreements (SLAs) and operational level agreements (OLAs).	a. Number of design review deficiencies b. Number of in-process design changes
Activities	**Capability Level**
1. Design progressively the business process activities and work flows that need to be performed in conjunction with the new application system to meet the enterprise objectives, including the design of the manual control activities.	2
2. Design the application processing steps. These steps include specification of transaction types and business processing rules, automated controls, data definitions/business objects, use cases, external interfaces, design constraints, and other requirements (e.g., licensing, legal, standards and internationalization/localization).	
3. Classify data inputs and outputs according to enterprise architecture standards. Specify the source data collection design. Document the data inputs (regardless of source) and validation for processing transactions as well as the methods for validation. Design the identified outputs, including data sources.	
4. Design the system/solution interface, including any automated data exchange.	
5. Design data storage, location, retrieval and recoverability.	
6. Design appropriate redundancy, recovery and backup.	
7. Design the interface between the user and the system application so that it is easy to use and self-documenting.	3
8. Consider the impact of the solution's need for infrastructure performance, being sensitive to the number of computing assets, bandwidth intensity and time sensitivity of the information.	
9. Proactively evaluate for design weaknesses (e.g., inconsistencies, lack of clarity, potential flaws) throughout the life cycle. Identify improvements when required.	
10. Provide an ability to audit transactions and identify root causes of processing errors.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	SD2.2 System Design

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI03.03 Develop solution components. Develop solution components progressively in a separate environment, in accordance with detailed designs following standards and requirements for development and documentation, quality assurance (QA), and approval. Ensure that all control requirements in the business processes, supporting I&T applications and infrastructure services, services and technology products, and partner/vendor services are addressed.	a. Number of solution exceptions to design noted during stage reviews b. Number of detailed designs for business processes, supporting services, applications and infrastructure, and information repositories

Activities	Capability Level
1. Within a separate environment, develop the proposed detailed design for business processes, supporting services, applications, infrastructure and information repositories.	2
2. When third-party providers are involved with the solution development, ensure that maintenance, support, development standards and licensing are addressed and adhered to in contractual obligations.	
3. Track change requests and design, performance and quality reviews. Ensure active participation of all impacted stakeholders.	
4. Document all solution components according to defined standards. Maintain version control over all developed components and associated documentation.	
5. Assess the impact of solution customization and configuration on the performance and efficiency of acquired solutions and on interoperability with existing applications, operating systems and other infrastructure. Adapt business processes as required to leverage the application capability.	3
6. Ensure that responsibilities for using high-security or restricted-access infrastructure components are clearly defined and understood by those who develop and integrate infrastructure components. Their use should be monitored and evaluated.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISF, The Standard of Good Practice for Information Security 2016	SD1.2 System Development Environments
ISO/IEC 27002:2013/Cor.2:2015(E)	14.2 Security in development and support processes
ITIL V3, 2011	Service Strategy, 5.5 IT service strategy and application development
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.18 System and services acquisition (SA-3)

Management Practice	Example Metrics
BAI03.04 Procure solution components. Procure solution components, based on the acquisition plan, in accordance with requirements and detailed designs, architecture principles and standards, and the enterprise's overall procurement and contract procedures, QA requirements, and approval standards. Ensure that all legal and contractual requirements are identified and addressed by the vendor.	a. Percent of suppliers certified b. Percent of suppliers engaged in collaborative design

Activities	Capability Level
1. Create and maintain a plan for the acquisition of solution components. Consider future flexibility for capacity additions, transition costs, risk and upgrades over the lifetime of the project.	3
2. Review and approve all acquisition plans. Consider risk, costs, benefits and technical conformance with enterprise architecture standards.	
3. Assess and document the degree to which acquired solutions require adaptation of business process to leverage the benefits of the acquired solution.	
4. Follow required approvals at key decision points during the procurement processes.	
5. Record receipt of all infrastructure and software acquisitions in an asset inventory.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISF, The Standard of Good Practice for Information Security 2016	SD2.3 Software Acquisition
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	3.4 Buying Decisions
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.18 System and services acquisition (SA-4)

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI03.05 Build solutions. Install and configure solutions and integrate with business process activities. During configuration and integration of hardware and infrastructure software, implement control, security, privacy and auditability measures to protect resources and ensure availability and data integrity. Update the product or services catalogue to reflect the new solutions.	a. Gap between estimated and final development effort b. Number of software problems reported c. Number of review errors

Activities	Capability Level
1. Integrate and configure business and IT solution components and information repositories in line with detailed specifications and quality requirements. Consider the role of users, business stakeholders and the process owner in the configuration of business processes.	2
2. Complete and update business process and operational manuals, where necessary, to account for any customization or special conditions unique to the implementation.	
3. Consider all relevant information control requirements in solution component integration and configuration. Include implementation of business controls, where appropriate, into automated application controls such that processing is accurate, complete, timely, authorized and auditable.	
4. Implement audit trails during configuration and integration of hardware and infrastructural software to protect resources and ensure availability and integrity.	3
5. Consider when the effect of cumulative customizations and configurations (including minor changes that were not subjected to formal design specifications) requires a high-level reassessment of the solution and associated functionality.	
6. Configure acquired application software to meet business processing requirements.	
7. Define product and service catalogues for relevant internal and external target groups, based on business requirements.	
8. Ensure the interoperability of solution components with supporting tests, preferably automated.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
HITRUST CSF version 9, September 2017	10.05 Security in Development & Support Processes
ISF, The Standard of Good Practice for Information Security 2016	SD2.4 System Build

Management Practice	Example Metrics
BAI03.06 Perform quality assurance (QA). Develop, resource and execute a QA plan aligned with the QMS to obtain the quality specified in the requirements definition and in the enterprise's quality policies and procedures.	a. Number of reworked solution designs due to misalignment with requirements b. Number and robustness of documented monitor activities performed

Activities	Capability Level
1. Define a QA plan and practices include, for example, specification of quality criteria, validation and verification processes, definition of how quality will be reviewed, necessary qualifications of quality reviewers, and roles and responsibilities for the achievement of quality.	3
2. Frequently monitor the solution quality based on project requirements, enterprise policies, adherence to development methodologies, quality management procedures and acceptance criteria.	4
3. Employ, as appropriate, code inspection, test-driven development practices, automated testing, continuous integration, walk-throughs and testing of applications. Report on outcomes of the monitoring process and testing to the application software development team and IT management.	
4. Monitor all quality exceptions and address all corrective actions. Maintain a record of all reviews, results, exceptions and corrections. Repeat quality reviews, where appropriate, based on the amount of rework and corrective action.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISF, The Standard of Good Practice for Information Security 2016	SD1.3 Quality Assurance

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI03.07 Prepare for solution testing. Establish a test plan and required environments to test the individual and integrated solution components. Include the business processes and supporting services, applications and infrastructure.	a. Number of business users involved in creating a test plan b. Number and robustness of use cases created for testing

Activities	Capability Level
1. Create an integrated test plan and practices commensurate with the enterprise environment and strategic technology plans. Ensure that the integrated test plan and practices will enable the creation of suitable testing and simulation environments to help verify that the solution will operate successfully in the live environment and deliver the intended results and that controls are adequate.	2
2. Create a test environment that supports the full scope of the solution. Ensure that the test environment reflects, as closely as possible, real-world conditions, including the business processes and procedures, range of users, transaction types, and deployment conditions.	
3. Create test procedures that align with the plan and practices and allow evaluation of the operation of the solution in real-world conditions. Ensure that the test procedures evaluate the adequacy of the controls, based on enterprisewide standards that define roles, responsibilities and testing criteria, and are approved by project stakeholders and the sponsor/business process owner.	3
4. Document and save the test procedures, cases, controls and parameters for future testing of the application.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	AD.DE Safeguard Development Environment
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.10 Maintenance (MA-2, MA-3)

Management Practice	Example Metrics
BAI03.08 Execute solution testing. During development, execute testing continually (including control testing), in accordance with the defined test plan and development practices in the appropriate environment. Engage business process owners and end users in the test team. Identify, log and prioritize errors and issues identified during testing.	a. Number of errors found during testing b. Time and effort to complete tests

Activities	Capability Level
1. Undertake testing of solutions and their components in accordance with the testing plan. Include testers independent from the solution team, with representative business process owners and end users. Ensure that testing is conducted only within the development and test environments.	2
2. Use clearly defined test instructions, as defined in the test plan. Consider the appropriate balance between automated scripted tests and interactive user testing.	
3. Undertake all tests in accordance with the test plan and practices. Include the integration of business processes and IT solution components and of nonfunctional requirements (e.g., security, privacy, interoperability, usability).	
4. Identify, log and classify (e.g., minor, significant and mission-critical) errors during testing. Repeat tests until all significant errors have been resolved. Ensure that an audit trail of test results is maintained.	
5. Record testing outcomes and communicate results of testing to stakeholders in accordance with the test plan.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	
CMMI Cybermaturity Platform, 2018	AD.ST Secure Development Testing
ISF, The Standard of Good Practice for Information Security 2016	SD2.5 System Testing; SD2.6 Security Testing
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.18 System and services acquisition (SA-11)

A. Component: Process *(cont.)*		
Management Practice	**Example Metrics**	
BAI03.09 Manage changes to requirements. Track the status of individual requirements (including all rejected requirements) throughout the project life cycle. Manage the approval of changes to requirements.	a. Number of tracked, approved changes that generate new errors b. Percent of stakeholders satisfied with change management processes	
Activities		**Capability Level**
1. Assess the impact of all solution change requests on the solution development, the original business case and the budget. Categorize and prioritize them accordingly.		3
2. Track changes to requirements, enabling all stakeholders to monitor, review and approve the changes. Ensure that the outcomes of the change process are fully understood and agreed on by all the stakeholders and the sponsor/business process owner.		
3. Apply change requests, maintaining the integrity of integration and configuration of solution components. Assess the impact of any major solution upgrade and classify it according to agreed objective criteria (such as enterprise requirements), based on the outcome of analysis of the risk involved (such as impact on existing systems and processes or security/privacy), cost-benefit justification and other requirements.		
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
ISF, The Standard of Good Practice for Information Security 2016	SD2.9 Post-implementation Review	
Management Practice	**Example Metrics**	
BAI03.10 Maintain solutions. Develop and execute a plan for the maintenance of solution and infrastructure components. Include periodic reviews against business needs and operational requirements.	a. Number of demands for maintenance that are not satisfied b. Duration of demands for maintenance that are satisfied and that go unsatisfied	
Activities		**Capability Level**
1. Develop and execute a plan for the maintenance of solution components. Include periodic reviews against business needs and operational requirements such as patch management, upgrade strategies, risk, privacy, vulnerabilities assessment and security requirements.		2
2. Assess the significance of a proposed maintenance activity on current solution design, functionality and/or business processes. Consider risk, user impact and resource availability. Ensure that business process owners understand the effect of designating changes as maintenance.		3
3. In the event of major changes to existing solutions that result in significant change in current designs and/or functionality and/or business processes, follow the development process used for new systems. For maintenance updates, use the change management process.		
4. Ensure that the pattern and volume of maintenance activities are analyzed periodically for abnormal trends that indicate underlying quality or performance problems, cost/benefit of major upgrade, or replacement in lieu of maintenance.		4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
ISO/IEC 27002:2013/Cor.2:2015(E)	14.3 Test data	
Management Practice	**Example Metrics**	
BAI03.11 Define IT products and services and maintain the service portfolio. Define and agree on new or changed IT products or services and service level options. Document new or changed product and service definitions and service level options to be updated in the products and services portfolio.	a. Percent of stakeholders signing off on new I&T services b. Percent of new or changed service definitions and service level options documented in the services portfolio. c. Percent of new or changed service definitions and service level options updated in the services portfolio	

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Propose definitions of the new or changed IT products and services to ensure that they are fit for purpose. Document the proposed definitions in the portfolio list of products and services to be developed.	3
2. Propose new or changed service level options (service times, user satisfaction, availability, performance, capacity, security, privacy, continuity, compliance and usability) to ensure that the IT products and services are fit for use. Document the proposed service options in the portfolio.	
3. Interface with business relationship management and portfolio management to agree on the proposed product and service definitions and service level options.	
4. If product or service change falls within agreed approval authority, build the new or changed IT products and services or service level options. Otherwise, pass the change to portfolio management for investment review.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
BAI03.12 Design solutions based on the defined development methodology. Design, develop and implement solutions with the appropriate development methodology (i.e., waterfall, Agile or bimodal I&T), in accordance with the overall strategy and requirements.	a. Percent of solution development projects that apply selected development methodologies b. Percent of processes adapted to the chosen strategy
Activities	**Capability Level**
1. Analyze and assess the impact of choosing a development methodology (i.e., waterfall, Agile, bimodal) on the available resources, architecture requirements, configuration settings and system rigidity.	3
2. Establish the appropriate development methodology and organizational approach that delivers the proposed solution efficiently and effectively and that is capable of meeting business, architecture and system requirements. Adapt processes as required to the chosen strategy.	
3. Establish the needed project teams as defined by the chosen development methodology. Provide sufficient training.	
4. Consider applying a dual system, if required, in which cross-functional groups (digital factories) focus on developing one product or process using a different technology, operational, or managerial methodology from the rest of the company. Embedding these groups in business units has the advantage of spreading the new culture of agile development and making this digital factory approach the norm.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	SD1.1 System Development Methodology

B. Component: Organizational Structures																				
Key Management Practice	**Chief Information Officer**	**Chief Technology Officer**	**Chief Digital Officer**	**Business Process Owners**	**Portfolio Manager**	**Steering (Programs/Projects) Committee**	**Program Manager**	**Project Manager**	**Project Management Office**	**Relationship Manager**	**Head Architect**	**Head Development**	**Head IT Operations**	**Head IT Administration**	**Service Manager**	**Information Security Manager**	**Business Continuity Manager**	**Privacy Officer**
BAI03.01 Design high-level solutions.		R		R		A	R	R	R	R		R				R		
BAI03.02 Design detailed solution components.		R		R		A	R	R	R			R						
BAI03.03 Develop solution components.		R		R		A	R	R	R			R						
BAI03.04 Procure solution components.		R		R		A						R	R	R				
BAI03.05 Build solutions.		R		R		A	R	R	R			R				R		
BAI03.06 Perform quality assurance (QA).		R		R		A	R	R	R			R						
BAI03.07 Prepare for solution testing.		R		R		A						R	R		R	R	R	R
BAI03.08 Execute solution testing.		R		R		A						R	R			R		R
BAI03.09 Manage changes to requirements.		R		R		A	R	R	R		R	R				R		R
BAI03.10 Maintain solutions.	A	R		R			R	R	R			R				R		R
BAI03.11 Define IT products and services and maintain the service portfolio.	A														R	R		R
BAI03.12 Design solutions based on the defined development methodology.	A		R		R		R	R										

Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
BAI03.01 Design high-level solutions.	**From**	**Description**	**Description**	**To**
	APO03.01	Architecture principles	Approved high-level design specification	BAI04.03; BAI05.01
	APO03.02	Baseline domain descriptions and architecture definition		
	APO04.03	Research analyses of innovation possibilities		
	APO04.04	Evaluations of innovation ideas		
	BAI02.01	• Requirements definition repository • Confirmed acceptance criteria from stakeholders		
	BAI02.02	High-level acquisition/ development plan		
BAI03.02 Design detailed solution components.	APO03.01	Architecture principles	Internal and external SLAs	BAI04.02
	APO03.02	• Baseline domain descriptions and architecture definition • Information architecture model	Approved detailed design specification	BAI04.03; BAI05.01
	APO03.05	Solution development guidance		
	APO04.06	Assessments of innovative approaches		
	BAI02.01	• Requirements definition repository • Confirmed acceptance criteria from stakeholders		
	BAI02.02	Feasibility study report		
	BAI02.03	• Requirements risk register • Risk mitigation actions		
	BAI02.04	Approvals of requirements and proposed solutions by sponsor		
BAI03.03 Develop solution components.	BAI02.02	Feasibility study report	Documented solution components	BAI04.03; BAI05.05; BAI08.02; BAI08.03
	BAI02.04	Approvals of requirements and proposed solutions by sponsor		

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI03.04 Procure solution components.	**From**	**Description**	**Description**	**To**
	BAI02.04	Approvals of requirements and proposed solutions by sponsor	Approved acquisition plan	APO10.03
			Updates to asset inventory	BAI09.01
BAI03.05 Build solutions.			Integrated and configured solution components	BAI06.01
BAI03.06 Perform quality assurance (QA).	APO11.01	Results of QMS effectiveness reviews	Quality review results, exceptions and corrections	APO11.04
	BAI01.07	Quality management plan	Quality assurance plan	APO11.04
	BAI11.05	Project quality management plan		
BAI03.07 Prepare for solution testing.			Test procedures	BAI07.03
			Test plan	BAI07.03
BAI03.08 Execute solution testing.	APO04.05	Analysis of rejected initiatives	Test result communications	BAI07.03
			Test result logs and audit trails	BAI07.03
BAI03.09 Manage changes to requirements.	APO04.05	Results and recommendations from proof-of-concept initiatives	Record of all approved and applied change requests	BAI06.03
	BAI02.01	Record of requirement change requests		
BAI03.10 Maintain solutions.			Maintenance plan	APO08.05
			Updated solution components and related documentation	BAI05.05
BAI03.11 Define IT products and services and maintain the service portfolio.	APO02.04	• Gaps and changes required to realize target capability • Value benefit statement for target environment	Updated service portfolio	APO05.04
	APO06.02	Budget allocations	Service definitions	EDM02.01; DSS01.03
	APO06.03	• I&T budget • Budget communications		
	APO08.05	Definition of potential improvement projects		
	BAI10.02	Configuration baseline		
	BAI10.03	Approved changes to baseline		
	BAI10.04	Configuration status reports		
	EDM04.01	Guiding principles for allocating resources and capabilities		

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI03.12 Design solutions based on the defined development methodology.	**From**	**Description**	**Description**	**To**
	APO03.02	Baseline domain descriptions and architecture definition		
	APO03.05	Solution development guidance		
	APO07.03	Skills and competencies matrix		
	BAI02.01	• Confirmed acceptance criteria from stakeholders • Requirements definition repository		
	BAI02.02	Feasibility study report		
	BAI10.02	Configuration baseline		
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
No related guidance for this component				

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Application development	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	B. Build—B.1. Application Development
Business process testing	Skills Framework for the Information Age V6, 2015	BPTS
Component integration	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	B. Build—B.2. Component Integration
Database design	Skills Framework for the Information Age V6, 2015	DBDS
Documentation production	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	B. Build—B.5. Documentation Production
Hardware design	Skills Framework for the Information Age V6, 2015	HWDE
Porting/software configuration	Skills Framework for the Information Age V6, 2015	PORT
Programming/software development	Skills Framework for the Information Age V6, 2015	PROG
Release and deployment	Skills Framework for the Information Age V6, 2015	RELM
Solution architecture	Skills Framework for the Information Age V6, 2015	ARCH
Solution deployment	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	B. Build—B.4. Solution Deployment
Systems design	Skills Framework for the Information Age V6, 2015	DESN
Systems development management	Skills Framework for the Information Age V6, 2015	DLMG
Systems engineering	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	B. Build—B.6. Systems Engineering

D. Component: People, Skills and Competencies *(cont.)*		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Systems installation/ decommissioning	Skills Framework for the Information Age V6, 2015	HSIN
Systems integration	Skills Framework for the Information Age V6, 2015	SINT
Testing	Skills Framework for the Information Age V6, 2015	TEST
Testing	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	B. Build—B.3. Testing
User experience design	Skills Framework for the Information Age V6, 2015	HCEV

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Maintenance policy	Defines proper support of software and hardware components to ensure longer asset life, increase employee productivity and maintain an acceptable user experience.	National Institute of Standards and Technology Special Publication 800- 53, Revision 5 (Draft), August 2017	3.10 Maintenance (MA-1)
Software development policy	Standardizes software development across the organization by listing all protocols and standards to be followed.		
System and service acquisition policy	Provides procedures to assess, review and validate requirements for acquisition of system and services.	National Institute of Standards and Technology Special Publication 800- 53, Revision 5 (Draft), August 2017	3.18 System and services acquisition (SA-1)

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Ensure agile and scalable delivery of digital services; engage an ecosystem of partners with whom the organization can work or set up a bimodal IT structure with digital factories, agile leaders and teams, continuous flow, and a mindset toward improvement.		
Establish an open, unbiased culture that fairly and objectively evaluates alternatives when investigating potential new solutions (including whether to build or buy).		

G. Component: Services, Infrastructure and Applications
• Digital factory services, separating “fast IT” (the digital factory responsible for developing digital applications) from legacy core IT • Solution evaluation and selection services • Testing tools and services

Domain: Build, Acquire and Implement Management Objective: BAI04 — Managed Availability and Capacity	Focus Area: COBIT Core Model

Description

Balance current and future needs for availability, performance and capacity with cost-effective service provision. Include assessment of current capabilities, forecasting of future needs based on business requirements, analysis of business impacts, and assessment of risk to plan and implement actions to meet the identified requirements.

Purpose

Maintain service availability, efficient management of resources and optimization of system performance through prediction of future performance and capacity requirements.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG08 Optimization of internal business process functionality	AG05 Delivery of I&T services in line with business requirements
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG01 a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG05 a. Percent of business stakeholders satisfied that I&T service delivery meets agreed service levels b. Number of business disruptions due to I&T service incidents c. Percent of users satisfied with the quality of I&T service delivery
EG08 a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities	

A. Component: Process

Management Practice	Example Metrics
BAI04.01 Assess current availability, performance and capacity and create a baseline. Assess availability, performance and capacity of services and resources to ensure that cost-justifiable capacity and performance are available to support business needs and deliver against service level agreements (SLAs). Create availability, performance and capacity baselines for future comparison.	a. Percent of actual capacity usage b. Percent of actual availability c. Percent of actual performance

Activities	Capability Level
1. Consider the following (current and forecasted) in the assessment of availability, performance and capacity of services and resources: customer requirements, business priorities, business objectives, budget impact, resource utilization, IT capabilities and industry trends.	2
2. Identify and follow up on all incidents caused by inadequate performance or capacity.	3
3. Monitor actual performance and capacity usage against defined thresholds, supported, where necessary, with automated software.	4
4. Regularly evaluate the current levels of performance for all processing levels (business demand, service capacity and resource capacity) by comparing them against trends and SLAs. Take into account changes in the environment.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	DP.CP Capacity Planning
ISF, The Standard of Good Practice for Information Security 2016	SY2.2 Performance and Capacity Management
ISO/IEC 20000-1:2011(E)	6.5 Capacity management
ITIL V3, 2011	Service Design, 4.4 Availability Management; 4.5 Capacity Management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.14 Planning (PL-10, PL-11)

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI04.02 Assess business impact. Identify important services to the enterprise. Map services and resources to business processes and identify business dependencies. Ensure that the impact of unavailable resources is fully agreed on and accepted by the customer. For vital business functions, ensure that availability requirements can be satisfied per service level agreement (SLA).	a. Number of scenarios created to assess future availability situations b. Percent of business process owners signing off on analysis results

Activities	Capability Level
1. Identify only those solutions or services that are critical in the availability and capacity management process.	2
2. Map the selected solutions or services to the application(s) and infrastructure (IT and facility) on which they depend to enable a focus on critical resources for availability planning.	3
3. Collect data on availability patterns from logs of past failures and performance monitoring. Use modeling tools that help predict failures based on past usage trends and management expectations of new environment or user conditions.	4
4. Based on the collected data, create scenarios that describe future availability situations to illustrate a variety of potential capacity levels needed to achieve the availability performance objective.	
5. Based on the scenarios, determine the likelihood that the availability performance objective will not be achieved.	
6. Determine the impact of the scenarios on the business performance measures (e.g., revenue, profit, customer services). Engage the business-line, functional (especially finance) and regional leaders to understand their evaluation of impact.	
7. Ensure that business process owners fully understand and agree to the results of this analysis. From the business owners, obtain a list of unacceptable risk scenarios that require a response to reduce risk to acceptable levels.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISO/IEC 20000-1:2011(E)	6.3 Service continuity and availability management

Management Practice	Example Metrics
BAI04.03 Plan for new or changed service requirements. Plan and prioritize availability, performance and capacity implications of changing business needs and service requirements.	a. Number of unplanned capacity, performance or availability upgrades b. Percent that management performs comparisons of actual demand on resources against forecasted supply and demand

Activities	Capability Level
1. Identify availability and capacity implications of changing business needs and improvement opportunities. Use modeling techniques to validate availability, performance and capacity plans.	3
2. Review availability and capacity implications of service trend analysis.	4
3. Ensure that management performs comparisons of actual demand on resources against forecasted supply and demand to evaluate current forecasting techniques and make improvements where possible.	
4. Prioritize needed improvements and create cost-justifiable availability and capacity plans.	5
5. Adjust the performance and capacity plans and SLAs based on realistic, new, proposed and/or projected business processes and supporting services, applications and infrastructure changes. Also include reviews of actual performance and capacity usage, including workload levels.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISO/IEC 20000-1:2011(E)	5. Design and transition of new changed services

Management Practice	Example Metrics
BAI04.04 Monitor and review availability and capacity. Monitor, measure, analyze, report and review availability, performance and capacity. Identify deviations from established baselines. Review trend analysis reports identifying any significant issues and variances. Initiate actions where necessary and ensure that all outstanding issues are addressed.	a. Number of events exceeding planned limits for capacity b. Number of transaction peaks exceeding target performance

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Provide capacity reports to the budgeting processes.	2
2. Establish a process for gathering data to provide management with monitoring and reporting information for availability, performance and capacity workload of all I&T-related resources.	3
3. Provide regular reporting of the results in an appropriate form for review by IT and business management and communication to enterprise management.	4
4. Integrate monitoring and reporting activities in the iterative capacity management activities (monitoring, analysis, tuning and implementations).	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
BAI04.05 Investigate and address availability, performance and capacity issues. Address deviations by investigating and resolving identified availability, performance and capacity issues.	a. Number and percentage of unresolved availability, performance and capacity issues b. Number of availability incidents
Activities	**Capability Level**
1. Obtain guidance from vendor product manuals to ensure an appropriate level of performance availability for peak processing and workloads.	3
2. Define an escalation procedure for swift resolution in case of emergency capacity and performance problems.	
3. Identify performance and capacity gaps based on monitoring current and forecasted performance. Use the known availability, continuity and recovery specifications to classify resources and allow prioritization.	4
4. Define corrective actions (e.g., shifting workload, prioritizing tasks or adding resources when performance and capacity issues are identified).	5
5. Integrate required corrective actions into the appropriate planning and change management processes.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

B. Component: Organizational Structures								
Key Management Practice	**Executive Committee**	**Chief Information Officer**	**Chief Technology Officer**	**Business Process Owners**	**Head Architect**	**Head IT Operations**	**Service Manager**	**Business Continuity Manager**
BAI04.01 Assess current availability, performance and capacity and create a baseline.		R	A	R		R	R	
BAI04.02 Assess business impact.	A			R		R	R	
BAI04.03 Plan for new or changed service requirements.		R	A	R		R	R	
BAI04.04 Monitor and review availability and capacity.	A			R		R	R	
BAI04.05 Investigate and address availability, performance and capacity issues.		R	A	R	R	R	R	R
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**							
No related guidance for this component								

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
BAI04.01 Assess current availability, performance and capacity and create a baseline.	BAI02.01	Requirements definition repository	Evaluations against SLAs	APO09.05
	BAI02.03	Requirements risk register	Availability, performance and capacity baselines	Internal
BAI04.02 Assess business impact.	BAI03.02	Internal and external service level agreements (SLAs)	Availability, performance and capacity business impact assessments	Internal
			Availability, performance and capacity scenarios	Internal
BAI04.03 Plan for new or changed service requirements.	BAI02.01	Confirmed acceptance criteria from stakeholders	Performance and capacity plans	APO02.02
	BAI03.01	Approved high-level design specification	Prioritized improvements	APO02.02
	BAI03.02	Approved detailed design specification		
	BAI03.03	Documented solution components		
BAI04.04 Monitor and review availability and capacity.			Availability, performance and capacity monitoring review reports	MEA01.03
BAI04.05 Investigate and address availability, performance and capacity issues.			Corrective actions	APO02.02
			Emergency escalation procedure	DSS02.02
			Performance and capacity gaps	Internal

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Availability management	Skills Framework for the Information Age V6, 2015	AVMT
Capacity management	Skills Framework for the Information Age V6, 2015	CPMG

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Availability management policy	Informs infrastructure planning in terms of availability, scalability, reliability and potentially resilience. Includes guidelines to identify bandwidth, capacity and availability of services (prior to design and provisioning), establish service level agreements (SLAs), and implement continuous monitoring of circuits, traffic and response times.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
For enterprises that depend on information, availability and capacity management are critical to successful operations. Establish a culture in which product and service availability and capacity are prioritized (in line with business requirements) and supported by processes and behaviors that not only identify required availability and capacity before design, but also consider them in provisioning. Consistently define smart SLAs; continuously monitor circuits, traffic and response times; perform regular testing for business continuity and disaster recovery of infrastructure.		

G. Component: Services, Infrastructure and Applications
• Capacity planning tools • Provisioning services and tools • Service level monitoring tools

Page intentionally left blank

Domain: Build, Acquire and Implement Management Objective: BAI05 — Managed Organizational Change	Focus Area: COBIT Core Model

Description

Maximize the likelihood of successfully implementing sustainable enterprisewide organizational change quickly and with reduced risk. Cover the complete life cycle of the change and all affected stakeholders in the business and IT.

Purpose

Prepare and commit stakeholders for business change and reduce the risk of failure.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG05 Customer-oriented service culture • EG08 Optimization of internal business process functionality • EG12 Managed digital transformation programs	• AG03 Realized benefits from I&T-enabled investments and services portfolio • AG08 Enabling and supporting business processes by integrating applications and technology • AG09 Delivering programs on time, on budget and meeting requirements and quality standards

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG01	a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG03	a. Percent of I&T-enabled investments for which claimed benefits in the business case are met or exceeded b. Percent of I&T services for which expected benefits (as stated in service level agreements) are realized
EG05	a. Number of customer service disruptions b. Percent of business stakeholders satisfied that customer service delivery meets agreed levels c. Number of customer complaints d. Trend of customer satisfaction survey results	AG08	a. Time to execute business services or processes b. Number of I&T-enabled business programs delayed or incurring additional cost due to technology-integration issues c. Number of business process changes that need to be delayed or reworked because of technology-integration issues d. Number of applications or critical infrastructures operating in silos and not integrated
EG08	a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities	AG09	a. Number of programs/projects on time and within budget b. Number of programs needing significant rework due to quality defects c. Percent of stakeholders satisfied with program/project quality
EG12	a. Number of programs on time and within budget b. Percent of stakeholders satisfied with program delivery c. Percent of business transformation programs stopped d. Percent of business transformation programs with regular reported status updates		

A. Component: Process

Management Practice	Example Metrics
BAI05.01 Establish the desire to change. Understand the scope and impact of the desired change. Assess stakeholder readiness and willingness to change. Identify actions that will motivate stakeholder acceptance and participation to make the change work successfully.	a. Level of senior management involvement b. Level of stakeholder desire for the change

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Assess the scope and impact of the envisioned change, the various stakeholders who are affected, the nature of the impact on and involvement required from each stakeholder group, and the current readiness and ability to adopt the change.	2
2. To establish the desire to change, identify, leverage and communicate current pain points, negative events, risk, customer dissatisfaction and business problems, as well as initial benefits, future opportunities and rewards, and competitive advantages.	
3. Issue key communications from the executive committee or CEO to demonstrate commitment to the change.	
4. Provide visible leadership from senior management to establish direction and to align, motivate and inspire stakeholders to desire the change.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PROSCI® 3-Phase Change Management Process	Phase 1. Preparing for change—Define your change management strategy
Management Practice	**Example Metrics**
BAI05.02 Form an effective implementation team. Establish an effective implementation team by assembling appropriate members, creating trust, and establishing common goals and effectiveness measures.	a. Number of identified skills or capacity issues in implementation team b. Stakeholder satisfaction ratings of implementation team
Activities	**Capability Level**
1. Identify and assemble an effective core implementation team that includes appropriate members from business and IT with the capacity to spend the required amount of time and contribute knowledge and expertise, experience, credibility, and authority. Consider including external parties such as consultants to provide an independent view or to address skill gaps. Identify potential change agents within different parts of the enterprise with whom the core team can work to support the vision and cascade changes.	3
2. Create trust within the core implementation team through carefully planned events with effective communication and joint activities.	
3. Develop a common vision and goals that support the enterprise objectives.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PROSCI® 3-Phase Change Management Process	Phase 1. Preparing for change—Prepare your change management team
Management Practice	**Example Metrics**
BAI05.03 Communicate desired vision. Communicate the desired vision for the change in the language of those affected by it. The communication should be made by senior management and include the rationale for, and benefits of, the change; the impacts of not making the change; and the vision, the road map and the involvement required of the various stakeholders.	a. Number of questions with regards to the change b. Stakeholder feedback on level of understanding of the change
Activities	**Capability Level**
1. Develop a vision communication plan to address the core audience groups, their behavioral profiles and information requirements, communication channels, and principles.	3
2. Deliver the communication at appropriate levels of the enterprise, in accordance with the plan.	
3. Reinforce the communication through multiple forums and repetition.	
4. Make all levels of leadership accountable for demonstrating the vision.	
5. Check understanding of the desired vision and respond to any issues highlighted by staff.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI05.04 Empower role players and identify short-term wins. Empower those with implementation roles by assigning accountability. Provide training and align organizational structures and HR processes. Identify and communicate short-term wins that are important from a change-enablement perspective.	a. Level of satisfaction of role players operating, using and maintaining the change b. Percent of role players trained c. Percent of role players with appropriate assigned authority d. Role player feedback on level of empowerment e. Role player self-assessment of relevant capabilities

Activities	Capability Level
1. Plan the training opportunities staff will need to develop the appropriate skills and attitudes to feel empowered.	2
2. Identify, prioritize and deliver opportunities for quick wins. These could be related to current known areas of difficulty or external factors that need to be addressed urgently.	
3. Leverage delivered quick wins by communicating the benefits to those impacted to show the vision is on track. Fine-tune the vision, keep leaders on board and build momentum.	
4. Identify organizational structures compatible with the vision; if required, make changes to ensure alignment.	3
5. Align HR processes and measurement systems (e.g., performance evaluation, compensation decisions, promotion decisions, recruiting and hiring) to support the vision.	
6. Identify and manage leaders who continue to resist needed change.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
BAI05.05 Enable operation and use. Plan and implement all technical, operational and usage aspects so all those who are involved in the future state environment can exercise their responsibility.	a. Percent of users appropriately empowered for the change b. Percent of plans developed for operation and use of the change

Activities	Capability Level
1. Develop a plan for operation and use of the change. The plan should communicate and build on realized quick wins, address behavioral and cultural aspects of the broader transition, and increase buy-in and engagement. Ensure that the plan covers a holistic view of the change and provides documentation (e.g., procedures), mentoring, training, coaching, knowledge transfer, enhanced immediate post-go-live support and ongoing support.	3
2. Implement the operation and use plan. Define and track success measures, including hard business measures and perception measures that indicate how people feel about a change. Take remedial action as necessary.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PROSCI® 3-Phase Change Management Process	Phase 2. Managing change

Management Practice	Example Metrics
BAI05.06 Embed new approaches. Embed new approaches by tracking implemented changes, assessing the effectiveness of the operation and use plan, and sustaining ongoing awareness through regular communication. Take corrective measures as appropriate (which may include enforcing compliance).	a. Level of satisfaction of users with adoption of the change b. Percent of compliance audits which identified root causes for low adoption c. Number of compliance audits conducted to identify root causes for low adoption and recommended corrective action

Activities	Capability Level
1. Make process owners accountable for normal day-to-day operations.	2
2. Celebrate successes and implement reward and recognition programs to reinforce the change.	3
3. Provide ongoing awareness through regular communication of the change and its adoption.	
4. Use performance measurement systems to identify root causes for low adoption. Take corrective action.	4
5. Conduct compliance audits to identify root causes for low adoption. Recommend corrective action.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PROSCI® 3-Phase Change Management Process	Phase 3. Reinforcing change

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI05.07 Sustain changes. Sustain changes through effective training of new staff, ongoing communication campaigns, continued commitment of top management, monitoring of adoption and sharing of lessons learned across the enterprise.	a. Number of trainings and knowledge transfers performed b. Percent of top management engagement towards reinforcing the change

Activities	Capability Level
1. Sustain and reinforce the change through regular communication that demonstrates top management commitment.	2
2. Provide mentoring, training, coaching and knowledge transfer to new staff to sustain the change.	3
3. Perform periodic reviews of the operation and use of the change. Identify improvements.	4
4. Capture lessons learned relating to implementation of the change. Share knowledge across the enterprise.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PROSCI® 3-Phase Change Management Process	Phase 3. Reinforcing change

B. Component: Organizational Structures																		
Key Management Practice	**Executive Committee**	**Chief Executive Officer**	**Chief Operating Officer**	**Chief Information Officer**	**Chief Technology Officer**	**Chief Digital Officer**	**I&T Governance Board**	**Business Process Owners**	**Program Manager**	**Project Manager**	**Project Management Office**	**Head Human Resources**	**Head Development**	**Head IT Operations**	**Service Manager**	**Information Security Manager**	**Business Continuity Manager**
BAI05.01 Establish the desire to change.	R	A		R	R	R	R	R	R	R		R					
BAI05.02 Form an effective implementation team.	A			R	R	R			R	R	R		R				
BAI05.03 Communicate desired vision.	A			R	R	R	R		R	R							
BAI05.04 Empower role players and identify short-term wins.	A			R	R	R			R	R		R					
BAI05.05 Enable operation and use.	A		R	R	R	R		R			R		R	R	R	R	R
BAI05.06 Embed new approaches.	A		R	R	R	R		R			R		R	R	R	R	R
BAI05.07 Sustain changes.	A		R	R	R	R		R	R	R	R		R	R	R	R	R
Related Guidance (Standards, Frameworks, Compliance Requirements)																		
No related guidance for this component																		

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
BAI05.01 Establish the desire to change.	**From**	**Description**	**Description**	**To**
	APO11.02	Results of quality of service, including customer feedback	Communications from executive management committing to change	Internal
	BAI02.01	• Requirements definition repository • Confirmed acceptance criteria from stakeholders	Communications of drivers for change	Internal
	BAI02.03	• Requirements risk register • Risk mitigation actions		
	BAI03.01	Approved high-level design specification		
	BAI03.02	Approved detailed design specification		
BAI05.02 Form an effective implementation team.	BAI02.01	Confirmed acceptance criteria from stakeholders	Common vision and goals	BAI01.02
			Implementation team and roles	BAI01.04
BAI05.03 Communicate desired vision.			Vision communication plan	BAI01.04
			Vision communications	BAI01.05
BAI05.04 Empower role players and identify short-term wins.	Outside COBIT	Enterprise organizational structure	Aligned HR performance objectives	APO07.04
			Identified quick wins	BAI01.04
			Communication of benefits	BAI01.06
BAI05.05 Enable operation and use.	BAI03.03	Documented solution components	Operation and use plan	APO08.04; BAI08.03; DSS01.01; DSS01.02; DSS06.02
	BAI03.10	Updated solution components and related documentation	Success measures and results	APO08.05; BAI07.07; BAI07.08; MEA01.03
BAI05.06 Embed new approaches.			HR performance review results	APO07.04
			Awareness communications	Internal
			Compliance audit results	MEA02.02; MEA03.03
BAI05.07 Sustain changes.			Knowledge transfer plans	BAI08.02; BAI08.03
			Communications of management's commitment	Internal
			Reviews of operational use	MEA02.02
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
No related guidance for this component				

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Business change management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.7. Business Change Management
Change implementation planning and management	Skills Framework for the Information Age V6, 2015	CIPM
Organization design and implementation	Skills Framework for the Information Age V6, 2015	ORDI

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Organizational change management policy	Provides framework and outlines principles for managing organizational change. Reflects current legislation and provides good people-management practices; ensures consistent approach to managing change across the organization.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Realizing value from I&T-enabled investments requires more than delivering I&T solutions and services. It also requires changes to business processes, skills and competencies, culture and behavior, etc., all of which must be included in the business case for the investment. Leadership must create a culture of continuous change through flexibility, openness and confidence and establish appropriate change management support and communication.		

G. Component: Services, Infrastructure and Applications
• Communication tools and channels • Surveying tools

Domain: Build, Acquire and Implement Management Objective: BAI06 — Managed IT Changes	Focus Area: COBIT Core Model

Description

Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. This includes change standards and procedures, impact assessment, prioritization and authorization, emergency changes, tracking, reporting, closure, and documentation.

Purpose

Enable fast and reliable delivery of change to the business. Mitigate the risk of negatively impacting the stability or integrity of the changed environment.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
EG01 Portfolio of competitive products and services	AG06 Agility to turn business requirements into operational solutions
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG01 a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG06 a. Level of satisfaction of business executives with I&T responsiveness to new requirements b. Average time to market for new I&T-related services and applications c. Average time to turn strategic I&T objectives into agreed and approved initiatives d. Number of critical business processes supported by up-to-date infrastructure and applications

A. Component: Process

Management Practice	Example Metrics
BAI06.01 Evaluate, prioritize and authorize change requests. Evaluate all requests for change to determine the impact on business processes and I&T services, and to assess whether change will adversely affect the operational environment and introduce unacceptable risk. Ensure that changes are logged, prioritized, categorized, assessed, authorized, planned and scheduled.	a. Amount of rework caused by failed changes b. Percent of unsuccessful changes due to inadequate impact assessments

Activities	Capability Level
1. Use formal change requests to enable business process owners and IT to request changes to business process, infrastructure, systems or applications. Make sure that all such changes arise only through the change request management process.	2
2. Categorize all requested changes (e.g., business process, infrastructure, operating systems, networks, application systems, purchased/packaged application software) and relate affected configuration items.	
3. Prioritize all requested changes based on the business and technical requirements; resources required; and the legal, regulatory and contractual reasons for the requested change.	
4. Formally approve each change by business process owners, service managers and IT technical stakeholders, as appropriate. Changes that are low-risk and relatively frequent should be pre-approved as standard changes.	
5. Plan and schedule all approved changes.	
6. Plan and evaluate all requests in a structured fashion. Include an impact analysis on business process, infrastructure, systems and applications, business continuity plans (BCPs) and service providers to ensure that all affected components have been identified. Assess the likelihood of adversely affecting the operational environment and the risk of implementing the change. Consider security, privacy, legal, contractual and compliance implications of the requested change. Consider also inter-dependencies among changes. Involve business process owners in the assessment process, as appropriate.	3
7. Consider the impact of contracted services providers (e.g., of outsourced business processing, infrastructure, application development and shared services) on the change management process. Include integration of organizational change management processes with change management processes of service providers and the impact on contractual terms and SLAs.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISF, The Standard of Good Practice for Information Security 2016	SY2.4 Change Management
ISO/IEC 20000-1:2011(E)	9.2 Change management
ITIL V3, 2011	Service Transition, 4.2 Change Management
PMBOK Guide Sixth Edition, 2017	Part 1: 4.6 Perform Integrated Change Control

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI06.02 Manage emergency changes. Carefully manage emergency changes to minimize further incidents. Ensure the emergency change is controlled and takes place securely. Verify that emergency changes are appropriately assessed and authorized after the change.	a. Number of emergency changes not authorized after the incident b. Percent of total changes that are emergency fixes
Activities	**Capability Level**
1. Define what constitutes an emergency change.	2
2. Ensure that a documented procedure exists to declare, assess, approve preliminarily, authorize after the change and record an emergency change.	
3. Verify that all emergency access arrangements for changes are appropriately authorized, documented and revoked after the change has been applied.	3
4. Monitor all emergency changes and conduct post-implementation reviews involving all concerned parties. The review should consider and initiate corrective actions based on root causes such as problems with business process, application system development and maintenance, development and test environments, documentation and manuals, and data integrity.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
BAI06.03 Track and report change status. Maintain a tracking and reporting system to document rejected changes and communicate the status of approved, in-process and complete changes. Make certain that approved changes are implemented as planned.	a. Number and age of backlogged change requests b. Percent of change request status reported to stakeholders in a timely manner
Activities	**Capability Level**
1. Categorize change requests in the tracking process (e.g., rejected, approved but not yet initiated, approved and in process, and closed).	4
2. Implement change status reports with performance metrics to enable management review and monitoring of both the detailed status of changes and the overall state (e.g., aged analysis of change requests). Ensure that status reports form an audit trail so changes can subsequently be tracked from inception to eventual disposition.	
3. Monitor open changes to ensure that all approved changes are closed in a timely fashion, depending on priority.	
4. Maintain a tracking and reporting system for all change requests.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	IP.CC Apply Change Control
Management Practice	**Example Metrics**
BAI06.04 Close and document the changes. Whenever changes are implemented, update the solution, user documentation and procedures affected by the change.	a. Number of review errors found in the documentation b. Percent of user documentation and procedures updates performed in a timely manner
Activities	**Capability Level**
1. Include changes in the documentation within the management procedure. Examples of documentation include business and IT operational procedures, business continuity and disaster recovery documentation, configuration information, application documentation, help screens, and training materials.	2
2. Define an appropriate retention period for change documentation and pre- and post-change system and user documentation.	3
3. Subject documentation to the same level of review as the actual change.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

B. Component: Organizational Structures										
Key Management Practice	Chief Information Officer	Business Process Owners	Program Manager	Project Manager	Head Development	Head IT Operations	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI06.01 Evaluate, prioritize and authorize change requests.	A	R			R	R	R	R	R	R
BAI06.02 Manage emergency changes.	A				R	R	R	R		R
BAI06.03 Track and report change status.	A	R	R	R	R	R	R			
BAI06.04 Close and document the changes.	A	R	R	R	R	R	R		R	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	Inputs		Outputs	
	From	Description	Description	To
BAI06.01 Evaluate, prioritize and authorize change requests.	BAI03.05	Integrated and configured solution components	Change plan and schedule	BAI07.01
	DSS02.03	Approved service requests	Approved requests for change	BAI07.01
	DSS03.03	Proposed solutions to known errors	Impact assessments	Internal
	DSS03.05	Identified sustainable solutions		
	DSS04.08	Approved changes to the plans		
	DSS06.01	Root cause analyses and recommendations		
BAI06.02 Manage emergency changes.			Post-implementation review of emergency changes	Internal
BAI06.03 Track and report change status.	BAI03.09	Record of all approved and applied change requests	Change request status reports	BAI01.06; BAI10.03
BAI06.04 Close and document the changes.			Change documentation	Internal

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Change management	Skills Framework for the Information Age V6, 2015	CHMG
Change support	e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework, 2016	C. Run - C.2. Change Support

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
IT change management policy	Communicates management intent that all changes to enterprise IT are managed and implemented so as to minimize risk and impact to stakeholders. Covers in-scope assets and standard change management process.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Leaders must create a culture of continuous improvement in IT solutions and services, recognizing that improvement requires them to understand the impact of technology change on the enterprise, its inherent risk and associated mitigation, as well as its cost. Leaders must balance the impact of change against its expected benefits and contribution to I&T strategy and enterprise objectives.		

G. Component: Services, Infrastructure and Applications
• Configuration management tools • IT change management tools

Domain: Build, Acquire and Implement Management Objective: BAI07 — Managed IT Change Acceptance and Transitioning	Focus Area: COBIT Core Model

Description

Formally accept and make operational new solutions. Include implementation planning, system and data conversion, acceptance testing, communication, release preparation, promotion to production of new or changed business processes and I&T services, early production support, and a post-implementation review.

Purpose

Implement solutions safely and in line with the agreed expectations and outcomes.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
EG01 Portfolio of competitive products and services	AG06 Agility to turn business requirements into operational solutions
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG01 a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG06 a. Level of satisfaction of business executives with I&T responsiveness to new requirements b. Average time to market for new I&T-related services and applications c. Average time to turn strategic I&T objectives into agreed and approved initiatives d. Number of critical business processes supported by up-to-date infrastructure and applications

A. Component: Process

Management Practice	Example Metrics
BAI07.01 Establish an implementation plan. Establish an implementation plan that covers system and data conversion, acceptance testing criteria, communication, training, release preparation, promotion to production, early production support, a fallback/back-up plan, and a post-implementation review. Obtain approval from relevant parties.	a. Number and category of stakeholders signing off on the implementation plan b. Number of implementation plans that are robust and contain all required components

Activities	Capability Level
1. Create an implementation plan that reflects the broad implementation strategy, the sequence of implementation steps, resource requirements, inter-dependencies, criteria for management acceptance of the production implementation, installation verification requirements, transition strategy for production support, and update of business continuity plans.	2
2. From external solution providers, obtain commitment to their involvement in each step of the implementation.	
3. Identify and document the fallback and recovery processes.	
4. Confirm that all implementation plans are approved by technical and business stakeholders and reviewed by internal audit, as appropriate.	3
5. Formally review the technical and business risk associated with implementation. Ensure that the key risk is considered and addressed in the planning process.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ITIL V3, 2011	Service Transition, 4.1 Transition Planning and Support

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI07.02 Plan business process, system and data conversion. Prepare for business process, I&T service data and infrastructure migration as part of the enterprise's development methods. Include audit trails and a recovery plan should the migration fail.	a. Percent of successful conversion b. Percent of necessary adjustments made to procedures (including revised roles and responsibilities and control procedures)

Activities	Capability Level
1. Define a business process, I&T service data and infrastructure migration plan. In developing the plan, consider, for example, hardware, networks, operating systems, software, transaction data, master files, backups and archives, interfaces with other systems (both internal and external), possible compliance requirements, business procedures, and system documentation.	2
2. In the business process conversion plan, consider all necessary adjustments to procedures, including revised roles and responsibilities and control procedures.	
3. Confirm that the data conversion plan does not require changes in data values unless absolutely necessary for business reasons. Document changes made to data values, and secure approval from the business process data owner.	
4. Plan retention of backup and archived data to conform to business needs and regulatory or compliance requirements.	
5. Rehearse and test the conversion before attempting a live conversion.	
6. Coordinate and verify the timing and completeness of the conversion cutover so there is a smooth, continuous transition with no loss of transaction data. Where necessary, in the absence of any other alternative, freeze live operations.	
7. Plan to back up all systems and data taken at the point prior to conversion. Maintain audit trails to enable the conversion to be retraced. Ensure that there is a recovery plan that covers rollback of migration and fallback to previous processing should the migration fail.	
8. In the data conversion plan, incorporate methods for collecting, converting and verifying data to be converted, and identifying and resolving any errors found during conversion. Include comparing the original and converted data for completeness and integrity.	3
9. Consider the risk of conversion problems, business continuity planning and fallback procedures in the business process, data and infrastructure migration plan where there are risk management, business needs or regulatory/compliance requirements.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ITIL V3, 2011	Service Transition, 4.1 Transition Planning and Support

Management Practice	Example Metrics
BAI07.03 Plan acceptance tests. Establish a test plan based on enterprisewide standards that define roles, responsibilities, and entry and exit criteria. Ensure that the plan is approved by relevant parties.	a. Percent of stakeholders satisfied with the completeness of testing process b. Number of documented test plans that include all testing phases and robust testing scenarios and are appropriate to the operational requirements and environment

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Develop and document the test plan, which aligns to the program, project quality plan and relevant organizational standards. Communicate and consult with appropriate business process owners and IT stakeholders.	2
2. Ensure that the test plan reflects an assessment of risk from the project and that all functional and technical requirements are tested. Based on assessment of the risk of system failure and faults on implementation, include in the plan requirements for performance, stress, usability, pilot, security testing and privacy.	
3. Ensure that the test plan addresses the potential need for internal or external accreditation of outcomes of the test process (e.g., financial or regulatory requirements).	
4. Ensure that the test plan identifies necessary resources to execute testing and evaluate the results. Examples of resources may be construction of test environments and use of staff time for the test group, including potential temporary replacement of test staff in the production or development environments. Ensure that stakeholders are consulted on the resource implications of the test plan.	
5. Ensure that the test plan identifies testing phases appropriate to the operational requirements and environment. Examples of such testing phases include unit test, system test, integration test, user acceptance test, performance test, stress test, data conversion test, security test, privacy test, operational readiness test, and backup and recovery tests.	
6. Confirm that the test plan considers test preparation (including site preparation), training requirements, installation or an update of a defined test environment, planning/performing/documenting/retaining test cases, error and problem handling, correction and escalation, and formal approval.	
7. Confirm that all test plans are approved by stakeholders, including business process owners and IT, as appropriate. Stakeholders may include application development managers, project managers and business process end users.	
8. Ensure that the test plan establishes clear criteria for measuring the success of undertaking each testing phase. Consult the business process owners and IT stakeholders in defining the success criteria. Determine that the plan establishes remediation procedures when the success criteria are not met. For example, if there is a significant failure in a testing phase, the plan should provide guidance on whether to proceed to the next phase, stop testing or postpone implementation.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
BAI07.04 Establish a test environment. Define and establish a secure test environment representative of the planned business process and IT operations environment in terms of performance, capacity, security, internal controls, operational practices, data quality, privacy requirements and workloads.	a. Level of comparability between test environment and future business and operational landscape b. Level of sanitized test data (and/or databases) that are representative of the production environment
Activities	**Capability Level**
1. Create a database of test data that are representative of the production environment. Sanitize data used in the test environment from the production environment according to business needs and organizational standards. For example, consider whether compliance or regulatory requirements oblige the use of sanitized data.	2
2. Protect sensitive test data and results against disclosure, including access, retention, storage and destruction. Consider the effect of interaction of organizational systems with those of third parties.	3
3. Put in place a process to enable proper retention or disposal of test results, media and other associated documentation that will enable adequate review and subsequent analysis or efficient retesting as required by the test plan. Consider the effect of regulatory or compliance requirements.	
4. Ensure that the test environment is representative of the future business and operational landscape. Include business process procedures and roles, likely workload stress, operating systems, necessary application software, database management systems, and network and computing infrastructure found in the production environment.	
5. Ensure that the test environment is secure and incapable of interacting with production systems.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI07.05 Perform acceptance tests. Test changes independently, in accordance with the defined test plan, prior to migration to the live operational environment.	a. Number of identified gaps between acceptance test results and the defined success criteria b. Number of successful acceptance tests

Activities	Capability Level
1. Review the categorized log of errors found in the testing process by the development team. Verify that all errors have been remediated or formally accepted.	2
2. Evaluate the final acceptance against the success criteria and interpret the final acceptance testing results. Present them in a form that is understandable to business process owners and IT, so an informed review and evaluation can take place.	3
3. Approve the acceptance, with formal sign-off by the business process owners, third parties (as appropriate) and IT stakeholders prior to promotion.	
4. Ensure that testing of changes is undertaken in accordance with the testing plan. Ensure that the testing is designed and conducted by a test group that is independent from the development team. Consider the extent to which business process owners and end users are involved in the test group. Ensure that testing is conducted only within the test environment.	
5. Ensure that the tests and anticipated outcomes are in accordance with the defined success criteria set out in the testing plan.	
6. Consider using clearly defined test instructions (scripts) to implement the tests. Ensure that the independent test group assesses and approves each test script to confirm that it adequately addresses test success criteria set out in the test plan. Consider using scripts to verify the extent to which the system meets security and privacy requirements.	
7. Consider the appropriate balance between automated scripted tests and interactive user testing.	
8. Undertake tests of security in accordance with the test plan. Measure the extent of security weaknesses or loopholes. Consider the effect of security incidents since construction of the test plan. Consider the effect on access and boundary controls. Consider privacy.	
9. Undertake tests of system and application performance in accordance with the test plan. Consider a range of performance metrics (e.g., end-user response times and database management system update performance).	
10. When undertaking testing, ensure that the fallback and rollback elements of the test plan have been addressed.	
11. Identify, log and classify (e.g., minor, significant, mission-critical) errors during testing. Ensure that an audit trail of test results is available. In accordance with the test plan, communicate results of testing to stakeholders to facilitate bug fixing and further quality enhancement.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ITIL V3, 2011	Service Transition, 4.5 Service Validation and Testing

Management Practice	Example Metrics
BAI07.06 Promote to production and manage releases. Promote the accepted solution to the business and operations. Where appropriate, run the solution as a pilot implementation or in parallel with the old solution for a defined period and compare behavior and results. If significant problems occur, revert to the original environment based on the fallback/back-up plan. Manage releases of solution components.	a. Number and percent of releases not ready for release on schedule b. Percent of stakeholder satisfaction with the implemented solution

Activities	Capability Level
1. Prepare for transfer of business procedures and supporting services, applications and infrastructure from testing to the production environment in accordance with organizational change management standards.	2
2. Determine the extent of pilot implementation or parallel processing of the old and new systems in line with the implementation plan.	
3. Promptly update relevant business process and system documentation, configuration information and contingency plan documents, as appropriate.	
4. Ensure that all media libraries are updated promptly with the version of the solution component being transferred from testing to the production environment. Archive the existing version and its supporting documentation. Ensure that promotion to production of systems, application software and infrastructure is under configuration control.	
5. Where distribution of solution components is conducted electronically, control automated distribution to ensure that users are notified, and distribution occurs only to authorized and correctly identified destinations. In the release process, include backup procedures to enable the distribution of changes to be reviewed in the event of a malfunction or error.	
6. Where distribution takes physical form, keep a formal log of what items have been distributed, to whom, where they have been implemented, and when each has been updated.	

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISO/IEC 20000-1:2011(E)	9.3 Release and deployment management
ITIL V3 2011	Service Transition, 4.4 Release and Deployment Management
Management Practice	**Example Metrics**
BAI07.07 Provide early production support. For an agreed period of time, provide early support to users and I&T operations to resolve issues and help stabilize the new solution.	a. Number of additional I&T system resources provided for support b. Number of additional staff resources provided for support
Activities	**Capability Level**
1. Provide additional resources, as required, to end users and support personnel until the release has stabilized.	3
2. Provide additional I&T systems resources, as required, until the release is in a stable operational environment.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
BAI07.08 Perform a post-implementation review. Conduct a post-implementation review to confirm outcome and results, identify lessons learned, and develop an action plan. Evaluate actual performance and outcomes of the new or changed service against expected performance and outcomes anticipated by the user or customer.	a. Number and percent of root cause analyses completed b. Number or percent of releases that fail to stabilize within an acceptable period c. Percent of releases causing downtime
Activities	**Capability Level**
1. Establish procedures to ensure that post-implementation reviews identify, assess and report on the extent to which the following events have occurred: enterprise requirements have been met; expected benefits have been realized; the system is considered usable; internal and external stakeholder expectations are met; unexpected impacts on the enterprise have occurred; key risk is mitigated; and the change management, installation and accreditation processes were performed effectively and efficiently.	3
2. Consult business process owners and IT technical management in the choice of metrics for measurement of success and achievement of requirements and benefits.	4
3. Conduct the post-implementation review in accordance with the organizational change management process. Engage business process owners and third parties, as appropriate.	
4. Consider requirements for post-implementation review arising from outside business and IT (e.g., internal audit, ERM, compliance).	
5. Agree on and implement an action plan to address issues identified in the post-implementation review. Engage business process owners and IT technical management in the development of the action plan.	5
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ITIL V3, 2011	Service Transition, 4.6 Change Evaluation

B. Component: Organizational Structures

Key Management Practice	Chief Information Officer	Business Process Owners	Data Management Function	Head Development	Head IT Operations	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI07.01 Establish an implementation plan.	A	R		R		R	R	R	
BAI07.02 Plan business process, system and data conversion.	A	R	R	R		R	R	R	
BAI07.03 Plan acceptance tests.	A	R		R	R		R	R	R
BAI07.04 Establish a test environment.	A	R		R	R		R	R	
BAI07.05 Perform acceptance tests.	A	R		R	R		R	R	R
BAI07.06 Promote to production and manage releases.	A	R		R	R	R		R	
BAI07.07 Provide early production support.	A	R		R	R	R			
BAI07.08 Perform a post-implementation review.	A	R		R	R	R			

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)

Management Practice	Inputs		Outputs	
	From	Description	Description	To
BAI07.01 Establish an implementation plan.	BAI01.07	Quality management plan	Implementation fallback and recovery processes	Internal
	BAI06.01	• Approved requests for change • Change plan and schedule	Approved implementation plan	Internal
	BAI11.05	Project quality management plan		
BAI07.02 Plan business process, system and data conversion.			Migration plan	DSS06.02
BAI07.03 Plan acceptance tests.	BAI01.07	Requirements for independent verification of deliverables	Approved acceptance test plan	BAI01.04; BAI11.04
	BAI03.07	• Test plan • Test procedures		
	BAI03.08	• Test result logs and audit trails • Test result communications		
	BAI11.05	Requirements for independent verification of project deliverables		

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI07.04 Establish a test environment.	**From**	**Description**	**Description**	**To**
			Test data	Internal
BAI07.05 Perform acceptance tests.			Approved acceptance and release for production	BAI01.04
			Evaluation of acceptance results	BAI01.06
			Test results log	Internal
BAI07.06 Promote to production and manage releases.			Release plan	BAI10.01
			Release log	Internal
BAI07.07 Provide early production support.	APO11.02	Results of quality of service, including customer feedback	Supplemental support plan	APO08.04; APO08.05; DSS02.04
	BAI05.05	Success measures and results		
BAI07.08 Perform a post-implementation review.	APO11.03	• Results of solution and service delivery quality monitoring • Root causes of quality delivery failures	Remedial action plan	BAI01.09; BAI11.09
	APO11.04	Results of quality reviews and audits	Post-implementation review report	BAI01.09; BAI11.09
	BAI05.05	Success measures and results		

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Business process testing	Skills Framework for the Information Age V6, 2015	BPTS
Release and deployment	Skills Framework for the Information Age V6, 2015	RELM
Service acceptance	Skills Framework for the Information Age V6, 2015	SEAC
Testing	Skills Framework for the Information Age V6, 2015	TEST
User experience evaluation	Skills Framework for the Information Age V6, 2015	USEV

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
IT change management policy	Communicates management intent that all changes to enterprise IT are managed and implemented so as to minimize risk and impact to stakeholders. Covers in-scope assets and standard change management process.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Establish a culture that ensures timely communication of IT change requests to affected groups; consult the affected groups regarding implementation and testing of changes.		

G. Component: Services, Infrastructure and Applications
• IT change management tools • Release management tools • Testing tools and services

Domain: Build, Acquire and Implement Management Objective: BAI08 — Managed Knowledge	Focus Area: COBIT Core Model

Description

Maintain the availability of relevant, current, validated and reliable knowledge and management information to support all process activities and to facilitate decision making related to the governance and management of enterprise I&T. Plan for the identification, gathering, organizing, maintaining, use and retirement of knowledge.

Purpose

Provide the knowledge and information required to support all staff in the governance and management of enterprise I&T and allow for informed decision making.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG10 Staff skills, motivation and productivity • EG13 Product and business innovation	• AG12 Competent and motivated staff with mutual understanding of technology and business • AG13 Knowledge, expertise and initiatives for business innovation

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG01	a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG12	a. Percent of I&T-savvy business people (i.e., those having the required knowledge and understanding of I&T to guide, direct, innovate and see I&T opportunities in their domain of business expertise) b. Percent of business-savvy I&T people (i.e., those having the required knowledge and understanding of relevant business domains to guide, direct, innovate and see I&T opportunities for the business domain) c. Number or percentage of business people with technology management experience
EG10	a. Staff productivity compared to benchmarks b. Level of stakeholder satisfaction with staff expertise and skills c. Percent of staff whose skills are insufficient for competency in their role d. Percent of satisfied staff	AG13	a. Level of business executive awareness and understanding of I&T innovation possibilities b. Number of approved initiatives resulting from innovative I&T ideas c. Number of innovation champions recognized/awarded
EG13	a. Level of awareness and understanding of business innovation opportunities b. Stakeholder satisfaction with levels of product and innovation expertise and ideas c. Number of approved product and service initiatives resulting from innovative ideas		

A. Component: Process	
Management Practice	**Example Metrics**
BAI08.01 Identify and classify sources of information for governance and management of I&T. Identify, validate and classify diverse sources of internal and external information required to enable governance and management of I&T, including strategy documents, incident reports and configuration information that progresses from development to operations before going live.	a. Percent of categorized information validated b. Percent of appropriateness of content types, artifacts, and structured and unstructured information

Activities	Capability Level
1. Identify potential knowledge users, including owners of information who may need to contribute and approve knowledge. Obtain knowledge requirements and sources of information from identified users.	2
2. Consider content types (procedures, processes, structures, concepts, policies, rules, facts, classifications), artefacts (documents, records, video, voice), and structured and unstructured information (experts, social media, email, voice mail, Rich Site Summary (RSS) feeds).	
3. Classify sources of information based on a content classification scheme (e.g., information architecture model). Map sources of information to the classification scheme.	3
4. Collect, collate and validate information sources based on information validation criteria (e.g., understandability, relevance, importance, integrity, accuracy, consistency, confidentiality, currency and reliability).	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
BAI08.02 Organize and contextualize information into knowledge. Organize information based on classification criteria. Identify and create meaningful relationships among information elements and enable use of information. Identify owners, and leverage and implement enterprise-defined information levels of access to management information and knowledge resources.	a. Number of relationships identified among sources of information (tagging) b. Percent of stakeholder satisfaction with the organization and contextualization of information into knowledge

Activities	Capability Level
1. Identify shared attributes and match sources of information, creating relationships among information sets (information tagging).	3
2. Create views to related data sets, considering stakeholder and organizational requirements.	
3. Devise and implement a scheme to manage unstructured knowledge not available through formal sources (e.g., expert knowledge).	
4. Publish and make knowledge accessible to relevant stakeholders, based on roles and access mechanisms.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
COSO Enterprise Risk Management, June 2017	10. Information, Communication, and Reporting - Principle 18

Management Practice	Example Metrics
BAI08.03 Use and share knowledge. Propagate available knowledge resources to relevant stakeholders and communicate how these resources can be used to address different needs (e.g., problem solving, learning, strategic planning and decision making).	a. Percent of available knowledge actually used b. Percent of knowledge user satisfaction

Activities	Capability Level
1. Set management expectations and demonstrate appropriate attitude regarding the usefulness of knowledge and the need to share knowledge related to the governance and management of enterprise I&T.	2
2. Identify potential knowledge users by knowledge classification.	
3. Transfer knowledge to knowledge users, based on a needs gap analysis and effective learning techniques. Create an environment, tools and artifacts that support the sharing and transfer of knowledge. Ensure appropriate access controls are in place, in line with defined knowledge classification.	3
4 .Measure the use of knowledge tools and elements and evaluate the impact on governance processes.	4
5. Improve information and knowledge for governance processes that show knowledge gaps.	5

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	PP.IS Apply Information Sharing; IR.ES Ensure Information sharing
ITIL V3, 2011	Service Transition, 4.7 Knowledge Management
PMBOK Guide Sixth Edition, 2017	Part 1: 4.4 Manage project knowledge
Management Practice	**Example Metrics**
BAI08.04 Evaluate and update or retire information. Measure the use and evaluate the currency and relevance of information. Update information or retire obsolete information.	a. Frequency of update b. Level of satisfaction of users

Activities	Capability Level
1. Define the controls for knowledge retirement and retire knowledge accordingly.	3
2. Evaluate the usefulness, relevance and value of knowledge elements. Update outdated information that still has relevance and value to the organization. Identify related information that is no longer relevant to the enterprise's knowledge requirements and retire or archive according to policy.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

B. Component: Organizational Structures																		
Key Management Practice	**Chief Information Officer**	**Chief Technology Officer**	**Chief Digital Officer**	**Business Process Owners**	**Portfolio Manager**	**Program Manager**	**Project Manager**	**Data Management Function**	**Head Architect**	**Head Development**	**Head IT Operations**	**Head IT Administration**	**Service Manager**	**Information Security Manager**	**Business Continuity Manager**	**Privacy Officer**	**Legal Counsel**
BAI08.01 Identify and classify sources of information for governance and management of I&T.	A			R				R		R	R		R				
BAI08.02 Organize and contextualize information into knowledge.	A							R		R	R	R					
BAI08.03 Use and share knowledge.	A	R	R	R	R	R	R	R				R					R
BAI08.04 Evaluate and update or retire information.	A			R		R	R	R	R	R	R	R	R	R	R	R	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	Inputs		Outputs	
	From	Description	Description	To
BAI08.01 Identify and classify sources of information for governance and management of I&T.	Outside COBIT	Knowledge requirements and sources	Classification of information sources	Internal
BAI08.02 Organize and contextualize information into knowledge.	BAI03.03	Documented solution components	Published knowledge repositories	APO07.03
	BAI05.07	Knowledge transfer plans		
BAI08.03 Use and share knowledge.	BAI03.03	Documented solution components	Knowledge awareness and training schemes	APO07.03
	BAI05.05	Operation and use plan	Knowledge user database	Internal
	BAI05.07	Knowledge transfer plans		
BAI08.04 Evaluate and update or retire information.			Rules for knowledge retirement	Internal
			Knowledge use evaluation results	Internal
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
No related guidance for this component				

D. Component: People, Skills and Competencies		
Skill	Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
Information and knowledge management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	D. Enable—D.10. Information and Knowledge Management

E. Component: Policies and Procedures			
Relevant Policy	Policy Description	Related Guidance	Detailed Reference
Governance knowledge use policy	Guides creation and use of knowledge assets relating to I&T governance. I&T knowledge assets should be readily accessible for reference.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	Related Guidance	Detailed Reference
Embed a knowledge-sharing culture in the enterprise. Proactively communicate the value of knowledge to encourage knowledge creation, use, reuse and sharing. Encourage the sharing and transfer of knowledge by identifying and leveraging motivational factors.		

G. Component: Services, Infrastructure and Applications
• Collaboration platform • Knowledge repository

Domain: Build, Acquire and Implement Management Objective: BAI09 — Managed Assets	Focus Area: COBIT Core Model

Description

Manage I&T assets through their life cycle to make sure that their use delivers value at optimal cost, they remain operational (fit for purpose), and they are accounted for and physically protected. Ensure that those assets that are critical to support service capability are reliable and available. Manage software licenses to ensure that the optimal number are acquired, retained and deployed in relation to required business usage, and the software installed is in compliance with license agreements.

Purpose

Account for all I&T assets and optimize the value provided by their use.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG04 Quality of financial information • EG07 Quality of management information • EG09 Optimization of business process costs	AG04 Quality of technology-related financial information

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG04	a. Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of enterprise financial information b. Cost of noncompliance with finance-related regulations	AG04	a. Satisfaction of key stakeholders regarding the level of transparency, understanding and accuracy of I&T financial information b. Percent of I&T services with defined and approved operational costs and expected benefits
EG07	a. Degree of board and executive management satisfaction with decision-making information b. Number of incidents caused by incorrect business decisions based on inaccurate information c. Time to provide information supporting effective business decisions d. Timeliness of management information		
EG09	a. Ratio of cost vs. achieved service levels b. Satisfaction levels of board and executive management with business processing costs		

A. Component: Process

Management Practice	Example Metrics
BAI09.01 Identify and record current assets. Maintain an up-to-date, accurate record of all I&T assets that are required to deliver services and that are owned or controlled by the organization with an expectation of future benefit (including resources with economic value, such as hardware or software). Ensure alignment with configuration management and financial management.	a. Percent of assets accurately recorded in asset register b. Percent of assets that are fit for purpose c. Percent of assets inventoried and kept current

Activities	Capability Level
1. Identify all owned assets in an asset register that records current status. Assets are reported on the balance sheet; they are bought or created to increase the value of a firm or benefit the enterprise's operations (e.g., hardware and software). Identify all owned assets and maintain alignment with the change management and configuration management processes, the configuration management system, and the financial accounting records.	2
2. Identify legal, regulatory or contractual requirements that need to be addressed when managing the asset.	
3. Verify that the assets are fit for purpose (i.e., in a useful condition).	
4. Ensure accounting for all assets.	3
5. Verify the existence of all owned assets by performing regular physical and logical inventory checks and reconciliation. Include the use of software discovery tools.	4
6. Determine on a regular basis whether each asset continues to provide value. If so, estimate the expected useful life for delivering value.	

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	RI.AD Asset Discovery & Identification
ISF, The Standard of Good Practice for Information Security 2016	BA1.1 Business Application Register
ISO/IEC 27002:2013/Cor.2:2015(E)	8.1 Responsibility for assets
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.13 Physical and environmental protection (PE-9)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 1: Inventory of Authorized and Unauthorized Devices; CSC 2: Inventory of Authorized and Unauthorized Software
Management Practice	**Example Metrics**
BAI09.02 Manage critical assets. Identify assets that are critical in providing service capability. Maximize their reliability and availability to support business needs.	a. Number of critical assets b. Average downtime per critical asset c. Number of incident trends identified

Activities	Capability Level
1. Identify assets that are critical in providing service capability by referencing requirements in service definitions, SLAs and the configuration management system.	2
2. On a regular basis, consider the risk of failure or need for replacement of each critical asset.	
3. Communicate to affected customers and users the expected impact (e.g., performance restrictions) of maintenance activities.	
4. Incorporate planned downtime in an overall production schedule. Schedule the maintenance activities to minimize the adverse impact on business processes.	3
5. Maintain the resilience of critical assets by applying regular preventive maintenance. Monitor performance and, if required, provide alternative and/or additional assets to minimize the likelihood of failure.	
6. Establish a preventive maintenance plan for all hardware, considering cost/benefit analysis, vendor recommendations, risk of outage, qualified personnel and other relevant factors.	
7. Establish maintenance agreements involving third-party access to organizational I&T facilities for on-site and off-site activities (e.g., outsourcing). Establish formal service contracts containing or referring to all necessary security and privacy conditions, including access authorization procedures, to ensure compliance with the organizational security/privacy policies and standards.	
8. Ensure that remote access services and user profiles (or other means used for maintenance or diagnosis) are active only when required.	
9. Monitor performance of critical assets by examining incident trends. Where necessary, take action to repair or replace.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	ID.AM Asset Management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.13 Physical and environmental protection (PE-20)
Management Practice	**Example Metrics**
BAI09.03 Manage the asset life cycle. Manage assets from procurement to disposal. Ensure that assets are utilized as effectively and efficiently as possible and are accounted for and physically protected until appropriately retired.	a. Percent of assets managed from procurement to disposal b. Utilization percentage per asset c. Percent of assets deployed following the standard implementation life cycle

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Procure all assets based on approved requests and in accordance with the enterprise procurement policies and practices.	2
2. Source, receive, verify, test and record all assets in a controlled manner, including physical labeling as required.	
3. Approve payments and complete the process with suppliers according to agreed contract conditions.	
4. Deploy assets following the standard implementation life cycle, including change management and acceptance testing.	3
5. Allocate assets to users, with acceptance of responsibilities and sign-off, as appropriate.	
6. Whenever possible, reallocate assets when they are no longer required due to a change of user role, redundancy within a service, or retirement of a service.	
7. Plan, authorize and implement retirement-related activities, retaining appropriate records to meet ongoing business and regulatory needs.	
8. Dispose of assets securely, considering, for example, the permanent deletion of any recorded data on media devices and potential damage to the environment.	
9. Dispose of assets responsibly when they serve no useful purpose due to retirement of all related services, obsolete technology or lack of users with regard to environmental impact.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	DP.ML Manage Asset Lifecycle
ISF, The Standard of Good Practice for Information Security 2016	IM2.1 Document Management; PA1.1 Hardware Life Cycle Management
ITIL V3, 2011	Service Transition, 4.3 Service Asset and Configuration Management
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	PR.MA Maintenance
Management Practice	**Example Metrics**
BAI09.04 Optimize asset value. Regularly review the overall asset base to identify ways to optimize value in alignment with business needs.	a. Benchmark costs b. Number of assets not utilized
Activities	**Capability Level**
1. On a regular basis, review the overall asset base, considering whether it is aligned with business requirements.	3
2. Assess maintenance costs, consider reasonableness, and identify lower-cost options. Include, where necessary, replacement with new alternatives.	4
3. Review warranties and consider value-for-money and replacement strategies to determine lowest-cost options.	5
4. Use capacity and utilization statistics to identify underutilized or redundant assets that could be considered for disposal or replacement to reduce costs.	
5. Review the overall base to identify opportunities for standardization, single sourcing, and other strategies that may lower procurement, support and maintenance costs.	
6. Review the overall state to identify opportunities to leverage emerging technologies or alternative sourcing strategies to reduce costs or increase value-for-money.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
BAI09.05 Manage licenses. Manage software licenses to maintain the optimal number of licenses and support business requirements. Ensure that the number of licenses owned is sufficient to cover the installed software in use.	a. Percent of used licenses against purchased licenses b. Percent of licenses still being paid for but not being used c. Percent of products and licenses that should be upgraded to achieve better value

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Maintain a register of all purchased software licenses and associated license agreements.	2
2. On a regular basis, conduct an audit to identify all instances of installed licensed software.	3
3. Compare the number of installed software instances with the number of licenses owned. Ensure that the license compliance measurement method is compliant with the license and contractual requirements.	4
4. When instances are lower than the number owned, decide whether there is a need to retain or terminate licenses, considering the potential to save on unnecessary maintenance, training and other costs.	
5. When instances are higher than the number owned, consider first the opportunity to uninstall instances that are no longer required or justified, and then, if necessary, purchase additional licenses to comply with the license agreement.	
6. On a regular basis, consider whether better value can be obtained by upgrading products and associated licenses.	5
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

B. Component: Organizational Structures									
Key Management Practice	**Chief Information Officer**	**Chief Technology Officer**	**Head Architect**	**Head Development**	**Head IT Operations**	**Head IT Administration**	**Service Manager**	**Information Security Manager**	**Privacy Officer**
BAI09.01 Identify and record current assets.		A			R	R			
BAI09.02 Manage critical assets.		A	R	R	R	R		R	R
BAI09.03 Manage the asset life cycle.		A			R	R	R		
BAI09.04 Optimize asset value.	A	R	R	R	R	R	R		
BAI09.05 Manage licenses.	A	R		R	R	R			
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**								
No related guidance for this component									

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
BAI09.01 Identify and record current assets.	**From**	**Description**	**Description**	**To**
	BAI03.04	Updates to asset inventory	Results of fit-for-purpose reviews	APO02.02
	BAI10.02	Configuration repository	Asset register	APO06.01; BAI10.03
			Results of physical inventory checks	BAI10.03; BAI10.04; DSS05.03
BAI09.02 Manage critical assets.			Communications of planned maintenance downtime	APO08.04
			Maintenance agreements	Internal
BAI09.03 Manage the asset life cycle.			Authorized asset retirements	BAI10.03
			Updated asset register	BAI10.03
			Approved asset procurement requests	Internal
BAI09.04 Optimize asset value.			Opportunities to reduce asset costs or increase value	APO02.02
			Results of cost-optimization reviews	APO02.02
BAI09.05 Manage licenses.			Action plan to adjust license numbers and allocations	APO02.05
			Register of software licenses	BAI10.02
			Results of installed license audits	MEA03.03
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
No related guidance for this component				

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Asset management	Skills Framework for the Information Age V6, 2015	ASMG
Systems installation/ decommissioning	Skills Framework for the Information Age V6, 2015	HSIN

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Asset management policy	Provides guidelines for asset life cycle management, asset protection measures, system classification and ownership, data ownership, and data classification		
Intellectual property (IP) policy	Addresses risk related to use, ownership, sale and distribution of the outputs of I&T-related creative endeavors by employees (e.g., software development). Mandates appropriate documentation, level of detail, etc., from inception of work.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Establish a culture that identifies, assesses, and reports the relative economic and strategic value of each asset to the enterprise in an open, consistent and transparent manner.		

G. Component: Services, Infrastructure and Applications
Asset management tools

Domain: Build, Acquire and Implement Management Objective: BAI10 — Managed Configuration	Focus Area: COBIT Core Model

Description

Define and maintain descriptions and relationships among key resources and capabilities required to deliver I&T-enabled services. Include collecting configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository.

Purpose

Provide sufficient information about service assets to enable the service to be effectively managed. Assess the impact of changes and deal with service incidents.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG02 Managed business risk • EG06 Business service continuity and availability	AG07 Security of information, processing infrastructure and applications, and privacy

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG02	a. Percent of critical business objectives and services covered by risk assessment b. Ratio of significant incidents that were not identified in risk assessments vs. total incidents c. Frequency of updating risk profile	AG07	a. Number of confidentiality incidents causing financial loss, business disruption or public embarrassment b. Number of availability incidents causing financial loss, business disruption or public embarrassment c. Number of integrity incidents causing financial loss, business disruption or public embarrassment
EG06	a. Number of customer service or business process interruptions causing significant incidents b. Business cost of incidents c. Number of business processing hours lost due to unplanned service interruptions d. Percent of complaints as a function of committed service availability targets		

A. Component: Process

Management Practice	Example Metrics
BAI10.01 Establish and maintain a configuration model. Establish and maintain a logical model of the services, assets, infrastructure and recording of configuration items (CIs), including the relationships among them. Include the CIs considered necessary to manage services effectively and to provide a single, reliable description of the assets in a service.	a. Number of stakeholders signing off on the configuration model b. Percent of accuracy of relationships of configuration items

Activities	Capability Level
1. Define and agree on the scope and level of detail for configuration management (i.e., which services, assets and infrastructure configurable items to include).	3
2. Establish and maintain a logical model for configuration management, including information on CI types, attributes, relationship types, relationship attributes and status codes.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Data Management Maturity Model, 2014	Supporting Processes - Configuration Management
ISF, The Standard of Good Practice for Information Security 2016	SY1 System Configuration
ISO/IEC 20000-1:2011(E)	9.1 Configuration management
ITIL V3, 2011	Service Transition, 4.3 Service Asset and Configuration Management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.5 Configuration management (CM-6)

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI10.02 Establish and maintain a configuration repository and baseline. Establish and maintain a configuration management repository and create controlled configuration baselines.	a. Number of configuration items (CIs) listed in the repository b. Percent of accuracy of configuration baselines of a service, application or infrastructure
Activities	**Capability Level**
1. Identify and classify CIs and populate the repository.	2
2. Create, review and formally agree on configuration baselines of a service, application or infrastructure.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	IP.CB Apply Configuration Baselines
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.4 Implementation (Task 2)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.19 System and service acquisition (SA-10)
Management Practice	**Example Metrics**
BAI10.03 Maintain and control configuration items. Maintain an up-to-date repository of configuration items (CIs) by populating any configuration changes.	a. Frequency of changes/updates to the repository b. Percent of accuracy and completeness of CIs repository
Activities	**Capability Level**
1. Regularly identify all changes to CIs.	2
2. To ensure completeness and accuracy, review proposed changes to CIs against the baseline.	
3. Update configuration details for approved changes to CIs.	
4. Create, review and formally agree on changes to configuration baselines whenever needed.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.5 Configuration management (CM-2)
Management Practice	**Example Metrics**
BAI10.04 Produce status and configuration reports. Define and produce configuration reports on status changes of configuration items.	a. Number of identified unauthorized changes b. Percent of accuracy of status changes of CIs against the baseline
Activities	**Capability Level**
1. Identify status changes of CIs and report against the baseline.	2
2. Match all configuration changes with approved requests for change to identify any unauthorized changes. Report unauthorized changes to change management.	3
3. Identify reporting requirements from all stakeholders, including content, frequency and media. Produce reports according to the identified requirements.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.5 Configuration management (CM-3)
Management Practice	**Example Metrics**
BAI10.05 Verify and review integrity of the configuration repository. Periodically review the configuration repository and verify completeness and correctness against the desired target.	a. Number of deviations between the configuration repository and live configuration b. Number of discrepancies relating to incomplete or missing configuration information

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Periodically verify live configuration items against the configuration repository by comparing physical and logical configurations and using appropriate discovery tools, as required.	4
2. Report and review all deviations for approved corrections or action to remove any unauthorized assets.	
3. Periodically verify that all physical configuration items, as defined in the repository, physically exist. Report any deviations to management.	
4. Set and periodically review the target for completeness of the configuration repository based on business need.	
5. Periodically compare the degree of completeness and accuracy against targets and take remedial action, as necessary, to improve the quality of the repository data.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.5 Configuration management (CM-4)

B. Component: Organizational Structures									
Key Management Practice	Chief Information Officer	Chief Technology Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	
BAI10.01 Establish and maintain a configuration model.		A			R	R	R		
BAI10.02 Establish and maintain a configuration repository and baseline.		A		R	R	R	R	R	
BAI10.03 Maintain and control configuration items.	A	R		R	R	R			
BAI10.04 Produce status and configuration reports.		A			R	R			
BAI10.05 Verify and review integrity of the configuration repository.		A	R	R	R		R		

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
BAI10.01 Establish and maintain a configuration model.	**From**	**Description**	**Description**	**To**
	BAI07.06	Release plan	Logical configuration model	Internal
			Scope of configuration management model	Internal
BAI10.02 Establish and maintain a configuration repository and baseline.	BAI09.05	Register of software licenses	Configuration baseline	BAI03.11; BAI03.12
			Configuration repository	BAI09.01; DSS02.01
BAI10.03 Maintain and control configuration items.	BAI06.03	Change request status reports	Approved changes to baseline	BAI03.11
	BAI09.01	• Asset register • Results of physical inventory checks	Updated repository with CIs	DSS02.01
	BAI09.03	• Updated asset register • Authorized asset retirements		
BAI10.04 Produce status and configuration reports.	BAI09.01	Results of physical inventory checks	Configuration status reports	BAI03.11; DSS02.01
BAI10.05 Verify and review integrity of the configuration repository.			Results of repository completeness reviews	Internal
			Results of physical verification of CIs	Internal
			License deviations	MEA03.03

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.4 Implementation (Task 2): Inputs and Outputs

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Configuration management	Skills Framework for the Information Age V6, 2015	CFMG

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Configuration management policy	Communicates guidance for establishing and using a comprehensive configuration repository, including all technology components, associated configuration definitions and interdependencies with other technology components. Helps ensure that system and software changes are minimally disruptive to services. Ensures that changes are coordinated among applicable groups, so conflicts or duplication of effort do not occur.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Establish a culture that supports a structured approach to configuration management across departments in which users recognize the value of strict configuration management (e.g., avoiding version conflicts or duplicative effort) and apply the rules and procedures that were put in place.		

G. Component: Services, Infrastructure and Applications
Configuration management tools and repositories

Page intentionally left blank

Domain: Build, Acquire and Implement Management objective: BAI11 — Managed Projects	Focus Area: COBIT Core Model

Description

Manage all projects that are initiated within the enterprise in alignment with enterprise strategy and in a coordinated way based on the standard project management approach. Initiate, plan, control and execute projects, and close with a post-implementation review.

Purpose

Realize defined project outcomes and reduce the risk of unexpected delays, costs and value erosion by improving communications to and involvement of business and end users. Ensure the value and quality of project deliverables and maximize their contribution to the defined programs and investment portfolio.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG08 Optimization of internal business process functionality • EG12 Managed digital transformation programs	• AG03 Realized benefits from I&T-enabled investments and services portfolio • AG06 Agility to turn business requirements into operational solutions • AG09 Delivering programs on time, on budget and meeting requirements and quality standards

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG01	a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG03	a. Percent of I&T-enabled investments for which claimed benefits in the business case are met or exceeded b. Percent of I&T services for which expected benefits (as stated in service level agreements) are realized
EG08	a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities	AG06	a. Level of satisfaction of business executives with I&T responsiveness to new requirements b. Average time to market for new I&T-related services and applications c. Average time to turn strategic I&T objectives into agreed and approved initiatives d. Number of critical business processes supported by up-to-date infrastructure and applications
EG12	a. Number of programs on time and within budget b. Percent of stakeholders satisfied with program delivery c. Percent of business transformation programs stopped d. Percent of business transformation programs with regular reported status updates	AG09	a. Number of programs/projects on time and within budget b. Number of programs needing significant rework due to quality defects c. Percent of stakeholders satisfied with program/project quality

A. Component: Process	
Management Practice	**Example Metrics**
BAI11.01 Maintain a standard approach for project management. Maintain a standard approach for project management that enables governance and management review, decision-making and delivery-management activities. These activities should focus consistently on business value and goals (i.e., requirements, risk, costs, schedule and quality targets).	a. Percent of successful projects based on the defined standard approach b. Number of updates to project management approach, good practices, tools and templates

Activities	Capability Level
1. Maintain and enforce a standard approach to project management aligned to the enterprise's specific environment and with good practice based on defined process and use of appropriate technology. Ensure that the approach covers the full life cycle and disciplines to be followed, including the management of scope, resources, risk, cost, quality, time, communication, stakeholder involvement, procurement, change control, integration and benefit realization.	2
2. Provide appropriate project management training and consider certification for project managers.	
3. Put in place a project management office (PMO) that maintains the standard approach for program and project management across the organization. The PMO supports all projects by creating and maintaining required project documentation templates, providing training and best practices for project managers, tracking metrics on the use of best practices for project management, etc. In some cases, the PMO may also report on project progress to senior management and/or stakeholders, help prioritize projects, and ensure all projects support the overall business objectives of the enterprise.	3
4. Evaluate lessons learned on the use of the project management approach. Update the good practices, tools and templates accordingly.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.15 Program management (PM-2)

Management Practice	Example Metrics
BAI11.02 Start up and initiate a project. Define and document the nature and scope of the project to confirm and develop a common understanding of project scope among stakeholders. The definition should be formally approved by the project sponsors.	a. Percent of stakeholders approving enterprise need, scope, planned outcome and level of project risk b. Percent of projects in which stakeholders received a clear written statement defining the nature, scope and benefit of the project

Activities	Capability Level
1. To create a common understanding of project scope among stakeholders, provide them a clear written statement defining the nature, scope and deliverables of every project.	2
2. Ensure that each project has one or more sponsors with sufficient authority to manage execution of the project within the overall program.	
3. Ensure that key stakeholders and sponsors within the enterprise (business and IT) agree on and accept the requirements for the project, including definition of project success (acceptance) criteria and key performance indicators (KPIs).	
4. Appoint a dedicated manager for the project. Ensure that the individual has the required understanding of technology and business and the commensurate competencies and skills to manage the project effectively and efficiently.	
5. Ensure that the project definition describes the requirements for a project communication plan that identifies internal and external project communications.	
6. With the approval of stakeholders, maintain the project definition throughout the project, reflecting changing requirements.	
7. To track the execution of a project, put in place mechanisms such as regular reporting and stage-gate, release or phase reviews, to occur in a timely manner and with appropriate approval.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PMBOK Guide Sixth Edition, 2017	Part 1: 4.1 Develop project charter; Part 1: 6. Project schedule management

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI11.03 Manage stakeholder engagement. Manage stakeholder engagement to ensure an active exchange of accurate, consistent and timely information that reaches all relevant stakeholders. This includes planning, identifying and engaging stakeholders and managing their expectations.	a. Level of stakeholder satisfaction with involvement b. Percent of stakeholders effectively engaged
Activities	**Capability Level**
1. Plan how stakeholders inside and outside the enterprise will be identified, analyzed, engaged and managed through the life cycle of the project.	3
2. Identify, engage and manage stakeholders by establishing and maintaining appropriate levels of co-ordination, communication and liaison to ensure they are involved in the project.	
3. Analyze stakeholder interests, requirements and engagement. Take remedial actions as required.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 13. Project stakeholder management Part 1: 10. Project communications management
Management Practice	**Example Metrics**
BAI11.04 Develop and maintain the project plan. Establish and maintain a formal, approved, integrated project plan (covering business and IT resources) to guide project execution and control throughout the life of the project. The scope of projects should be clearly defined and tied to building or enhancing business capability.	a. Percent of active projects undertaken without valid and updated project value maps b. Percent of milestone or task completion vs. plan
Activities	**Capability Level**
1. Develop a project plan that provides information to enable management to control project progress progressively. The plan should include details of project deliverables and acceptance criteria, required internal and external resources and responsibilities, clear work breakdown structures and work packages, estimates of resources required, milestones/release plan/phases, key dependencies, budget and costs, and identification of a critical path.	2
2. Maintain the project plan and any dependent plans (e.g., risk plan, quality plan, benefits realization plan). Ensure that the plans are up to date and reflect actual progress and approved material changes.	
3. Ensure that there is effective communication of project plans and progress reports. Ensure that any changes made to individual plans are reflected in other plans.	
4. Determine the activities, interdependencies and required collaboration and communication within the project and among multiple projects within a program.	
5. Ensure that each milestone is accompanied by a significant deliverable requiring review and sign-off.	
6. Establish a project baseline (e.g., cost, schedule, scope, quality) that is appropriately reviewed, approved and incorporated into the integrated project plan.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 4.2 Develop project management plan
Management Practice	**Example Metrics**
BAI11.05 Manage project quality. Prepare and execute a quality management plan, processes and practices that align with quality management standards (QMS). Describe the approach to project quality and implementation. The plan should be formally reviewed and agreed on by all parties concerned and incorporated into the integrated project plans.	a. Percent of build-to-products without errors b. Number of cancelled projects

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. To provide quality assurance for the project deliverables, identify ownership and responsibilities, quality review processes, success criteria and performance metrics.	2
2. Identify assurance tasks and practices required to support the accreditation of new or modified systems during project planning. Include them in the integrated plans. Ensure that the tasks provide assurance that internal controls and security and privacy solutions meet the defined requirements.	3
3. Define any requirements for independent validation and verification of the quality of deliverables in the plan.	
4. Perform quality assurance and control activities in accordance with the quality management plan and QMS.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 8. Project quality management
Management Practice	**Example Metrics**
BAI11.06 Manage project risk. Eliminate or minimize specific risk associated with projects through a systematic process of planning, identifying, analyzing, responding to, monitoring and controlling the areas or events with potential to cause unwanted change. Define and record any risk faced by project management.	a. Number of identified delays and issues b. Number of projects with a formal project risk management approach aligned with the ERM framework
Activities	**Capability Level**
1. Establish a formal project risk management approach aligned with the ERM framework. Ensure that the approach includes identifying, analyzing, responding to, mitigating, monitoring and controlling risk.	2
2. Assign to appropriately skilled personnel the responsibility for executing the enterprise's project risk management process within a project and ensure that this is incorporated into the solution development practices. Consider allocating this role to an independent team, especially if an objective viewpoint is required or a project is considered critical.	
3. Identify owners for actions to avoid, accept or mitigate risk.	
4. Perform the project risk assessment of identifying and quantifying risk continuously throughout the project. Manage and communicate risk appropriately within the project governance structure.	3
5. Reassess project risk periodically, including at initiation of each major project phase and as part of major change request assessments.	
6. Maintain and review a project risk register of all potential project risk and a risk mitigation log of all project issues and their resolution. Analyze the log periodically for trends and recurring problems to ensure that root causes are corrected.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.15 Program management (PM-4)
PMBOK Guide Sixth Edition, 2017	Part 1: 11. Project risk management
Management Practice	**Example Metrics**
BAI11.07 Monitor and control projects. Measure project performance against key project performance criteria such as schedule, quality, cost and risk. Identify any deviations from expected targets. Assess the impact of deviations on the project and overall program and report results to key stakeholders.	a. Percent of activities aligned to scope and expected outcomes b. Percent of deviations from plan addressed c. Frequency of project status reviews

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Establish and use a set of project criteria including, but not limited to, scope, expected business benefit, schedule, quality, cost and level of risk.	2
2. Report to identified key stakeholders project progress within the project, deviations from established key project performance criteria (such as, but not limited to, the expected business benefits), and potential positive and negative effects on the project.	
3. Document and submit any necessary changes to the project's key stakeholders for their approval before adoption. Communicate revised criteria to project managers for use in future performance reports.	
4. For the deliverables produced in each iteration, release or project phase, gain approval and sign-off from designated managers and users in the affected business and IT functions.	
5. Base the approval process on clearly defined acceptance criteria agreed on by key stakeholders before work commences on the project phase or iteration deliverable.	3
6. Assess the project at agreed major stage-gates, releases or iterations. Make formal go/no-go decisions based on predetermined critical success criteria.	
7. Establish and operate a change control system for the project so that all changes to the project baseline (e.g., scope, expected business benefits, schedule, quality, cost, risk level) are appropriately reviewed, approved and incorporated into the integrated project plan in line with the program and project governance framework.	
8. Measure project performance against key project performance criteria. Analyze deviations from established key project performance criteria for cause and assess positive and negative effects on the project.	4
9. Monitor changes to the project and review existing key project performance criteria to determine whether they still represent valid measures of progress.	
10. Recommend and monitor remedial action, when required, in line with the project governance framework.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 4.5 Monitor and control project work
Management Practice	**Example Metrics**
BAI11.08 Manage project resources and work packages. Manage project work packages by placing formal requirements on authorizing and accepting work packages and assigning and coordinating appropriate business and IT resources.	a. Number of resource issues (e.g., skills, capacity) b. Number of clearly defined roles, responsibilities and prerogatives of project manager, assigned staff and other involved parties
Activities	**Capability Level**
1. Identify business and IT resource needs for the project and clearly map appropriate roles and responsibilities, with escalation and decision-making authorities agreed and understood.	2
2. Identify required skills and time requirements for all individuals involved in the project phases in relation to defined roles. Staff the roles based on available skills information (e.g., IT skills matrix).	
3. Utilize experienced project management and team leader resources with skills appropriate to the size, complexity and risk of the project.	
4. Consider and clearly define the roles and responsibilities of other involved parties, including finance, legal, procurement, HR, internal audit and compliance.	
5. Clearly define and agree on the responsibility for procurement and management of third-party products and services, and manage the relationships.	
6. Identify and authorize the execution of the work according to the project plan.	
7. Identify project plan gaps and provide feedback to the project manager to remediate.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 4.3 Direct and manage project work

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI11.09 Close a project or iteration. At the end of each project, release or iteration, require the project stakeholders to ascertain whether the project, release or iteration delivered the required results in terms of capabilities and contributed as expected to program benefits. Identify and communicate any outstanding activities required to achieve planned results of the project and/or benefits of the program. Identify and document lessons learned for future projects, releases, iterations and programs.	a. Level of stakeholder satisfaction expressed at project closure review b. Percent of outcomes with first-time acceptance

Activities	Capability Level
1. Obtain stakeholder acceptance of project deliverables and transfer ownership.	2
2. Define and apply key steps for project closure, including post-implementation reviews that assess whether a project attained desired results.	3
3. Plan and execute post-implementation reviews to determine whether projects delivered expected results. Improve the project management and system development process methodology.	
4. Identify, assign, communicate and track any uncompleted activities required to ensure the project delivered the required results in terms of capabilities and the results contributed as expected to the program benefits.	
5. Regularly, and upon completion of the project, collect lessons learned from the project participants. Review them and the key activities that led to delivered benefits and value. Analyze the data and make recommendations for improving the current project and the project management method for future projects.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PMBOK Guide Sixth Edition, 2017	Part 1: 4.7 Close project or phase

B. Component: Organizational Structures

Key Management Practice	Chief Executive Officer	Chief Risk Officer	Chief Information Officer	Chief Technology Officer	Business Process Owners	Steering (Programs/Projects) Committee	Program Manager	Project Manager	Project Management Office	Head Development	Information Security Manager
BAI11.01 Maintain a standard approach for project management.	A		R				R	R			
BAI11.02 Start up and initiate a project.		R		R	R	A	R	R	R	R	
BAI11.03 Manage stakeholder engagement.			R			A		R			
BAI11.04 Develop and maintain the project plan.						A		R	R		
BAI11.05 Manage project quality.		R	R			A		R			R
BAI11.06 Manage project risk.			R			A		R			R
BAI11.07 Monitor and control projects.					R	A		R	R	R	
BAI11.08 Manage project resources and work packages.					R	A	R		R	R	
BAI11.09 Close a project or iteration.						A		R	R		

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PMBOK Guide Sixth Edition, 2017	Part 1: 3. The role of the project manager

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
BAI11.01 Maintain a standard approach for project management.	APO03.04	• Architecture governance requirements • Implementation phase descriptions	Updated project management approaches	Internal
	APO10.04	Identified vendor delivery risk		
	EDM02.03	Requirements for stage-gate reviews		
	EDM02.04	Actions to improve value delivery		
BAI11.02 Start up and initiate a project.			Project definitions	Internal
			Project scope statements	Internal
BAI11.03 Manage stakeholder engagement.			Results of stakeholder engagement effectiveness assessments	Internal
			Stakeholder engagement plan	Internal
BAI11.04 Develop and maintain the project plan.	BAI07.03	Approved acceptance test plan	Project reports and communications	Internal
			Project baseline	Internal
			Project plans	Internal
BAI11.05 Manage project quality.	APO11.01	Quality management plans	Project quality management plan	BAI02.04; BAI03.06; BAI07.01
	APO11.02	Customer requirements for quality management	Requirements for independent verification of project deliverables	BAI07.03
BAI11.06 Manage project risk.	APO12.02	Risk analysis results	Project risk register	Internal
	BAI02.03	• Requirements risk register • Risk mitigation actions	Project risk assessment results	Internal
	Outside COBIT	Enterprise risk management (ERM) framework	Project risk management plan	Internal
BAI11.07 Monitor and control projects.			Agreed changes to project	Internal
			Project progress reports	Internal
			Project performance criteria	Internal
BAI11.08 Manage project resources and work packages.			Project resource requirements	APO07.05; APO07.06
			Gaps in project planning	Internal
			Project roles and responsibilities	Internal

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI11.09 Close a project or iteration.	**From**	**Description**	**Description**	**To**
	BAI07.08	• Post-implementation review report • Remedial action plan	Post-implementation review results	APO02.04
			Stakeholder project acceptance confirmations	Internal
			Project lessons learned	Internal
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
PMBOK Guide Sixth Edition, 2017		Part 1: 4. Project integration management: Inputs and Outputs; Part 1: 6. Project schedule management: Inputs and Outputs; Part 1: 10. Project communications management: Inputs & Outputs; Part 1: 11. Project risk management: Inputs and Outputs		

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Portfolio, program and project support	Skills Framework for the Information Age V6, 2015	PROF
Project and portfolio management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.2. Project and Portfolio Management
Project management	Skills Framework for the Information Age V6, 2015	PRMG

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Program/project management policy	Guides management of risk related to programs and projects. Details management position and expectation regarding program and project management. Treats accountability, goals and objectives regarding performance, budget, risk analysis, reporting and mitigation of adverse events during program/project execution.	PMBOK guide Sixth edition, 2017	Part 1: 2.3.1 Processes, policies and procedures

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Establish an enterprisewide project management culture that ensures consistent and optimal implementation of project management across the enterprise, taking into account organizational structure and business environment. Ensure that all initiatives are translated into projects (or changes, where minor in scope); ensure that no ad hoc actions occur outside the scope of project management.		

G. Component: Services, Infrastructure and Applications
Project management tools

4.4 Deliver, Service and Support (DSS)

01 Managed Operations

02 Managed Service Requests and Incidents

03 Managed Problems

04 Managed Continuity

05 Managed Security Services

06 Managed Business Process Controls

Page intentionally left blank

Domain: Deliver, Service and Support Management Objective: DSS01 - Managed Operations	Focus Area: COBIT Core Model

Description

Coordinate and execute the activities and operational procedures required to deliver internal and outsourced I&T services. Include the execution of predefined standard operating procedures and the required monitoring activities.

Purpose

Deliver I&T operational product and service outcomes as planned.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG08 Optimization of internal business process functionality	AG05 Delivery of I&T services in line with business requirements
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG01 a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG05 a. Percent of business stakeholders satisfied that I&T service delivery meets agreed service levels b. Number of business disruptions due to I&T service incidents c. Percent of users satisfied with the quality of I&T service delivery
EG08 a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities	

A. Component: Process

Management Practice	Example Metrics
DSS01.01 Perform operational procedures. Maintain and perform operational procedures and operational tasks reliably and consistently.	a. Number of incidents caused by operational problems b. Number of nonstandard operational procedures executed

Activities	Capability Level
1. Develop and maintain operational procedures and related activities to support all delivered services.	2
2. Maintain a schedule of operational activities and perform the activities.	
3. Verify that all data expected for processing are received and processed completely, accurately and in a timely manner. Deliver output in accordance with enterprise requirements. Support restart and reprocessing needs. Ensure that users are receiving the right outputs in a secure and timely manner.	3
4. Manage the performance and throughput of the scheduled activities.	4
5. Monitor incidents and problems dealing with operational procedures and take appropriate action to improve reliability of operational tasks performed.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	TP.SE Safeguard Operational Environment
HITRUST CSF version 9, September 2017	09.01 Document Operating Procedures
ISO/IEC 27002:2013/Cor.2:2015(E)	12.1 Operational procedures and responsibilities
ITIL V3, 2011	Service Operation, 4.1 Event Management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.13 Physical and environmental protection (PE-13, PE-14, PE-15)

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
DSS01.02 Manage outsourced I&T services. Manage the operation of outsourced I&T services to maintain the protection of enterprise information and reliability of service delivery.	a. Number of specific/smart KPIs included in outsourcing contracts b. Frequency of failure by outsourcing partner to meet KPIs

Activities	Capability Level
1. Ensure that the enterprise's requirements for security of information processes adhere to contracts and SLAs with third parties hosting or providing services.	3
2. Ensure that the enterprise's operational business and IT processing requirements and priorities for service delivery adhere to contracts and SLAs with third parties hosting or providing services.	
3. Integrate critical internal IT management processes with those of outsourced service providers. This should cover, for example, performance and capacity planning, change management, configuration management, service request and incident management, problem management, security management, business continuity, and the monitoring of process performance and reporting.	
4. Plan for independent audit and assurance of the operational environments of outsourced providers to confirm that agreed requirements are being adequately addressed.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISF, The Standard of Good Practice for Information Security 2016	SC1.2 Outsourcing
ISO/IEC 20000-1:2011(E)	4.2 Governance of processes operated by other parties

Management Practice	Example Metrics
DSS01.03 Monitor I&T infrastructure. Monitor the I&T infrastructure and related events. Store sufficient chronological information in operations logs to reconstruct and review time sequences of operations and other activities surrounding or supporting operations.	a. Percent of critical operational event types covered by automatic detection systems b. Percent of infrastructure assets monitored based on service criticality and the relationship between configuration items and services that depend on them

Activities	Capability Level
1. Log events. Identify the level of information to be recorded, based on a consideration of risk and performance.	2
2. Identify and maintain a list of infrastructure assets that need to be monitored, based on service criticality and the relationship between configuration items and services that depend on them.	3
3. Define and implement rules that identify and record threshold breaches and event conditions. Find a balance between generating spurious minor events and significant events so event logs are not overloaded with unnecessary information.	
4. Produce event logs and retain them for an appropriate period to assist in future investigations.	
5. Ensure that incident tickets are created in a timely manner when monitoring identified deviations from defined thresholds.	
6. Establish procedures for monitoring event logs. Conduct regular reviews.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.10 Maintenance (MA-2, MA-3)

Management Practice	Example Metrics
DSS01.04 Manage the environment. Maintain measures for protection against environmental factors. Install specialized equipment and devices to monitor and control the environment.	a. Number of people trained to respond to environmental alarm procedures b. Number of risk scenarios defined for environmental threats

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Identify natural and man-made disasters that might occur in the area where the IT facilities are located. Assess the potential effect on the IT facilities.	2
2. Identify how I&T equipment, including mobile and off-site equipment, is protected against environmental threats. Ensure that the policy limits or excludes eating, drinking and smoking in sensitive areas, and prohibits storage of stationery and other supplies that pose a fire hazard within computer rooms.	
3. Keep the IT sites and server rooms clean and in a safe condition at all times (i.e., no mess, no paper or cardboard boxes, no filled dustbins, no flammable chemicals or materials).	
4. Situate and construct IT facilities to minimize and mitigate susceptibility to environmental threats (e.g., theft, air, fire, smoke, water, vibration, terror, vandalism, chemicals, explosives). Consider specific security zones and/or fireproof cells (e.g., locating production and development environments/servers away from each other).	3
5. Compare measures and contingency plans against insurance policy requirements and report results. Address points of noncompliance in a timely manner.	
6. Respond to environmental alarms and other notifications. Document and test procedures, which should include prioritization of alarms and contact with local emergency response authorities. Train personnel in these procedures.	
7. Regularly monitor and maintain devices that proactively detect environmental threats (e.g., fire, water, smoke, humidity).	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	2.1 System and system elements; 3.2 Categorization (Task 5, 6)
Management Practice	**Example Metrics**
DSS01.05 Manage facilities. Manage facilities, including power and communications equipment, in line with laws and regulations, technical and business requirements, vendor specifications, and health and safety guidelines.	a. Time since last test of uninterruptible power supply b. Number of people trained on health and safety guidelines
Activities	**Capability Level**
1. Examine the IT facilities' requirement for protection against power fluctuations and outages, in conjunction with other business continuity planning requirements. Procure suitable uninterruptible supply equipment (e.g., batteries, generators) to support business continuity planning.	2
2. Regularly test the uninterruptible power supply's mechanisms. Ensure that power can be switched to the supply without any significant effect on business operations.	
3. Ensure that the facilities housing the I&T systems have more than one source for dependent utilities (e.g., power, telecommunications, water, gas). Separate the physical entrance of each utility.	
4. Confirm that cabling external to the IT site is located underground or has suitable alternative protection. Determine that cabling within the IT site is contained within secured conduits, and access to wiring cabinets is restricted to authorized personnel. Properly protect cabling against damage caused by fire, smoke, water, interception and interference.	
5. Ensure that cabling and physical patching (data and phone) are structured and organized. Cabling and conduit structures should be documented (e.g., blueprint building plan and wiring diagrams).	
6. On regular basis, educate personnel on health and safety laws, regulations, and relevant guidelines. Educate personnel on fire and rescue drills to ensure knowledge and actions taken in case of fire or similar incidents.	
7. Ensure that IT sites and equipment are maintained according to the supplier's recommended service intervals and specifications. Ensure that maintenance is carried out only by authorized personnel.	3
8. Analyze the facilities housing's high-availability systems for redundancy and fail-over cabling requirements (external and internal).	
9. Ensure that IT sites and facilities are in ongoing compliance with relevant health and safety laws, regulations, guidelines, and vendor specifications.	
10. Record, monitor, manage and resolve facilities incidents in line with the I&T incident management process. Make available reports on facilities incidents for which disclosure is required by laws and regulations.	4
11. Analyze physical alterations to IT sites or premises to reassess the environmental risk (e.g., fire or water damage). Report results of this analysis to business continuity and facilities management.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

B. Component: Organizational Structures

Key Management Practice	Chief Operating Officer	Chief Information Officer	Chief Technology Officer	Head IT Operations	Information Security Manager	Privacy Officer
DSS01.01 Perform operational procedures.	R	A	R	R		
DSS01.02 Manage outsourced I&T services.		A	R	R	R	R
DSS01.03 Monitor I&T infrastructure.		R	A	R	R	
DSS01.04 Manage the environment.		R	A	R	R	
DSS01.05 Manage facilities.		R	A	R	R	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)

Management Practice	Inputs		Outputs	
	From	Description	Description	To
DSS01.01 Perform operational procedures.	BAI05.05	Operation and use plan	Backup log	Internal
			Operational schedule	Internal
DSS01.02 Manage outsourced I&T services.	APO09.03	• SLAs • OLAs	Independent assurance plans	MEA04.02
	BAI05.05	Operation and use plan		
DSS01.03 Monitor I&T infrastructure.	BAI03.11	Service definitions	Asset monitoring rules and event conditions	DSS02.01; DSS02.02
			Incident tickets	DSS02.02
			Event logs	Internal
DSS01.04 Manage the environment.			Environmental policies	APO01.09
			Insurance policy reports	MEA03.03
DSS01.05 Manage facilities.			Health and safety awareness	Internal
			Facilities assessment reports	MEA01.03

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.2 Categorization (Task 5, 6): Inputs and Outputs

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Database administration	Skills Framework for the Information Age V6, 2015	DBAD
Facilities management	Skills Framework for the Information Age V6, 2015	DCMA
IT infrastructure	Skills Framework for the Information Age V6, 2015	ITOP
Methods and tools	Skills Framework for the Information Age V6, 2015	METL
Service delivery	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	C. Run—C.3. Service Delivery
Storage management	Skills Framework for the Information Age V6, 2015	STMG

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Service management policy	Provides direction and guidance to ensure effective management and implementation of all I&T services to meet business and customer requirements, within a framework of performance measurement. Covers management of risk related to I&T services. (The ITIL V3 framework offers detailed guidance on service management and optimization of risk related to services.)	(1) ISO/IEC 20000-1:2011(E); (2) ITIL V3, 2011	(1) 4.1.2 Service management policy; (2) Service Strategy, 3. Service strategy principles

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Create a culture of habitual excellence throughout the organization. Encourage employees to excel. Create an environment in which operational procedures deliver (more than) the necessary services while also allowing employees to question the status quo and try new ideas. Manage operational excellence through employee engagement and continuous improvement. Apply a customer-centric approach (for both internal and external customers).		

G. Component: Services, Infrastructure and Applications
• Cloud hosting services • Infrastructure monitoring tools • Service level monitoring tools

Page intentionally left blank

Domain: Deliver, Service and Support Management Objective: DSS02 - Managed Service Requests and Incidents	Focus Area: COBIT Core Model

Description

Provide timely and effective response to user requests and resolution of all types of incidents. Restore normal service; record and fulfil user requests; and record, investigate, diagnose, escalate and resolve incidents.

Purpose

Achieve increased productivity and minimize disruptions through quick resolution of user queries and incidents. Assess the impact of changes and deal with service incidents. Resolve user requests and restore service in response to incidents.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG08 Optimization of internal business process functionality	AG05 Delivery of I&T services in line with business requirements
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG01 a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG05 a. Percent of business stakeholders satisfied that I&T service delivery meets agreed service levels b. Number of business disruptions due to I&T service incidents c. Percent of users satisfied with the quality of I&T service delivery
EG08 a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities	

A. Component: Process

Management Practice	Example Metrics
DSS02.01 Define classification schemes for incidents and service requests. Define classification schemes and models for incidents and service requests.	a. Total number of service requests and incidents per priority level b. Total number of incidents escalated

Activities	Capability Level
1. Define incident and service request classification and prioritization schemes, and criteria for problem registration. Use this information to ensure consistent approaches for handling and informing users about problems and conducting trend analysis.	3
2. Define incident models for known errors to enable efficient and effective resolution.	
3. Define service request models according to service request type to enable self-help and efficient service for standard requests.	
4. Define incident escalation rules and procedures, especially for major incidents and security incidents.	
5. Define knowledge sources on incidents and requests and describe how to use them.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	IA.IP Implement Incident Investigation Processes
HITRUST CSF version 9, September 2017	11.01 Reporting Information Security Incidents and Weaknesses
ISF, The Standard of Good Practice for Information Security 2016	TM2 Security Incident Management
ISO/IEC 20000-1:2011(E)	8.1 Incident and service request management
ISO/IEC 27002:2013/Cor.2:2015(E)	16. Information security incident management

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
DSS02.02 Record, classify and prioritize requests and incidents. Identify, record and classify service requests and incidents and assign a priority according to business criticality and service agreements.	a. Number of types and categories defined for recording service requests and incidents b. Number of service requests and incidents that are not categorized
Activities	**Capability Level**
1. Log all service requests and incidents, recording all relevant information, so they can be handled effectively and a full historical record can be maintained.	2
2. To enable trend analysis, classify service requests and incidents by identifying type and category.	
3. Prioritize service requests and incidents based on the SLA service definition of business impact and urgency.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
DSS02.03 Verify, approve and fulfill service requests. Select the appropriate request procedures and verify that the service requests fulfill defined request criteria. Obtain approval, if required, and fulfill the requests.	a. Mean elapsed time for handling each type of service request b. Percent of service requests that fulfill defined request criteria
Activities	**Capability Level**
1. Verify entitlement for service requests using, where possible, a predefined process flow and standard changes.	2
2. Obtain financial and functional approval or sign-off, if required, or predefined approvals for agreed standard changes.	
3. Fulfill the requests by performing the selected request procedure. Where possible, use self-help automated menus and predefined request models for frequently requested items.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ITIL V3, 2011	Service Operation, 4.3 Request Fulfilment
Management Practice	**Example Metrics**
DSS02.04 Investigate, diagnose and allocate incidents. Identify and record incident symptoms, determine possible causes, and allocate for resolution.	a. Number of identified and recorded incident symptoms b. Number of correctly determined symptom causes c. Number of duplicate problems in the reference log
Activities	**Capability Level**
1. Identify and describe relevant symptoms to establish the most probable causes of the incidents. Reference available knowledge resources (including known errors and problems) to identify possible incident resolutions (temporary workarounds and/or permanent solutions).	2
2. If a related problem or known error does not already exist and if the incident satisfies agreed criteria for problem registration, log a new problem.	
3. Assign incidents to specialist functions if deeper expertise is needed. Engage the appropriate level of management, where and if needed.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
DSS02.05 Resolve and recover from incidents. Document, apply and test the identified solutions or workarounds. Perform recovery actions to restore the I&T-related service.	a. Percent of incidents resolved within agreed SLA b. Percent of stakeholder satisfaction with resolution and recovery from incident
Activities	**Capability Level**
1. Select and apply the most appropriate incident resolutions (temporary workaround and/or permanent solution).	2
2. Record whether workarounds were used for incident resolution.	
3. Perform recovery actions, if required.	
4. Document incident resolution and assess if the resolution can be used as a future knowledge source.	

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ITIL V3, 2011	Service Operation, 4.2 Incident Management
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	RC.RP Recovery Planning
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.9 Incident response (IR-4, IR-5, IR-6)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 201	CSC 19: Incident Response and Management
Management Practice	**Example Metrics**
DSS02.06 Close service requests and incidents. Verify satisfactory incident resolution and/or fulfilment of requests, and close.	a. Level of user satisfaction with service request fulfilment b. Percent of incidents resolved within an agreed/acceptable period of time
Activities	**Capability Level**
1. Verify with the affected users that the service request has been fulfilled satisfactorily or the incident has been resolved satisfactorily and within an agreed/acceptable period of time.	2
2. Close service requests and incidents.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
DSS02.07 Track status and produce reports. Regularly track, analyze and report incidents and fulfilment of requests. Examine trends to provide information for continual improvement.	a. Mean time between incidents for the I&T-enabled service b. Number and percent of incidents causing disruption to business-critical processes
Activities	**Capability Level**
1. Monitor and track incident escalations and resolutions and request handling procedures to progress toward resolution or completion.	2
2 Identify information stakeholders and their needs for data or reports. Identify reporting frequency and medium.	3
3. Produce and distribute timely reports or provide controlled access to online data.	4
4. Analyze incidents and service requests by category and type. Establish trends and identify patterns of recurring issues, SLA breaches or inefficiencies.	
5. Use the information as input to continual improvement planning.	5
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	MI.IM Ensure Incident Mitigation; IR.IR Incident Reporting
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.9 Incident response (IR-7, IR-8)

B. Component: Organizational Structures							
Key Management Practice	Chief Technology Officer	Business Process Owners	Head Development	Head IT Operations	Service Manager	Information Security Manager
DSS02.01 Define classification schemes for incidents and service requests.	A		R	R	R	
DSS02.02 Record, classify and prioritize requests and incidents.	A			R	R	
DSS02.03 Verify, approve and fulfil service requests.	A	R	R	R	R	
DSS02.04 Investigate, diagnose and allocate incidents.	A	R		R	R	
DSS02.05 Resolve and recover from incidents.	A		R	R	R	R
DSS02.06 Close service requests and incidents.	A			R	R	R
DSS02.07 Track status and produce reports.	A			R	R	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISO/IEC 27002:2013/Cor.2:2015(E)	16.1.1 Responsibilities and procedures

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	Inputs		Outputs	
	From	Description	Description	To
DSS02.01 Define classification schemes for incidents and service requests.	APO09.03	SLAs	Criteria for problem registration	DSS03.01
	BAI10.02	Configuration repository	Rules for incident escalation	Internal
	BAI10.03	Updated repository with configuration items	Incident and service request classification schemes and models	Internal
	BAI10.04	Configuration status reports		
	DSS01.03	Asset monitoring rules and event conditions		
	DSS03.01	Problem classification scheme		
	DSS04.03	Incident response actions and communications		
DSS02.02 Record, classify and prioritize requests and incidents.	APO09.03	SLAs	Classified and prioritized incidents and service requests	APO08.03; APO09.04; APO13.03; DSS03.05
	BAI04.05	Emergency escalation procedure	Incident and service request log	Internal; MEA04.07
	DSS01.03	• Asset monitoring rules and event conditions • Incident tickets		
	DSS05.07	Security-related incident tickets		

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
DSS02.03 Verify, approve and fulfil service requests.	**From**	**Description**	**Description**	**To**
	APO12.06	Risk-related root causes	Approved service requests	BAI06.01
			Fulfilled service requests	Internal
DSS02.04 Investigate, diagnose and allocate incidents.	BAI07.07	Supplemental support plan	Problem log	DSS03.01
			Incident symptoms	Internal
DSS02.05 Resolve and recover from incidents.	APO12.06	Risk-related incident response plans	Incident resolutions	DSS03.03; DSS03.04; DSS03.05; MEA04.07
	DSS03.03	Known error records		
	DSS03.04	Communication of knowledge learned		
DSS02.06 Close service requests and incidents.	DSS03.04	Closed problem records	User confirmation of satisfactory fulfilment or resolution	APO08.03
			Closed service requests and incidents	APO08.03; APO09.04; DSS03.04
DSS02.07 Track status and produce reports.	APO09.03	OLAs	Incident status and trends report	APO08.03; APO09.04; APO11.04; APO12.01; MEA01.03
	DSS03.01	Problem status reports	Request fulfilment status and trends report	APO08.03; APO09.04; APO11.04; MEA01.03
	DSS03.02	Problem resolution reports		
	DSS03.05	Problem resolution monitoring reports		
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
No related guidance for this component				

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Application support	Skills Framework for the Information Age V6, 2015	ASUP
Customer service support	Skills Framework for the Information Age V6, 2015	CSMG
Incident management	Skills Framework for the Information Age V6, 2015	USUP
Network support	Skills Framework for the Information Age V6, 2015	NTAS
User support	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	C. Run—C.1. User Support

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Service request policy	States rationale and provides guidance for service and incident requests and their documentation.	ITIL V3, 2011	Service Operation, 3. Service operation principles

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Enable employees to identify incidents on a correct and timely basis and implement appropriate escalation paths. Encourage prevention. Respond to and resolve incidents immediately. Avoid a hero culture.		

G. Component: Services, Infrastructure and Applications
Incident tracking tools and system

Domain: Deliver, Service and Support Management Objective: DSS03 - Managed Problems	Focus Area: COBIT Core Model

Description

Identify and classify problems and their root causes. Provide timely resolution to prevent recurring incidents. Provide recommendations for improvements.

Purpose

Increase availability, improve service levels, reduce costs, improve customer convenience and satisfaction by reducing the number of operational problems, and identify root causes as part of problem resolution.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG08 Optimization of internal business process functionality	AG05 Delivery of I&T services in line with business requirements
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG01 a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG05 a. Percent of business stakeholders satisfied that I&T service delivery meets agreed service levels b. Number of business disruptions due to I&T service incidents c. Percent of users satisfied with the quality of I&T service delivery
EG08 a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities	

A. Component: Process

Management Practice	Example Metrics
DSS03.01 Identify and classify problems. Define and implement criteria and procedures to identify and report problems. Include problem classification, categorization and prioritization.	a. Percent of major incidents for which problems were logged b. Percent of incidents solved in accordance with agreed SLAs c. Percent of problems appropriately identified, including classification, categorization and prioritization

Activities	Capability Level
1. Identify problems through the correlation of incident reports, error logs and other problem identification resources.	2
2. Handle all problems formally with access to all relevant data. Include information from the IT change management system and IT configuration/asset and incident details.	
3. Define appropriate support groups to assist with problem identification, root cause analysis and solution determination to support problem management. Determine support groups based on predefined categories, such as hardware, network, software, applications and support software.	
4. Define priority levels through consultation with the business to ensure that problem identification and root cause analysis are handled in a timely manner according to the agreed SLAs. Base priority levels on business impact and urgency.	
5. Report the status of identified problems to the service desk so customers and IT management can be kept informed.	
6. Maintain a single problem management catalog to register and report problems identified. Use the catalog to establish audit trails of the problem management processes, including the status of each problem (i.e., open, reopen, in progress or closed).	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISO/IEC 20000-1:2011(E)	8.2 Problem management

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
DSS03.02 Investigate and diagnose problems. Investigate and diagnose problems using relevant subject matter experts to assess and analyze root causes.	a. Number of identified problems classified as known errors b. Percent of problems investigated and diagnosed throughout their life cycle

Activities	Capability Level
1. Identify problems that may be known errors by comparing incident data with the database of known and suspected errors (e.g., those communicated by external vendors). Classify problems as known errors.	3
2. Associate the affected configuration items to the established/known error.	
3. Produce reports to communicate the progress in resolving problems and to monitor the continuing impact of problems not solved. Monitor the status of the problem-handling process throughout its life cycle, including input from IT change and configuration management.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
DSS03.03 Raise known errors. As soon as root causes of problems are identified, create known-error records, document appropriate workarounds and identify potential solutions.	a. Number of problems with satisfactory resolution that addressed root causes b. Percent of stakeholder satisfaction with identification of root causes, creation of known-error records and appropriate workarounds, and identification of potential solutions

Activities	Capability Level
1. As soon as the root causes of problems are identified, create known-error records and develop a suitable workaround.	2
2. Identify, evaluate, prioritize and process (via IT change management) solutions to known errors, based on a cost/benefit business case and business impact and urgency.	3

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
DSS03.04 Resolve and close problems. Identify and initiate sustainable solutions addressing the root cause. Raise change requests via the established change management process, if required, to resolve errors. Ensure that the personnel affected are aware of the actions taken and the plans developed to prevent future incidents from occurring.	a. Decrease in number of recurring incidents caused by unresolved problems b. Percent of workarounds defined for open problems

Activities	Capability Level
1. Close problem records either after confirmation for successful elimination of the known error or after agreement with the business on how to alternatively handle the problem.	2
2. Inform the service desk of the schedule for problem closure (e.g., the schedule for fixing the known errors, the possible workaround or the fact that the problem will remain until the change is implemented) and the consequences of the approach taken. Keep affected users and customers informed as appropriate.	
3. Throughout the resolution process, obtain regular reports from IT change management on progress in resolving problems and errors.	3
4. Monitor the continuing impact of problems and known errors on services.	4
5. Review and confirm the success of resolutions of major problems.	
6. Make sure the knowledge learned from the review is incorporated into a service review meeting with the business customer.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
DSS03.05 Perform proactive problem management. Collect and analyze operational data (especially incident and change records) to identify emerging trends that may indicate problems. Log problem records to enable assessment.	a. Percent of problems logged as part of the proactive problem management activity b. Percent of key stakeholder satisfaction with the communication of problem information related to IT changes and incidents

Activities	Capability Level
1. Capture problem information related to I&T changes and incidents and communicate it to key stakeholders. Communicate via reports and periodic meetings among incident, problem, change and configuration management process owners to consider recent problems and potential corrective actions.	3
2. Ensure that process owners and managers from incident, problem, change and configuration management meet regularly to discuss known problems and future planned changes.	
3. Identify and initiate sustainable solutions (permanent fixes) addressing the root cause. Raise change requests via the established change management processes.	
4. To enable the enterprise to monitor the total costs of problems, capture change efforts resulting from problem management process activities (e.g., fixes to problems and known errors) and report on them.	4
5. Produce reports to monitor problem resolution against the business requirements and SLAs. Ensure the proper escalation of problems, such as escalating to a higher management level according to agreed criteria, contacting external vendors, or referring to the change advisory board to increase the priority of an urgent request for change (RFC) to implement a temporary workaround.	
6. To optimize the use of resources and reduce workarounds, track problem trends.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	MI.IC Ensure Incident Containment
ITIL V3, 2011	Service Operation, 4.4 Problem Management

B. Component: Organizational Structures

Key Management Practice	Executive Committee	Chief Information Officer	Chief Technology Officer	Head Development	Head IT Operations	Service Manager	Information Security Manager
DSS03.01 Identify and classify problems.		R	A	R	R	R	
DSS03.02 Investigate and diagnose problems.			A		R	R	R
DSS03.03 Raise known errors.			A		R	R	R
DSS03.04 Resolve and close problems.			A		R	R	
DSS03.05 Perform proactive problem management.	R		A		R	R	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
DSS03.01 Identify and classify problems.	**From**	**Description**	**Description**	**To**
	APO12.06	Risk-related root causes	Problem classification scheme	DSS02.01
	DSS02.01	Criteria for problem registration	Problem status reports	DSS02.07
	DSS02.04	Problem log	Problem register	Internal
DSS03.02 Investigate and diagnose problems.	APO12.06	Risk-related root causes	Problem resolution reports	DSS02.07
			Root causes of problems	Internal; DSS03.05
DSS03.03 Raise known errors.	APO12.06	Risk-related root causes	Proposed solutions to known errors	BAI06.01
	DSS02.05	Incident resolutions	Known error records	DSS02.05
DSS03.04 Resolve and close problems.	DSS02.05	Incident resolutions	Communication of knowledge learned	APO08.04; DSS02.05
	DSS02.06	Closed service requests and incidents	Closed problem records	DSS02.06
DSS03.05 Perform proactive problem management.	APO12.06	Risk-related root causes	Identified sustainable solutions	BAI06.01
	DSS02.02	• Classified and prioritized incidents and service requests • Incident resolutions	Problem resolution monitoring reports	DSS02.07, MEA04.07
	DSS03.04	Root causes of problems		
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
No related guidance for this component				

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Application support	Skills Framework for the Information Age V6, 2015	ASUP
Network support	Skills Framework for the Information Age V6, 2015	NTAS
Problem management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	C. Run—C.4. Problem Management
Problem management	Skills Framework for the Information Age V6, 2015	PBMG

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Problem resolution policy	Documents rationale and provides guidance for addressing problems that result from incidents and identifying validated workarounds.	ITIL V3, 2011	Service Operation, 3. Service operation principles

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Support a culture of proactive problem management (detection, action and prevention) with clearly defined roles and responsibilities. Ensure a transparent and open environment for reporting problems by providing independent reporting mechanisms and/or rewarding people who bring problems forward.		

G. Component: Services, Infrastructure and Applications
Problem tracking/resolution system

Page intentionally left blank

Domain: Deliver, Service and Support Management Objective: DSS04 - Managed Continuity	Focus Area: COBIT Core Model

Description

Establish and maintain a plan to enable the business and IT organizations to respond to incidents and quickly adapt to disruptions. This will enable continued operations of critical business processes and required I&T services and maintain availability of resources, assets and information at a level acceptable to the enterprise.

Purpose

Adapt rapidly, continue business operations and maintain availability of resources and information at a level acceptable to the enterprise in the event of a significant disruption (e.g., threats, opportunities, demands).

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG02 Managed business risk • EG06 Business service continuity and availability • EG08 Optimization of internal business process functionality	• AG05 Delivery of I&T services in line with business requirements • AG07 Security of information, processing infrastructure and applications, and privacy

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG01	a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG05	a. Percent of business stakeholders satisfied that I&T service delivery meets agreed service levels b. Number of business disruptions due to I&T service incidents c. Percent of users satisfied with the quality of I&T service delivery
EG02	a. Percent of critical business objectives and services covered by risk assessment b. Ratio of significant incidents that were not identified in risk assessments vs. total incidents c. Frequency of updating risk profile	AG07	a. Number of confidentiality incidents causing financial loss, business disruption or public embarrassment b. Number of availability incidents causing financial loss, business disruption or public embarrassment c. Number of integrity incidents causing financial loss, business disruption or public embarrassment
EG06	a. Number of customer service or business process interruptions causing significant incidents b. Business cost of incidents c. Number of business processing hours lost due to unplanned service interruptions d. Percent of complaints as a function of committed service availability targets		
EG08	a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities		

A. Component: Process	
Management Practice	**Example Metrics**
DSS04.01 Define the business continuity policy, objectives and scope. Define business continuity policy and scope, aligned with enterprise and stakeholder objectives, to improve business resilience.	a. Percent of business continuity objectives and scope reworked due to misidentified processes and activities b. Percent of key stakeholders participating, defining and agreeing on continuity policy and scope
Activities	**Capability Level**
1. Identify internal and outsourced business processes and service activities that are critical to the enterprise operations or necessary to meet legal and/or contractual obligations.	2
2. Identify key stakeholders and roles and responsibilities for defining and agreeing on continuity policy and scope.	
3. Define and document the agreed minimum policy objectives and scope for business resilience.	
4. Identify essential supporting business processes and related I&T services.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
HITRUST CSF version 9, September 2017	12.01 Information Security Aspects of Business Continuity Management
ISF, The Standard of Good Practice for Information Security 2016	BC1.1 Business Continuity Strategy; BC1.2 Business Continuity Programme
ISO/IEC 27002:2013/Cor.2:2015(E)	17. Information security aspects of business continuity management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.6 Contingency planning (CP-1)
Management Practice	**Example Metrics**
DSS04.02 Maintain business resilience. Evaluate business resilience options and choose a cost-effective and viable strategy that will ensure enterprise continuity, disaster recovery and incident response in the face of a disaster or other major incident or disruption.	a. Total downtime resulting from major incident or disruption b. Percent of key stakeholders involved in business impact analyses evaluating the impact over time of a disruption to critical business functions and the effect that a disruption would have on them
Activities	**Capability Level**
1. Identify potential scenarios likely to give rise to events that could cause significant disruptive incidents.	2
2. Conduct a business impact analysis to evaluate the impact over time of a disruption to critical business functions and the effect that a disruption would have on them.	
3. Establish the minimum time required to recover a business process and supporting I&T, based on an acceptable length of business interruption and maximum tolerable outage.	
4. Determine the conditions and owners of key decisions that will cause the continuity plans to be invoked.	
5. Assess the likelihood of threats that could cause loss of business continuity. Identify measures that will reduce the likelihood and impact through improved prevention and increased resilience.	3
6. Analyze continuity requirements to identify possible strategic business and technical options.	
7. Identify resource requirements and costs for each strategic technical option and make strategic recommendations.	
8. Obtain executive business approval for selected strategic options.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	BC1.3 Resilient Technical Environments
ITIL V3, 2011	Service Design, 4.6 IT Continuity Management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.6 Contingency planning (CP-2)

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
DSS04.03 Develop and implement a business continuity response. Develop a business continuity plan (BCP) and disaster recovery plan (DRP) based on the strategy. Document all procedures necessary for the enterprise to continue critical activities in the event of an incident.	a. Number of critical business systems not covered by the plan b. Percent of key stakeholders involved in developing BCPs and DRPs

Activities	Capability Level
1. Define the incident response actions and communications to be taken in the event of disruption. Define related roles and responsibilities, including accountability for policy and implementation.	2
2. Ensure that key suppliers and outsource partners have effective continuity plans in place. Obtain audited evidence as required.	
3. Define the conditions and recovery procedures that would enable resumption of business processing. Include updating and reconciliation of information databases to preserve information integrity.	
4. Develop and maintain operational BCPs and DRPs that contain the procedures to be followed to enable continued operation of critical business processes and/or temporary processing arrangements. Include links to plans of outsourced service providers.	
5. Define and document the resources required to support the continuity and recovery procedures, considering people, facilities and IT infrastructure.	
6. Define and document the information backup requirements required to support the plans. Include plans and paper documents as well as data files. Consider the need for security and off-site storage.	
7. Determine required skills for individuals involved in executing the plan and procedures.	
8. Distribute the plans and supporting documentation securely to appropriately authorized interested parties. Make sure the plans and documentation are accessible under all disaster scenarios.	3

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISF, The Standard of Good Practice for Information Security 2016	BC1.4 Crisis Management; BC2.1 Business Continuity Planning
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.6 Contingency planning (CP-6, CP-9, CP-10)

Management Practice	Example Metrics
DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP). Test continuity on a regular basis to exercise plans against predetermined outcomes, uphold business resilience and allow innovative solutions to be developed.	a. Frequency of tests b. Number of exercises and tests that achieved recovery objectives

Activities	Capability Level
1. Define objectives for exercising and testing the business, technical, logistical, administrative, procedural and operational systems of the plan to verify completeness of the BCP and DRP in meeting business risk.	2
2. Define and agree on stakeholder exercises that are realistic and validate continuity procedures. Include roles and responsibilities and data retention arrangements that cause minimum disruption to business processes.	
3. Assign roles and responsibilities for performing continuity plan exercises and tests.	
4. Schedule exercises and test activities as defined in the continuity plans.	3
5. Conduct a post-exercise debriefing and analysis to consider the achievement.	4
6. Based on the results of the review, develop recommendations for improving the current continuity plans.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	PP.RS Develop and Maintain Response Plans; PP.RP Develop and Maintain Recovery Plans
ISF, The Standard of Good Practice for Information Security 2016	BC2.3 Business Continuity Testing
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 20: Penetration Tests and Red Team Exercises

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
DSS04.05 Review, maintain and improve the continuity plans. Conduct a management review of the continuity capability at regular intervals to ensure its continued suitability, adequacy and effectiveness. Manage changes to the plans in accordance with the change control process to ensure that continuity plans are kept up to date and continually reflect actual business requirements.	a. Percent of agreed improvements to the plan that have been reflected in the plan b. Percent of continuity plans and business impact assessments that are up to date

Activities	Capability Level
1. On a regular basis, review the continuity plans and capability against any assumptions made and current business operational and strategic objectives.	3
2. On a regular basis, review the continuity plans to consider the impact of new or major changes to enterprise organization, business processes, outsourcing arrangements, technologies, infrastructure, operating systems and application systems.	
3. Consider whether a revised business impact assessment may be required, depending on the nature of the change.	
4. Recommend changes in policy, plans, procedures, infrastructure, and roles and responsibilities. Communicate them as appropriate for management approval and processing via the IT change management process.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
DSS04.06 Conduct continuity plan training. Provide all concerned internal and external parties with regular training sessions regarding procedures and their roles and responsibilities in case of disruption.	a. Percent of internal and external stakeholders who received training b. Percent of relevant internal and external parties whose skills and competencies are current

Activities	Capability Level
1. Roll out BCP and DRP awareness and training.	2
2. Define and maintain training requirements and plans for those performing continuity planning, impact assessments, risk assessments, media communication and incident response. Ensure that the training plans consider frequency of training and training delivery mechanisms.	3
3. Develop competencies based on practical training, including participation in exercises and tests.	
4. Based on the exercise and test results, monitor skills and competencies.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.6 Contingency planning (CP-4)

Management Practice	Example Metrics
DSS04.07 Manage backup arrangements. Maintain availability of business-critical information.	a. Percent of backup media transferred and stored securely b. Percent of successful and timely restoration from backup or alternate media copies

Activities	Capability Level
1. Back up systems, applications, data and documentation according to a defined schedule. Consider frequency (monthly, weekly, daily, etc.), mode of backup (e.g., disk mirroring for real-time backups vs. DVD-ROM for long-term retention), type of backup (e.g., full vs. incremental), and type of media. Consider also automated online backups, data types (e.g., voice, optical), creation of logs, critical end-user computing data (e.g., spreadsheets), physical and logical location of data sources, security and access rights, and encryption.	2
2. Define requirements for on-site and off-site storage of backup data that meet the business requirements. Consider the accessibility required to back up data.	
3. Periodically test and refresh archived and backup data.	
4. Ensure that systems, applications, data and documentation maintained or processed by third parties are adequately backed up or otherwise secured. Consider requiring return of backups from third parties. Consider escrow or deposit arrangements.	

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	IP.BP Apply Backup Processes
HITRUST CSF version 9, September 2017	09.05 Information Back-Up
ISF, The Standard of Good Practice for Information Security 2016	SY2.3 Backup
ISO/IEC 27002:2013/Cor.2:2015(E)	12.3 Backup
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.6 Contingency planning (CP-3)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 10: Data Recovery Capability
Management Practice	**Example Metrics**
DSS04.08 Conduct post-resumption review. Assess the adequacy of the business continuity plan (BCP) and disaster response plan (DRP) following successful resumption of business processes and services after a disruption.	a. Percent of issues identified and subsequently addressed in the plan b. Percent of issues identified and subsequently addressed in training materials

Activities	Capability Level
1. Assess adherence to the documented BCP and DRP.	4
2. Determine the effectiveness of the plans, continuity capabilities, roles and responsibilities, skills and competencies, resilience to the incident, technical infrastructure, and organizational structures and relationships.	
3. Identify weaknesses or omissions in the plans and capabilities and make recommendations for improvement. Obtain management approval for any changes to the plans and apply via the enterprise change control process.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

B. Component: Organizational Structures														
Key Management Practice	**Executive Committee**	**Chief Operating Officer**	**Chief Information Officer**	**Chief Technology Officer**	**Chief Information Security Officer**	**Business Process Owners**	**Data Management Function**	**Head Architect**	**Head Development**	**Head IT Operations**	**Service Manager**	**Information Security Manager**	**Business Continuity Manager**
DSS04.01 Define the business continuity policy, objectives and scope.	R	A	R		R	R				R	R		R
DSS04.02 Maintain business resilience.	R	A	R			R		R		R		R	R
DSS04.03 Develop and implement a business continuity response.			R	R		R				R		R	A
DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP).			R	R		R				R		R	A
DSS04.05 Review, maintain and improve the continuity plans.		A	R	R	R	R				R			R
DSS04.06 Conduct continuity plan training.			R	R		R			R	R		R	A
DSS04.07 Manage backup arrangements.				A			R			R		R	R
DSS04.08 Conduct post-resumption review.			R	R	R	R				R			A

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
DSS04.01 Define the business continuity policy, objectives and scope.	**From**	**Description**	**Description**	**To**
	APO09.03	SLAs	Policy and objectives for business continuity	APO01.02
			Assessments of current continuity capabilities and gaps	Internal
			Disruptive incident scenarios	Internal
DSS04.02 Maintain business resilience.	APO12.06	• Risk impact communication • Risk-related root causes	Approved strategic options	APO02.05
			BIAs	APO12.02
			Continuity requirements	Internal
DSS04.03 Develop and implement a business continuity response.	APO09.03	OLAs	Incident response actions and communications	DSS02.01
			BCP	Internal
DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP).			Test results and recommendations	Internal
			Test exercises	Internal
			Test objectives	Internal
DSS04.05 Review, maintain and improve the continuity plans.			Recommended changes to plans	Internal
			Results of reviews of plans	Internal
DSS04.06 Conduct continuity plan training.	HR	List of personnel requiring training	Monitoring results of skills and competencies	APO07.03
			Training requirements	APO07.03
DSS04.07 Manage backup arrangements.	APO14.10	• Backup plan • Backup test plan	Test results of backup data	Internal
			Backup data	Internal; APO14.08
DSS04.08 Conduct post-resumption review.			Approved changes to the plans	BAI06.01
			Post-resumption review report	Internal
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
No related guidance for this component				

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Continuity management	Skills Framework for the Information Age V6, 2015	COPL

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Business continuity policy	Outlines management's commitment to the business impact assessment (BIA), business contingency plan (including trusted recovery), recovery requirements for critical systems, defined thresholds and triggers for contingencies, escalation plan, data recovery plan, training and testing.		
Crisis management policy	Sets guidelines and sequence of crisis response in key areas of risk. Along with I&T security, network management, and data security and privacy, crisis management is one of the operational-level policies that should be considered for complete I&T risk management.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Embed the need for business resilience in the enterprise culture. Regularly and frequently update employees about core values, desired behaviors and strategic objectives to maintain the enterprise's composure and image in every situation. Regularly test business continuity procedures and disaster recovery.		

G. Component: Services, Infrastructure and Applications
• External hosting services • Incident monitoring tools • Remote storage facility services

Page intentionally left blank

Domain: Deliver, Service and Support Management Objective: DSS05 - Managed Security Services	Focus Area: COBIT Core Model

Description

Protect enterprise information to maintain the level of information security risk acceptable to the enterprise in accordance with the security policy. Establish and maintain information security roles and access privileges. Perform security monitoring.

Purpose

Minimize the business impact of operational information security vulnerabilities and incidents.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG02 Managed business risk • EG06 Business service continuity and availability	• AG02 Managed I&T-related risk • AG07 Security of information, processing infrastructure and applications, and privacy
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG02 a. Percent of critical business objectives and services covered by risk assessment b. Ratio of significant incidents that were not identified in risk assessments vs. total incidents c. Frequency of updating risk profile	AG02 a. Frequency of updating risk profile b. Percent of enterprise risk assessments including I&T-related risk c. Number of significant I&T-related incidents that were not identified in a risk assessment
EG06 a. Number of customer service or business process interruptions causing significant incidents b. Business cost of incidents c. Number of business processing hours lost due to unplanned service interruptions d. Percent of complaints as a function of committed service availability targets	AG07 a. Number of confidentiality incidents causing financial loss, business disruption or public embarrassment b. Number of availability incidents causing financial loss, business disruption or public embarrassment c. Number of integrity incidents causing financial loss, business disruption or public embarrassment

A. Component: Process

Management Practice	Example Metrics
DSS05.01 Protect against malicious software. Implement and maintain preventive, detective and corrective measures (especially up-to-date security patches and virus control) across the enterprise to protect information systems and technology from malicious software (e.g., ransomware, malware, viruses, worms, spyware, spam).	a. Number of successful malicious software attacks b. Percent of employees failing tests on malicious attacks (e.g., test of phishing email)

Activities	Capability Level
1. Install and activate malicious software protection tools on all processing facilities, with malicious software definition files that are updated as required (automatically or semi-automatically).	2
2. Filter incoming traffic, such as email and downloads, to protect against unsolicited information (e.g., spyware, phishing emails).	
3. Communicate malicious software awareness and enforce prevention procedures and responsibilities. Conduct periodic training about malware in email and Internet usage. Train users to not open, but report, suspicious emails and to not install shared or unapproved software.	3
4. Distribute all protection software centrally (version and patch-level) using centralized configuration and IT change management.	
5. Regularly review and evaluate information on new potential threats (e.g., reviewing vendors' products and services security advisories).	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	DP.DC Detect Malicious Code; RI.VT Vulnerability and Threat Identification
HITRUST CSF version 9, September 2017	09.04 Protection Against Malicious & Mobile Code
SF, The Standard of Good Practice for Information Security 2016	TS1 Security Solutions
SO/IEC 27002:2013/Cor.2:2015(E)	12.2 Protection against malware
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 4: Continuous Vulnerability Assessment and Remediation; CSC 8: Malware Defenses

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
DSS05.02 Manage network and connectivity security. Use security measures and related management procedures to protect information over all methods of connectivity.	a. Number of firewall breaches b. Number of vulnerabilities discovered c. Percent of time network and systems not available due to security incident

Activities	Capability Level
1. Allow only authorized devices to have access to corporate information and the enterprise network. Configure these devices to force password entry.	2
2. Implement network filtering mechanisms, such as firewalls and intrusion detection software. Enforce appropriate policies to control inbound and outbound traffic.	
3. Apply approved security protocols to network connectivity.	
4. Configure network equipment in a secure manner.	
5. Encrypt information in transit according to its classification.	3
6. Based on risk assessments and business requirements, establish and maintain a policy for security of connectivity.	
7. Establish trusted mechanisms to support the secure transmission and receipt of information.	
8. Carry out periodic penetration testing to determine adequacy of network protection.	4
9. Carry out periodic testing of system security to determine adequacy of system protection.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	AC.MI Manage Network Integrity & Segregation; CM.MN Monitor Networks; AC.CP Manage Communication Protections
HITRUST CSF version 9, September 2017	01.04 Network Access Control
ISF, The Standard of Good Practice for Information Security 2016	PA2.3 Mobile Device Connectivity; NC1.1 Network Device Configuration
ISO/IEC 27002:2013/Cor.2:2015(E)	13.1 Network security management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.20 System and information integrity (SI-8)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 9: Limitation and Control of Network Ports, Protocols, and Services; CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Management Practice	Example Metrics
DSS05.03 Manage endpoint security. Ensure that endpoints (e.g., laptop, desktop, server, and other mobile and network devices or software) are secured at a level that is equal to or greater than the defined security requirements for the information processed, stored or transmitted.	a. Number of incidents involving endpoint devices b. Number of unauthorized devices detected on the network or in the end-user environment c. Percent of individuals receiving awareness training relating to use of endpoint devices

Activities	Capability Level
1. Configure operating systems in a secure manner.	2
2. Implement device lockdown mechanisms.	
3. Manage remote access and control (e.g., mobile devices, teleworking).	
4. Manage network configuration in a secure manner.	
5. Implement network traffic filtering on endpoint devices.	
6. Protect system integrity.	
7. Provide physical protection of endpoint devices.	
8. Dispose of endpoint devices securely.	
9. Manage malicious access through email and web browsers. For example, block certain websites and deactivate click-through on links for smartphones.	
10. Encrypt information in storage according to its classification.	3

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	IP.MM Apply Mobile Device Management; TP.MP Apply Media Protection; DP.DP Detect Mobile Code and Browser Protection
ISF, The Standard of Good Practice for Information Security 2016	PM1.3 Remote Working; PA2.1 Mobile Device Configuration; PA2.4 Employee-owned Devices; PA2.5 Portable Storage Devices; NC1.6 Remote Maintenance
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.4 Assessment, authorization and monitoring (CA-8, CA-9); 3.19 System and communications protection (SC-10)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers; CSC 7: Email and Web Browser Protections
Management Practice	**Example Metrics**
DSS05.04 Manage user identity and logical access. Ensure that all users have information access rights in accordance with business requirements. Coordinate with business units that manage their own access rights within business processes.	a. Average time between change and update of accounts b. Number of accounts (vs. number of authorized users/staff) c. Number of incidents relating to unauthorized access to information
Activities	**Capability Level**
1. Maintain user access rights in accordance with business function, process requirements and security policies. Align the management of identities and access rights to the defined roles and responsibilities, based on least-privilege, need-to-have and need-to-know principles.	2
2. Administer all changes to access rights (creation, modifications and deletions) in a timely manner based only on approved and documented transactions authorized by designated management individuals.	3
3. Segregate, reduce to the minimum number necessary and actively manage privileged user accounts. Ensure monitoring on all activity on these accounts.	
4. Uniquely identify all information processing activities by functional roles. Coordinate with business units to ensure that all roles are consistently defined, including roles that are defined by the business itself within business process applications.	
5. Authenticate all access to information assets based on the individual's role or business rules. Coordinate with business units that manage authentication within applications used in business processes to ensure that authentication controls have been properly administered.	
6. Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT infrastructure, system operations, development and maintenance) are uniquely identifiable.	
7. Maintain an audit trail of access to information depending upon its sensitivity and regulatory requirements.	4
8. Perform regular management review of all accounts and related privileges.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
HITRUST CSF version 9, September 2017	10.03 Cryptographic Controls
ISF, The Standard of Good Practice for Information Security 2016	PM1.1 Employment Life Cycle; SA1 Access Management
ISO/IEC 27002:2013/Cor.2:2015(E)	7.3 Termination and change of employment; 9. Access control
ITIL V3, 2011	Service Operation, 4.5 Access Management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.1 Access control (AC-11, AC-12); 3.11 Media protection (MP-2, MP-4, MP-7); 3.13 Physical and environmental protection (PE-2, PE-3, PE-6)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 1: Inventory of Authorized and Unauthorized Devices; CSC 2: Inventory of Authorized and Unauthorized Software; CSC 5: Controlled Use of Administrative Privileges; CSC 16: Account Monitoring and Control

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
DSS05.05 Manage physical access to I&T assets. Define and implement procedures (including emergency procedures) to grant, limit and revoke access to premises, buildings and areas, according to business need. Access to premises, buildings and areas should be justified, authorized, logged and monitored. This requirement applies to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.	a. Average rating for physical security assessments b. Number of physical information security-related incidents

Activities	Capability Level
1. Log and monitor all entry points to IT sites. Register all visitors, including contractors and vendors, to the site.	2
2. Ensure all personnel display properly approved identification at all times.	
3. Require visitors to be escorted at all times while on-site.	
4. Restrict and monitor access to sensitive IT sites by establishing perimeter restrictions, such as fences, walls and security devices on interior and exterior doors.	
5. Manage requests to allow appropriately authorized access to the computing facilities.	3
6. Ensure that access profiles remain current. Base access to IT sites (server rooms, buildings, areas or zones) on job function and responsibilities.	
7. Conduct regular physical information security awareness training.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	AC.MA Manage Access; ID.DI Determine Impacts
HITRUST CSF version 9, September 2017	01.01 Business Requirement for Access Control; 01.02 Authorized Access to Information Systems; 02.0 Human Resources Security
ISF, The Standard of Good Practice for Information Security 2016	NC1.2 Physical Network Management
ISO/IEC 27002:2013/Cor.2:2015(E)	11. Physical and environmental security

Management Practice	Example Metrics
DSS05.06 Manage sensitive documents and output devices. Establish appropriate physical safeguards, accounting practices and inventory management regarding sensitive I&T assets, such as special forms, negotiable instruments, special-purpose printers or security tokens.	a. Number of stolen output devices b. Percent of sensitive documents and output devices identified in inventory

Activities	Capability Level
1. Establish procedures to govern the receipt, use, removal and disposal of sensitive documents and output devices into, within, and outside of the enterprise.	2
2. Ensure cryptographic controls are in place to protect sensitive electronically stored information.	
3. Assign access privileges to sensitive documents and output devices based on the least-privilege principle, balancing risk and business requirements.	3
4. Establish an inventory of sensitive documents and output devices, and conduct regular reconciliations.	
5. Establish appropriate physical safeguards over sensitive documents.	

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	CM.Ph Monitor Physical
HITRUST CSF version 9, September 2017	01.06 Application & Information Access Control; 01.07 Mobile Computing & Teleworking; 08.0 Physical & Environmental Security; 10.03 Cryptographic Controls; 10.04 Security of System Files
ISF, The Standard of Good Practice for Information Security 2016	IR2.3 Business Impact Assessment - Confidentiality Requirements; IR2.4 Business Impact Assessment - Integrity Requirements; IR2.5 Business Impact Assessment - Availability Requirements; IM2.2 Sensitive Physical Information; PA2.2 Enterprise Mobility Man
ISO/IEC 27002:2013/Cor.2:2015(E)	10. Cryptography
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.1 Access control (AC-2, AC-3, AC-4, AC-5, AC-6, AC-13, AC-24); 3.7 Identification and authentication (IA-2, IA-10, IA-11)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 15: Wireless Access Control
Management Practice	**Example Metrics**
DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events. Using a portfolio of tools and technologies (e.g., intrusion detection tools), manage vulnerabilities and monitor the infrastructure for unauthorized access. Ensure that security tools, technologies and detection are integrated with general event monitoring and incident management.	a. Number of vulnerability tests carried out on perimeter devices b. Number of vulnerabilities discovered during testing c. Time taken to remediate any vulnerabilities d. Percent of tickets created in a timely manner when monitoring systems identify potential security incidents

Activities	Capability Level
1. Continually use a portfolio of supported technologies, services and assets (e.g., vulnerability scanners, fuzzers and sniffers, protocol analyzers) to identify information security vulnerabilities.	2
2. Define and communicate risk scenarios, so they can be easily recognized, and the likelihood and impact understood.	
3. Regularly review the event logs for potential incidents.	
4. Ensure that security--related incident tickets are created in a timely manner when monitoring identifies potential incidents.	
5. Log security-related events and retain records for appropriate period.	3

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISF, The Standard of Good Practice for Information Security 2016	IR2.6 Threat Profiling
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.7 Identification and authentication (IA-3); 3.11 Media protection (MP-1); 3.13 Physical and environmental protection (PE-5); 3.19 System and communications protection (SC-15)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	Maintenance, Monitoring, and Analysis of Audit Logs

B. Component: Organizational Structures

Key Management Practice	Chief Information Officer	Chief Information Security Officer	Business Process Owners	Head Human Resources	Head Development	Head IT Operations	Information Security Manager	Privacy Officer
DSS05.01 Protect against malicious software.		A	R	R	R	R	R	
DSS05.02 Manage network and connectivity security.		A			R	R	R	
DSS05.03 Manage endpoint security.		A			R	R	R	
DSS05.04 Manage user identity and logical access.		A	R			R	R	R
DSS05.05 Manage physical access to I&T assets.		A				R	R	R
DSS05.06 Manage sensitive documents and output devices.	A					R		R
DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events.		A				R	R	R

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)

Management Practice	Inputs		Outputs	
	From	Description	Description	To
DSS05.01 Protect against malicious software.			Malicious software prevention policy	APO01.02
			Evaluations of potential threats	APO12.02; APO12.03
DSS05.02 Manage network and connectivity security.	APO01.07	Data classification guidelines	Connectivity security policy	APO01.02
	APO09.03	SLAs	Results of penetration tests	MEA04.07
DSS05.03 Manage endpoint security.	APO03.02	Information architecture model	Security policies for endpoint devices	APO01.02
	APO09.03	• SLAs • OLAs		
	BAI09.01	Results of physical inventory checks		
	DSS06.06	Reports of violations		
DSS05.04 Manage user identity and logical access.	APO01.05	Definition of I&T-related roles and responsibilities	Results of reviews of user accounts and privileges	Internal
	APO03.02	Information architecture model	Approved user access rights	Internal

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
DSS05.05 Manage physical access to I&T assets.	**From**	**Description**	**Description**	**To**
			Access logs	DSS06.03, MEA04.07
			Approved access requests	Internal
DSS05.06 Manage sensitive documents and output devices.	APO03.02	Information architecture model	Access privileges	Internal
			Inventory of sensitive documents and devices	Internal
DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events.			Security incident tickets	DSS02.02
			Security incident characteristics	Internal
			Security event logs	Internal
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
No related guidance for this component				

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Information security	Skills Framework for the Information Age V6, 2015	SCTY
Information security management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage— E.8. Information Security Management
Penetration testing	Skills Framework for the Information Age V6, 2015	PENT
Security administration	Skills Framework for the Information Age V6, 2015	SCAD

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Information security policy	Sets guidelines to protect corporate information and associated systems and infrastructure.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Create a culture of awareness regarding user responsibility to maintain security and privacy practices.	1) HITRUST CSF version 9, September 2017; (2) ISF, The Standard of Good Practice for Information Security 2016	(1) 01.03 User Responsibilities; (2) PM2.1 Security Awareness Program

G. Component: Services, Infrastructure and Applications
• Directory services • Email filtering systems • Identity and access management system • Security awareness services • Security information and event management (SIEM) tools • Security operations center (SOC) services • Third-party security assessment services • URL filtering systems

Page intentionally left blank

Domain: Deliver, Service and Support Management Objective: DSS06 - Managed Business Process Controls	Focus Area: COBIT Core Model

Description

Define and maintain appropriate business process controls to ensure that information related to and processed by in-house or outsourced business processes satisfies all relevant information control requirements. Identify the relevant information control requirements. Manage and operate adequate input, throughput and output controls (application controls) to ensure that information and information processing satisfy these requirements.

Purpose

Maintain information integrity and the security of information assets handled within business processes in the enterprise or its outsourced operation.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG05 Customer-oriented service culture • EG08 Optimization of internal business process functionality • EG12 Managed digital transformation programs	AG08 Enabling and supporting business processes by integrating applications and technology

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG01	a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG08	a. Time to execute business services or processes b. Number of I&T-enabled business programs delayed or incurring additional cost due to technology-integration issues c. Number of business process changes that need to be delayed or reworked because of technology-integration issues d. Number of applications or critical infrastructures operating in silos and not integrated
EG05	a. Number of customer service disruptions b. Percent of business stakeholders satisfied that customer service delivery meets agreed levels c. Number of customer complaints d. Trend of customer satisfaction survey results		
EG08	a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities		
EG12	a. Number of programs on time and within budget b. Percent of stakeholders satisfied with program delivery c. Percent of business transformation programs stopped d. Percent of business transformation programs with regular reported status updates		

A. Component: Process

Management Practice	Example Metrics
DSS06.01 Align control activities embedded in business processes with enterprise objectives. Continually assess and monitor the execution of business process activities and related controls (based on enterprise risk), to ensure that processing controls align with business needs.	a. Percent of completed inventory of critical processes and key controls b. Percent of processing controls aligned with business needs

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Identify and document the necessary control activities for key business processes to satisfy control requirements for strategic, operational, reporting and compliance objectives.	2
2. Prioritize control activities based on the inherent risk to the business. Identify key controls.	
3. Ensure ownership of key control activities.	
4. Implement automated controls.	3
5. Continually monitor control activities on an end-to-end basis to identify opportunities for improvement.	4
6. Continually improve the design and operation of business process controls.	5
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.1 Preparation (Task 10, 11)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 14: Controlled Access Based on the Need to Know
Management Practice	**Example Metrics**
DSS06.02 Control the processing of information. Operate the execution of the business process activities and related controls, based on enterprise risk. Ensure that information processing is valid, complete, accurate, timely and secure (i.e., reflects legitimate and authorized business use).	a. Number of incidents and audit report findings indicating failure of key controls b. Percent of coverage of key controls within test plans
Activities	**Capability Level**
1. Authenticate the originator of transactions and verify that the individual has the authority to originate the transaction.	2
2. Ensure adequate segregation of duties regarding the origination and approval of transactions.	
3. Verify that transactions are accurate, complete and valid. Controls may include sequence, limit, range, validity, reasonableness, table look-ups, existence, key verification, check digit, completeness, duplicate and logical relationship checks, and time edits. Validation criteria and parameters should be subject to periodic reviews and confirmations. Validate input data and edit or, where applicable, send back for correction as close to the point of origination as possible.	3
4. Without compromising original transaction authorization levels, correct and resubmit data that were erroneously input. Where appropriate for reconstruction, retain original source documents for the appropriate amount of time.	
5. Maintain the integrity and validity of data throughout the processing cycle. Ensure that detection of erroneous transactions does not disrupt processing of valid transactions.	
6. Handle output in an authorized manner, deliver it to the appropriate recipient and protect the information during transmission. Verify the accuracy and completeness of the output.	
7. Maintain the integrity of data during unexpected interruptions in business processing. Confirm data integrity after processing failures.	
8. Before passing transaction data between internal applications and business/operational functions (inside or outside the enterprise), check for proper addressing, authenticity of origin and integrity of content. Maintain authenticity and integrity during transmission or transport.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
HITRUST CSF version 9, September 2017	13.01 Openness and Transparency; 13.02 Individual Choice and Participation
ISF, The Standard of Good Practice for Information Security 2016	BA1.4 Information Validation

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
DSS06.03 Manage roles, responsibilities, access privileges and levels of authority. Manage business roles, responsibilities, levels of authority and segregation of duties needed to support the business process objectives. Authorize access to all information assets related to business information processes, including those under the custody of the business, IT and third parties. This ensures that the business knows where the data are and who is handling data on its behalf.	a. Number of incidents and audit findings due to access or separation-of-duties violations b. Percent of business process roles with assigned access rights and levels of authority c. Percent of business process roles with clear separation of duties

Activities	Capability Level
1. Allocate roles and responsibilities based on approved job descriptions and business process activities.	2
2. Allocate levels of authority for approval of transactions, transaction limits and any other decisions relating to the business process, based on approved job roles.	
3. Allocate roles for sensitive activities so there is a clear segregation of duties.	
4. Allocate access rights and privileges based on the minimum that is required to perform job activities, based on pre-defined job roles. Remove or revise access rights immediately if the job role changes or a staff member leaves the business process area. Periodically review to ensure that the access is appropriate for the current threats, risk, technology and business need.	3
5. On a regular basis, provide awareness and training regarding roles and responsibilities so that everyone understands their responsibilities; the importance of controls; and the security, integrity, confidentiality and privacy of company information in all its forms.	
6. Ensure administrative privileges are sufficiently and effectively secured, tracked and controlled to prevent misuse.	
7. Periodically review access control definitions, logs and exception reports. Ensure that all access privileges are valid and aligned with current staff members and their allocated roles.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
HITRUST CSF version 9, September 2017	13.04 Collection, Use and Disclosure
ISO/IEC 27002:2013/Cor.2:2015(E)	7. Human resource security
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 5: Controlled Use of Administrative Privileges

Management Practice	Example Metrics
DSS06.04 Manage errors and exceptions. Manage business process exceptions and errors and facilitate remediation, executing defined corrective actions and escalating as necessary. This treatment of exceptions and errors provides assurance of the accuracy and integrity of the business information process.	a. Frequency of processing inefficiencies due to incomplete data entry b. Number of errors detected in a timely manner c. Number of data processing errors that were efficiently remediated

Activities	Capability Level
1. Review errors, exceptions and deviations.	2
2. Follow up, correct, approve and resubmit source documents and transactions.	
3. Maintain evidence of remedial actions.	
4. Define and maintain procedures to assign ownership for errors and exceptions, correct errors, override errors and handle out-of-balance conditions.	3
5. Report relevant business information process errors in a timely manner to perform root cause and trending analysis.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
DSS06.05 Ensure traceability and accountability for information events. Ensure that business information can be traced to an originating business event and associated with accountable parties. This discoverability provides assurance that business information is reliable and has been processed in accordance with defined objectives.	a. Number of incidents in which transaction history cannot be recovered b. Percent of completeness of traceable transaction log

Activities	Capability Level
1. Capture source information, supporting evidence and the record of transactions.	2
2. Define retention requirements, based on business requirements, to meet operational, financial reporting and compliance needs.	3
3. Dispose of source information, supporting evidence and the record of transactions in accordance with the retention policy.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
DSS06.06 Secure information assets. Secure information assets accessible by the business through approved methods, including information in electronic form (e.g., portable media devices, user applications and storage devices, or other methods that create new assets in any form), information in physical form (e.g., source documents or output reports) and information during transit. This benefits the business by providing end-to-end safeguarding of information.	a. Cases of sensitive transaction data delivered to wrong recipient b. Frequency of compromised integrity of critical data

Activities	Capability Level
1. Restrict use, distribution and physical access of information according to its classification.	2
2. Provide acceptable use awareness and training.	
3. Apply data classification and acceptable use and security policies and procedures to protect information assets under the control of the business.	3
4. Identify and implement processes, tools and techniques to reasonably verify compliance.	
5. Report to business and other stakeholders on violations and deviations.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	AC.MP Manage Access Permissions
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 18: Application Software Security

B. Component: Organizational Structures										
Key Management Practice	Executive Committee	Chief Information Officer	I&T Governance Board	Chief Information Security Officer	Business Process Owners	Data Management Function	Service Manager	Information Security Manager	Legal Counsel
DSS06.01 Align control activities embedded in business processes with enterprise objectives.	R		A		R				
DSS06.02 Control the processing of information.		R	A	R	R	R			R
DSS06.03 Manage roles, responsibilities, access privileges and levels of authority.		R	A	R	R			R	
DSS06.04 Manage errors and exceptions.		R		R	A		R		
DSS06.05 Ensure traceability and accountability for information events.		R		R	A				
DSS06.06 Secure information assets.		R		R	A				

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	Inputs		Outputs	
	From	Description	Description	To
DSS06.01 Align control activities embedded in business processes with enterprise objectives.	APO01.07	• Data classification guidelines • Data integrity procedures	Root cause analyses and recommendations	BAI06.01; MEA02.04; MEA04.04; MEA04.06; MEA04.07
			Results of processing effectiveness reviews	MEA02.04
DSS06.02 Control the processing of information.	BAI05.05	Operation and use plan	Processing control reports	Internal
	BAI07.02	Migration plan		
DSS06.03 Manage roles, responsibilities, access privileges and levels of authority.	APO11.01	Quality management system (QMS) roles, responsibilities and decision rights	Allocated levels of authority	APO01.05
	APO13.01	Information security management system (ISMS) scope statement	Allocated roles and responsibilities	APO01.05
	DSS05.05	Access logs	Allocated access rights	APO07.04
	EDM04.02	Assigned responsibilities for resource management		

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
DSS06.04 Manage errors and exceptions.	**From**	**Description**	**Description**	**To**
			Error reports and root cause analysis	Internal
			Evidence of error correction and remediation	MEA02.04
DSS06.05 Ensure traceability and accountability for information events.			Record of transactions	Internal
			Retention requirements	Internal; APO14.09
DSS06.06 Secure information assets.			Reports of violations	DSS05.03

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.1 Preparation (Task 10, 11): Inputs and Outputs

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Information security	Skills Framework for the Information Age V6, 2015	SCTY
Security administration	Skills Framework for the Information Age V6, 2015	SCAD

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Business controls guidance	Defines business process controls to ensure proper control and reduce risk of fraud and errors. Identifies manual controls to protect documents (e.g., source, input, processing and output documents); identifies supervisory controls to review the flow of documents and ensure correct processing. Includes I&T general controls (e.g., physical security, access and authentication, and change management) and application controls (e.g., edit checking, system configuration and security settings).		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Create a culture that embraces the need for sound controls in business processes, building them into applications in development or requiring them in applications bought or accessed as a service. Encourage all employees to have a controls consciousness to protect all assets of the organization (e.g., paper records and facilities).		

G. Component: Services, Infrastructure and Applications
• Automated application controls • Event log auditing tools

4.5 Monitor, Evaluate and Assess (MEA)

01 Managed Performance and Conformance Monitoring

02 Managed System of Internal Control

03 Managed Compliance With External Requirements

04 Managed Assurance

Page intentionally left blank

Domain: Monitor, Evaluate and Assess Management Objective: MEA01 — Managed Performance and Conformance Monitoring	Focus Area: COBIT Core Model

Description

Collect, validate and evaluate enterprise and alignment goals and metrics. Monitor that processes and practices are performing against agreed performance and conformance goals and metrics. Provide reporting that is systematic and timely.

Purpose

Provide transparency of performance and conformance and drive achievement of goals.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG04 Quality of financial information • EG07 Quality of management information • EG08 Optimization of internal business process functionality	• AG05 Delivery of I&T services in line with business requirements • AG10 Quality of I&T management information

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG01	a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG05	a. Percent of business stakeholders satisfied that I&T service delivery meets agreed service levels b. Number of business disruptions due to I&T service incidents c. Percent of users satisfied with the quality of I&T service delivery
EG04	a. Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of enterprise financial information b. Cost of noncompliance with finance-related regulations	AG10	a. Level of user satisfaction with quality, timeliness and availability of I&T-related management information, taking into account available resources b. Ratio and extent of erroneous business decisions in which erroneous or unavailable I&T-related information was a key factor c. Percentage of information meeting quality criteria
EG07	a. Degree of board and executive management satisfaction with decision-making information b. Number of incidents caused by incorrect business decisions based on inaccurate information c. Time to provide information supporting effective business decisions d. Timeliness of management information		
EG08	a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities		

A. Component: Process

Management Practice	Example Metrics
MEA01.01 Establish a monitoring approach. Engage with stakeholders to establish and maintain a monitoring approach to define the objectives, scope and method for measuring business solution and service delivery and contribution to enterprise objectives. Integrate this approach with the corporate performance management system.	a. Percent of processes with defined goals and metrics b. Percent of integration of monitoring approach within corporate performance management system

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Identify stakeholders (e.g., management, process owners and users).	2
2. Engage with stakeholders and communicate the enterprise requirements and objectives for monitoring, aggregating and reporting, using common definitions (e.g., business glossary, metadata and taxonomy), baselining and benchmarking.	
3. Align and continually maintain the monitoring and evaluation approach with the enterprise approach and the tools to be used for data gathering and enterprise reporting (e.g., business intelligence applications).	
4. Agree on the types of goals and metrics (e.g., conformance, performance, value, risk), taxonomy (classification and relationships between goals and metrics) and data (evidence) retention.	
5. Request, prioritize and allocate resources for monitoring, consider appropriateness, efficiency, effectiveness and confidentiality.	
6. Periodically validate the approach used and identify new or changed stakeholders, requirements and resources.	3
7. Agree on a life cycle management and change control process for monitoring and reporting. Include improvement opportunities for reporting, metrics, approach, baselining and benchmarking.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Supporting Processes - Measurement and Analysis
SF, The Standard of Good Practice for Information Security 2016	SI2 Security Performance
ISO/IEC 27001:2013/Cor.2:2015(E)	9.1 Monitoring, measurement, analysis and evaluation
ISO/IEC 27004:2016(E)	6. Characteristics; 7. Types of measures; 8. Processes
ISO/IEC 38500:2015(E)	5.5 Principle 4: Performance; 5.6 Principle 5: Conformance
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.1 Preparation (Task 13); 3.3 Selection (Task 2); 3.7 Monitoring (Task 1)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.4 Assessment, authorization and monitoring (CA-2, CA-7); 3.20 System and information integrity (SI-4)
Management Practice	**Example Metrics**
MEA01.02 Set performance and conformance targets. Work with stakeholders to define, periodically review, update and approve performance and conformance targets within the performance measurement system.	a. Percent of goals and metrics approved by stakeholders b. Percent of processes with effectiveness of goals and metrics reviewed and improved
Activities	**Capability Level**
1. Define the goals and metrics. Periodically review them with stakeholders to identify any significant missing items and define reasonableness of targets and tolerances.	2
2. Evaluate whether the goals and metrics are adequate, that is, specific, measurable, achievable, relevant and time-bound (SMART).	
3. Communicate proposed changes to performance and conformance targets and tolerances (relating to metrics) with key due diligence stakeholders (e.g., legal, audit, HR, ethics, compliance, finance).	
4. Publish changed targets and tolerances to users of this information.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Supporting Processes - Process Management
National Institute of Standards and Technology Special Publication 800-53, Revisionv5 (Draft), August 2017	3.4 Assessment, authorization and monitoring (CA-5)
Management Practice	**Example Metrics**
MEA01.03 Collect and process performance and conformance data. Collect and process timely and accurate data aligned with enterprise approaches.	a. Percent of critical processes monitored b. Percent of controls environment that is monitored, benchmarked and improved to meet organizational objectives

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Collect data from defined processes (automated, where possible).	2
2. Assess efficiency (effort in relation to insight provided) and appropriateness (usefulness and meaning) of collected data and validate the data's integrity (accuracy and completeness).	
3. Aggregate data to support measurement of agreed metrics.	
4. Align aggregated data to the enterprise reporting approach and objectives.	3
5. Use suitable tools and systems for the processing and analysis of data.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.20 System and information integrity (SI-2)
Management Practice	**Example Metrics**
MEA01.04 Analyze and report performance. Periodically review and report performance against targets. Use a method that provides a succinct all-around view of I&T performance and fits within the enterprise monitoring system.	a. Percent of goals and metrics aligned to enterprise monitoring system b. Percent of performance reports delivered as scheduled c. Percent of processes with assured output meeting targets within tolerances
Activities	**Capability Level**
1. Design process performance reports that are concise, easy to understand, and tailored to various management needs and audiences. Facilitate effective, timely decision making (e.g., scorecards, traffic light reports). Ensure that the cause and effect between goals and metrics are communicated in an understandable manner.	3
2. Distribute reports to the relevant stakeholders.	
3. Analyze the cause of deviations against targets, initiate remedial actions, assign responsibilities for remediation, and follow up. At appropriate times, review all deviations and search for root causes, where necessary. Document the issues for further guidance if the problem recurs. Document results.	4
4. Where feasible, integrate performance and compliance into individual staff members' performance objectives and link achievement of performance targets to the organizational reward compensation system.	
5. Compare the performance values to internal targets and benchmarks and, where possible, to external benchmarks (industry and key competitors).	
6. Analyze trends in performance and compliance and take appropriate action.	
7. Recommend changes to the goals and metrics, where appropriate.	5
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Supporting Processes - Measurement and Analysis
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.3 Audit and accountability (AU-6)
Management Practice	**Example Metrics**
MEA01.05 Ensure the implementation of corrective actions. Assist stakeholders in identifying, initiating and tracking corrective actions to address anomalies.	a. Number of recurring anomalies b. Number of corrective actions implemented
Activities	**Capability Level**
1. Review management responses, options and recommendations to address issues and major deviations.	2
2. Ensure that the assignment of responsibility for corrective action is maintained.	
3. Track the results of actions committed.	
4. Report the results to the stakeholders.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ITIL V3, 2011	Continual Service Improvement, 4.1 The 7-Step Improvement Process
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.7 Monitoring (Task 3)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.3 Audit and accountability (AU-5)

B. Component: Organizational Structures												
Key Management Practice	Executive Committee	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Chief Information Officer	I&T Governance Board	Business Process Owners	Relationship Manager	Head Development	Head IT Operations	Service Manager
MEA01.01 Establish a monitoring approach.	R	A	R	R	R	R					
MEA01.02 Set performance and conformance targets.	A						R	R	R	R	R
MEA01.03 Collect and process performance and conformance data.					A		R	R	R	R	R
MEA01.04 Analyze and report performance.					A		R	R	R	R	R
MEA01.05 Ensure the implementation of corrective actions.					A		R	R	R	R	R

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	Inputs		Outputs	
	From	Description	Description	To
MEA01.01 Establish a monitoring approach.	EDM05.01	• Evaluation of enterprise reporting requirements • Reporting and communications principles	Approved monitoring goals and metrics	Internal
			Monitoring requirements	Internal
	EDM05.02	Rules for validating and approving mandatory reports		
	EDM05.03	Assessment of reporting effectiveness		
MEA01.02 Set performance and conformance targets.	APO01.11	Performance goals and metrics for process improvement tracking	Monitoring targets	All APO; All BAI; All DSS; All MEA

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
MEA01.03 Collect and process performance and conformance data.	APO01.11	Process capability assessments	Processed monitoring data	Internal
	APO05.03	Investment portfolio performance reports		
	APO09.04	Service level performance reports		
	APO10.05	Results of vendor-compliance monitoring review		
	BAI01.06	Results of program performance reviews		
	BAI04.04	Availability, performance and capacity-monitoring review reports		
	BAI05.05	Success measures and results		
	DSS01.05	Facilities assessment reports		
	DSS02.07	• Incident status and trends report • Request fulfilment status and trends report		
MEA01.04 Analyze and report performance.			Performance reports	All APO; All BAI; All DSS; All MEA; EDM01.03
MEA01.05 Ensure the implementation of corrective actions.	APO01.09	Noncompliance remedial actions	Remedial actions and assignments	All APO; All BAI; All DSS; All MEA
	EDM05.02	Escalation guidelines	Status and results of actions	EDM01.03

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.1 Preparation (Task 13): Inputs and Outputs; 3.3 Selection (Task 2): Inputsand Outputs; 3.7 Monitoring (Task 1, Task 3): Inputs and Outputs

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Conformance review	Skills Framework for the Information Age V6, 2015	CORE
ICT quality management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.6. ICT Quality Management
Quality assurance	Skills Framework for the Information Age V6, 2015	QUAS

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Self-assessment policy	Provides guidance for management's responsibilities in assessing operations as part of the continuous improvement program. Often used to report internally to executives or board on current capabilities, progress and improvement, based on business requirements. Assessments may be used during or after a process improvement program (i.e., to assess progress after completing an improvement).		
Whistle-blower policy	Encourages employees to raise concerns and questions in full confidence. Ensures employees that they will receive a response and be able to escalate concerns if they are not satisfied with the response. Assures that employees are protected when they raise issues and should not fear reprisal.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
To achieve the organization's goals and optimize performance, promote a culture of continuous improvement of business and I&T processes.		

G. Component: Services, Infrastructure and Applications
• Performance measurement system (e.g., balanced scorecard, skills management tools) • Self-assessment tools

Domain: Monitor, Evaluate and Assess Management Objective: MEA02 — Managed System of Internal Control	Focus Area: COBIT Core Model

Description

Continuously monitor and evaluate the control environment, including self-assessments and self-awareness. Enable management to identify control deficiencies and inefficiencies and to initiate improvement actions. Plan, organize and maintain standards for internal control assessment and process control effectiveness.

Purpose

Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG03 Compliance with external laws and regulations • EG11 Compliance with internal policies	AG11 I&T compliance with internal policies
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG03 a. Cost of regulatory noncompliance, including settlements and fines b. Number of regulatory noncompliance issues causing public comment or negative publicity c. Number of noncompliance matters noted by regulators d. Number of regulatory noncompliance issues relating to contractual agreements with business partners	AG11 a. Number of incidents related to noncompliance with I&T-related policies b. Number of exceptions to internal policies c. Frequency of policy review and update
EG11 a. Number of incidents related to noncompliance to policy b. Percent of stakeholders who understand policies c. Percent of policies supported by effective standards and working practices	

A. Component: Process

Management Practice	Example Metrics
MEA02.01 Monitor internal controls. Continuously monitor, benchmark and improve the I&T control environment and control framework to meet organizational objectives.	a. Number of major internal control breaches b. Percent of controls environment and framework continuously monitored, benchmarked and improved to meet organizational objectives

Activities	Capability Level
1. Identify the boundaries of the internal control system. For example, consider how organizational internal controls take into account outsourced and/or offshore development or production activities.	3
2. Assess the status of external service providers' internal controls. Confirm that service providers comply with legal and regulatory requirements and contractual obligations.	
3. Perform internal control monitoring and evaluation activities based on organizational governance standards and industry-accepted frameworks and practices. Also include monitoring and evaluation of the efficiency and effectiveness of managerial supervisory activities.	
4. Ensure that control exceptions are promptly reported, followed up and analyzed, and appropriate corrective actions are prioritized and implemented according to the risk management profile (e.g., classify certain exceptions as a key risk and others as a non-key risk).	
5. Consider independent evaluations of the internal control system (e.g., by internal audit or peers).	
6. Maintain the internal control system, considering ongoing changes in business and I&T risk, the organizational control environment, and relevant business and I&T processes. If gaps exist, evaluate and recommend changes.	4
7. Regularly evaluate the performance of the control framework, benchmarking against industry accepted standards and good practices. Consider formal adoption of a continuous improvement approach to internal control monitoring.	5

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
HITRUST CSF version 9, September 2017	09.10 Monitoring
ISO/IEC 38502:2017(E)	5.5 Governance and internal control
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.3 Audit and accountability (AU-2)
Management Practice	**Example Metrics**
MEA02.02 Review effectiveness of business process controls. Review the operation of controls, including monitoring and test evidence, to ensure that controls within business processes operate effectively. Include activities to maintain evidence of the effective operation of controls through mechanisms such as periodic testing, continuous monitoring, independent assessments, command and control centers, and network operation centers. This evidence assures the enterprise that controls meet requirements related to business, regulatory and social responsibilities.	a. Number of weaknesses identified by external qualification and certification reports b. Number of controls being monitored and tested to ensure that controls within business processes operate effectively

Activities	Capability Level
1. Understand and prioritize risk to organizational objectives.	3
2. Identify key controls and develop a strategy suitable for validating controls.	
3. Identify information that will indicate whether the internal control environment is operating effectively.	
4. Maintain evidence of control effectiveness.	4
5. Develop and implement cost-effective procedures to obtain this information in line with applicable information quality criteria.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	
Management Practice	**Example Metrics**
MEA02.03 Perform control self-assessments. Encourage management and process owners to improve controls proactively through a continuing program of self-assessment that evaluates the completeness and effectiveness of management's control over processes, policies and contracts.	a. Number of self-assessments performed b. Number of identified gaps in self-assessments vs. industry standards or good practices

Activities	Capability Level
1. Define an agreed, consistent approach for performing control self-assessments and coordinating with internal and external auditors.	3
2. Maintain evaluation plans, and scope and identify evaluation criteria for conducting self-assessments. Plan the communication of results of the self-assessment process to business, IT and general management and the board. Consider internal audit standards in the design of self-assessments.	
3. Determine the frequency of periodic self-assessments, considering the overall effectiveness and efficiency of ongoing monitoring.	
4. Assign responsibility for self-assessment to appropriate individuals to ensure objectivity and competence.	
5. Provide for independent reviews to ensure objectivity of the self-assessment and enable the sharing of internal control good practices from other enterprises.	
6. Compare the results of the self-assessments against industry standards and good practices.	4
7. Summarize and report outcomes of self-assessments and benchmarking for remedial actions.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISO/IEC 27001:2013/Cor.2:2015(E)	9.3 Management review
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.7 Monitoring (Task 2)

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
MEA02.04 Identify and report control deficiencies. Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.	a. Time between internal control deficiency occurrence and reporting b. Time between exception identification and agreed actions addressed c. Percent of implementation of remedial actions arising from control assessments

Activities	Capability Level
1. Communicate procedures for escalation of control exceptions, root cause analysis, and reporting to process owners and I&T stakeholders.	3
2. Consider related enterprise risk to establish thresholds for escalation of control exceptions and breakdowns.	
3. Identify, report and log control exceptions. Assign responsibility for resolving them and reporting on the status.	
4. Decide which control exceptions should be communicated to the individual responsible for the function and which exceptions should be escalated. Inform affected process owners and stakeholders.	
5. Follow up on all exceptions to ensure that agreed-on actions have been addressed.	4
6. Identify, initiate, track and implement remedial actions arising from control assessments and reporting.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

B. Component: Organizational Structures

Key Management Practice	Chief Financial Officer	Chief Risk Officer	Chief Information Officer	Chief Technology Officer	I&T Governance Board	Business Process Owners	Project Management Office	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
MEA02.01 Monitor internal controls.		R	A	R		R	R	R	R	R	R	R	R	R
MEA02.02 Review effectiveness of business process controls.	R		A	R	R	R								
MEA02.03 Perform control self-assessments.		R	A	R		R	R	R	R	R	R	R	R	R
MEA02.04 Identify and report control deficiencies.			A	R		R	R	R	R	R	R	R	R	R

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
MEA02.01 Monitor internal controls.	**From**	**Description**	**Description**	**To**
	APO12.04	Results of third-party risk assessments	Results of benchmarking and other evaluations	All APO; All BAI; All DSS; All MEA; EDM01.03
	APO13.03	Information security management system (ISMS) audit reports	Results of internal control monitoring and reviews	All APO; All BAI; All DSS; All MEA; EDM01.03
	Outside COBIT	Industry standards and good practices		
MEA02.02 Review effectiveness of business process controls.	BAI05.06	Compliance audit results	Evidence of control effectiveness	Internal
	BAI05.07	Reviews of operational use		
MEA02.03 Perform control self-assessments.			Self-assessment plans and criteria	All APO; All BAI; All DSS; All MEA
			Results of reviews of self-assessments	All APO; All BAI; All DSS; All MEA; EDM01.03
			Results of self-assessments	Internal
MEA02.04 Identify and report control deficiencies.	APO11.03	Root causes of failure to deliver quality	Remedial actions	All APO; All BAI; All DSS; All MEA
	APO12.06	Risk-related root causes	Control deficiencies	All APO; All BAI; All DSS; All MEA
	DSS06.01	• Results of processing effectiveness reviews • Root cause analyses and recommendations		
	DSS06.04	Evidence of error correction and remediation		
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017		3.7 Monitoring (Task 2): Inputs and Outputs		

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Risk management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.3. Risk Management

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Internal control policy	Communicates management's internal control objectives. Establishes standards for the design and operation of the enterprise system of internal controls to reduce exposure to all risk. Provides guidance for continuously monitoring and evaluating the control environment, including self-awareness and self-assessments.		
Internal control self-assessment guidance	Recommends continuous monitoring of internal controls to identify deficiencies and gaps in effectiveness, determine their root causes, and initiate plans of action and corrective milestones for reporting to stakeholders.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Promote awareness of the importance of an effective control environment. Encourage a proactive risk- and self-aware culture, including commitment to self-assessment and independent assurance reviews.		

G. Component: Services, Infrastructure and Applications
• COBIT and related products/tools • Third-party internal control assessment services

Page intentionally left blank

Domain: Monitor, Evaluate and Assess Management Objective: MEA03 — Managed Compliance With External Requirements	Focus Area: COBIT Core Model

Description

Evaluate that I&T processes and I&T-supported business processes are compliant with laws, regulations and contractual requirements. Obtain assurance that the requirements have been identified and complied with; integrate IT compliance with overall enterprise compliance.

Purpose

Ensure that the enterprise is compliant with all applicable external requirements.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
EG03 Compliance with external laws and regulations	AG01 I&T compliance and support for business compliance with external laws and regulations
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG03 a. Cost of regulatory noncompliance, including settlements and fines b. Number of regulatory noncompliance issues causing public comment or negative publicity c. Number of noncompliance matters noted by regulators d. Number of regulatory noncompliance issues relating to contractual agreements with business partners	AG01 a. Cost of IT noncompliance, including settlements and fines, and the impact of reputational loss b. Number of IT-related noncompliance issues reported to the board, or causing public comment or embarrassment c. Number of noncompliance issues relating to contractual agreements with IT service providers

A. Component: Process

Management Practice	Example Metrics
MEA03.01 Identify external compliance requirements. On a continuous basis, monitor changes in local and international laws, regulations and other external requirements and identify mandates for compliance from an I&T perspective.	a. Frequency of compliance requirements reviews b. Percent of satisfaction of key stakeholders in regulatory review compliance process

Activities	Capability Level
1. Assign responsibility for identifying and monitoring any changes of legal, regulatory and other external contractual requirements relevant to the use of IT resources and the processing of information within the business and IT operations of the enterprise.	2
2. Identify and assess all potential compliance requirements and the impact on I&T activities in areas such as data flow, privacy, internal controls, financial reporting, industry-specific regulations, intellectual property, health and safety.	
3. Assess the impact of I&T-related legal and regulatory requirements on third-party contracts related to IT operations, service providers and business trading partners.	
4. Define the consequences of noncompliance.	
5. Obtain independent counsel, where appropriate, on changes to applicable laws, regulations and standards.	3
6. Maintain an up-to-date log of all relevant legal, regulatory and contractual requirements; their impact and required actions.	
7. Maintain a harmonized and integrated overall register of external compliance requirements for the enterprise.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	BC.RR Determine Legal / Regulatory Requirements
HITRUST CSF version 9, September 2017	06.01 Compliance with Legal Requirements
ISF, The Standard of Good Practice for Information Security 2016	SM2.3 Legal and Regulatory Compliance

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
MEA03.02 Optimize response to external requirements. Review and adjust policies, principles, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated. Consider adopting and adapting industry standards, codes of good practice, and good practice guidance.	a. Average time between identifying external compliance issues and resolution b. Percent of satisfaction of relevant personnel with communication of new and changed regulatory compliance requirements

Activities	Capability Level
1. Regularly review and adjust policies, principles, standards, procedures and methodologies for their effectiveness in ensuring necessary compliance and addressing enterprise risk. Use internal and external experts, as required.	3
2. Communicate new and changed requirements to all relevant personnel.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
King IV Report on Corporate Governance for South Africa, 2016	Part 5.4: Governance functional areas - Principle 13

Management Practice	Example Metrics
MEA03.03 Confirm external compliance. Confirm compliance of policies, principles, standards, procedures and methodologies with legal, regulatory and contractual requirements.	a. Number of critical noncompliance issues identified per year b. Percent of process owners signing off, confirming compliance

Activities	Capability Level
1. Regularly evaluate organizational policies, standards, procedures and methodologies in all functions of the enterprise to ensure compliance with relevant legal and regulatory requirements in relation to the processing of information.	3
2. Address compliance gaps in policies, standards and procedures on a timely basis.	
3. Periodically evaluate business and IT processes and activities to ensure adherence to applicable legal, regulatory and contractual requirements.	
4. Regularly review for recurring patterns of compliance failures and assess lessons learned.	4
5. Based on review and lessons learned, improve policies, standards, procedures, methodologies, and associated processes and activities.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
MEA03.04 Obtain assurance of external compliance. Obtain and report assurance of compliance and adherence with policies, principles, standards, procedures and methodologies. Confirm that corrective actions to address compliance gaps are closed in a timely manner.	a. Number of compliance reports obtained b. Percent of service provider compliance based on independent reviews c. Time between identification of compliance gap and corrective action d. Number of corrective action reports addressing compliance gaps closed in a timely manner

Activities	Capability Level
1. Obtain regular confirmation of compliance with internal policies from business and IT process owners and unit heads.	2
2. Perform regular (and, where appropriate, independent) internal and external reviews to assess levels of compliance.	
3. If required, obtain assertions from third-party I&T service providers on levels of their compliance with applicable laws and regulations.	
4. If required, obtain assertions from business partners on levels of their compliance with applicable laws and regulations as they relate to intercompany electronic transactions.	
5. Integrate reporting on legal, regulatory and contractual requirements at an enterprisewide level, involving all business units.	3
6. Monitor and report on noncompliance issues and, where necessary, investigate the root cause.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Data Management Maturity Model, 2014	Supporting Processes - Process Quality Assurance
ISO/IEC 27002:2013/Cor.2:2015(E)	18. Compliance

B. Component: Organizational Structures																		
Key Management Practice	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Chief Information Officer	I&T Governance Board	Business Process Owners	Project Management Office	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer	Legal Counsel	Compliance	Audit
MEA03.01 Identify external compliance requirements.				R		R								R	R	A	R
MEA03.02 Optimize response to external requirements.	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	A
MEA03.03 Confirm external compliance.	R	R	R	R	R	R								R	R	A	
MEA03.04 Obtain assurance of external compliance.				R											R	A	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	Inputs		Outputs	
	From	Description	Description	To
MEA03.01 Identify external compliance requirements.	Outside COBIT	Legal and regulatory compliance requirements	Log of required compliance actions	Internal
			Compliance requirements register	Internal
MEA03.02 Optimize response to external requirements.			Communications of changed compliance requirements	All APO; All BAI; All DSS; All MEA; EDM01.01
			Updated policies, principles, procedures and standards	APO01.09; APO01.11
MEA03.03 Confirm external compliance.	BAI05.06	Compliance audit results	Compliance confirmations	EDM01.03
	BAI09.05	Results of installed license audits	Identified compliance gaps	MEA04.08
	BAI10.05	License deviations		
	DSS01.04	Insurance policy reports		
MEA03.04 Obtain assurance of external compliance.	EDM05.02	Rules for validating and approving mandatory reports	Compliance assurance reports	EDM01.03
	EDM05.03	Assessment of reporting effectiveness	Reports of noncompliance issues and root causes	EDM01.03; MEA04.04

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Information security	Skills Framework for the Information Age V6, 2015	SCTY

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Compliance policy	Identifies regulatory, contractual and internal compliance requirements. Explains the process to assess compliance with regulatory, contractual and internal requirements. Lists roles and responsibilities for different activities in the process and provides guidance on metrics to measure compliance. Obtains compliance reports and confirms compliance or corrective actions to address remediation of compliance gaps in a timely manner.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Promote a compliance-aware culture, including zero tolerance of noncompliance with legal and regulatory requirements.		

G. Component: Services, Infrastructure and Applications
• Regulatory Watch services • Third-party compliance assessment services

Domain: Monitor, Evaluate and Assess Management Objective: MEA04 — Managed Assurance	Focus Area: COBIT Core Model

Description

Plan, scope and execute assurance initiatives to comply with internal requirements, laws, regulations and strategic objectives. Enable management to deliver adequate and sustainable assurance in the enterprise by performing independent assurance reviews and activities.

Purpose

Enable the organization to design and develop efficient and effective assurance initiatives, providing guidance on planning, scoping, executing and following up on assurance reviews, using a road map based on well-accepted assurance approaches.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG03 Compliance with external laws and regulations • EG11 Compliance with internal policies	AG11 I&T compliance with internal policies
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG03 a. Cost of regulatory noncompliance, including settlements and fines b. Number of regulatory noncompliance issues causing public comment or negative publicity c. Number of noncompliance matters noted by regulators d. Number of regulatory noncompliance issues relating to contractual agreements with business partners	AG11 a. Number of incidents related to noncompliance with I&T-related policies b. Number of exceptions to internal policies c. Frequency of policy review and update
EG11 a. Number of incidents related to noncompliance to policy b. Percent of stakeholders who understand policies c. Percent of policies supported by effective standards and working practices	

A. Component: Process

Management Practice	Example Metrics
MEA04.01 Ensure that assurance providers are independent and qualified. Ensure that the entities performing assurance are independent from the function, groups or organizations in scope. The entities performing assurance should demonstrate an appropriate attitude and appearance, competence in the skills and knowledge necessary to perform assurance, and adherence to codes of ethics and professional standards.	a. Percent of processes receiving independent review b. Percent of qualifications and competencies met by service providers

Activities	Capability Level
1. Establish adherence to applicable codes of ethics and standards (e.g., Code of Professional Ethics of ISACA) and (industry- and geography-specific) assurance standards (e.g., IT Audit and Assurance Standards of ISACA and the International Auditing and Assurance Standards Board's [IAASB's] International Framework for Assurance Engagements [IAASB Assurance Framework]).	2
2. Establish independence of assurance providers.	
3. Establish competency and qualification of assurance providers.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
HITRUST CSF version 9, September 2017	06.03 Information System Audit Considerations

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
MEA04.02 Develop risk-based planning of assurance initiatives. Determine assurance objectives based on assessments of the internal and external environment and context, the risk of not achieving enterprise goals, and the opportunities associated achievement of the same goals.	a. Percent of assurance initiatives following approved assurance program and plan standards b. Percent of assurance plan initiatives based on risk
Activities	**Capability Level**
1. Understand the enterprise strategy and priorities.	2
2. Understand the internal context of the enterprise. This understanding will help the assurance professional to better assess the enterprise goals and the relative importance of enterprise and alignment goals, as well as the most important threats to these goals. In turn, this will assist in defining a better and more relevant scope for the assurance engagement.	
3. Understand the external context of the enterprise. This understanding will help the assurance professional to better understand the enterprise goals and the relative importance of enterprise and alignment goals, as well as the most important threats to these goals. In turn, this will assist in defining a better and more relevant scope for the assurance engagement.	
4. Develop an overall yearly plan for assurance initiatives containing the consolidated assurance objectives.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
King IV Report on Corporate Governance for South Africa, 2016	Part 5.4: Governance functional areas—Principle 15
Management Practice	**Example Metrics**
MEA04.03 Determine the objectives of the assurance initiative. Define and agree with all stakeholders on the objectives of the assurance initiative.	a. Percent of objectives achieved through the assurance initiative b. Percent of stakeholder satisfaction with the assurance initiative's objectives
Activities	**Capability Level**
1. Define the assurance objective of the assurance initiative by identifying the stakeholders of the assurance initiative and their interests.	2
2. Agree on the high-level objectives and the organizational boundaries of the assurance engagement.	
3. Consider the use of the COBIT Goals Cascade and its different levels to express the assurance objective.	3
4. Ensure that the objectives of the assurance engagement consider all three value objective components: delivering benefits that support strategic objectives, optimizing the risk that strategic objectives are not achieved and optimizing resource levels required to achieve the strategic objectives.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Supporting Processes - Process Quality Assurance
Management Practice	**Example Metrics**
MEA04.04 Define the scope of the assurance initiative. Define and agree with all stakeholders on the scope of the assurance initiative, based on the assurance objectives.	a. Number of engagement plans, based on the scope, that consider information to be collected and stakeholders to be interviewed b. Percent of stakeholder satisfaction with the scope of the assurance initiative, based on the assurance objectives
Activities	**Capability Level**
1. Define all governance components in scope of the review, that is, the principles, policies and frameworks; processes; organizational structures; culture, ethics and behavior; information; services, infrastructure and applications; people, skills and competences	2
2. Based on the scope definition, define an engagement plan, considering information to be collected and stakeholders to be interviewed.	3
3. Confirm and refine the scope based on an understanding of the enterprise architecture.	
4. Refine the scope of the assurance engagement, based on available resources.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	TP.LA Apply Logging and Audit Processes

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.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
MEA04.06 Execute the assurance initiative, focusing on design effectiveness. Execute the planned assurance initiative. Validate and confirm the design of the internal controls in place. Additionally, and specifically in internal audit assignments, consider the cost-effectiveness of the governance component design.	a. Percent of assurance initiatives that consider cost effectiveness of design b. Percent of stakeholder satisfaction with the design of the assurance initiative

Activities	Capability Level
1. Refine the understanding of the IT assurance subject.	2
2. Refine the scope of the IT assurance subject.	
3. Observe/inspect and review the management control approach. Validate the design with the control owner for completeness, relevancy, timeliness and measurability.	3
4. Ask the control owner whether the responsibilities for the governance component and overall accountability have been assigned. Confirm the response. Test whether accountability and responsibilities are understood and accepted. Verify that the right skills and the necessary resources are available.	
5. Reconsider the balance of prevention vs. detection and correction types of management control activities.	
6. Consider the effort spent in maintaining the management controls and the associated cost/effectiveness.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISF, The Standard of Good Practice for Information Security 2016	SI1 Security Audit
ISO/IEC 27001:2013/Cor.2:2015(E)	9.2 Internal audit

Management Practice	Example Metrics
MEA04.07 Execute the assurance initiative, focusing on operating effectiveness. Execute the planned assurance initiative. Test whether the internal controls in place are appropriate and sufficient. Test the outcome of the key management objectives in scope of the assurance initiative.	a. Percent of assurance initiatives that test the outcome of key, in-scope management objectives b. Percent of stakeholder satisfaction with the execution of the assurance initiative

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Assess whether the expected outcomes for each of the management controls in scope are achieved. That is, assess the effectiveness of the management control (control effectiveness).	3
2. Ensure that the assurance professional tests the outcome or effectiveness of the management control by looking for direct and indirect evidence of the impact on the management controls goals. This implies the direct and indirect substantiation of measurable contribution of the management goals to the alignment goals, thereby recording direct and indirect evidence of actually achieving the expected outcomes.	
3. Determine whether the assurance professional obtains direct or indirect evidence for selected items/periods by applying a selection of testing techniques to ensure that the management control under review is working effectively. Ensure that the assurance professional also performs a limited review of the adequacy of the management control results and determines the level of substantive testing and additional work needed to provide assurance that the management control performance is adequate.	
4. Investigate whether a management control can be made more efficient and if its design can be more effective by optimizing steps or looking for synergies with other management controls.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	SI1 Security Audit
SO/IEC 27001:2013/Cor.2:2015(E)	9.2 Internal audit
Management Practice	**Example Metrics**
MEA04.08 Report and follow up on the assurance initiative. Provide positive assurance opinions, where appropriate, and recommendations for improvement relating to identified operational performance, external compliance and internal control weaknesses.	a. Stakeholder acceptance of the assurance report b. Stakeholder acceptance of recommendations for improvement relating to identified operational performance, external compliance and internal control weaknesses
Activities	**Capability Level**
1. Document the impact of control weaknesses.	2
2. Communicate with management during execution of the initiative so there is a clear understanding of the work performed and agreement on and acceptance of the preliminary findings and recommendations.	
3. Provide management with a report (aligned with the terms of reference, scope and agreed reporting standards) that supports the results of the initiative and enables a clear focus on key issues and important actions.	3
4. Supervise the assurance activities and make sure the work done is complete, meets objectives and is of an acceptable quality. Revise the approach or detailed steps if quality gaps occur.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
MEA04.09 Follow up on recommendations and actions. Agree on, follow up and implement the identified recommendations for improvement.	a. Number of recurring weaknesses b. Number of identified weaknesses resolved
Activities	**Capability Level**
1. Agree on and implement internally, within the organization, the necessary actions that need to be taken to resolve identified weaknesses and gaps.	2
2. Follow up, within the organization, to determine whether corrective actions were taken and internal control weaknesses were resolved.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

B. Component: Organizational Structures														
Key Management Practice	Chief Operating Officer	Chief Risk Officer	Chief Information Officer	Chief Technology Officer	Enterprise Risk Committee	Business Process Owners	Data Management Function	Head IT Operations	Service Manager	Information Security Manager	Business Continuity Manager	Legal Counsel	Audit
MEA04.01 Ensure that assurance providers are independent and qualified.			R	R	R	R						R	A
MEA04.02 Develop risk-based planning of assurance initiatives.	R	R	R	R		R						R	A
MEA04.03 Determine the objectives of the assurance initiative.	R	R	R	R		R						R	A
MEA04.04 Define the scope of the assurance initiative.	R	R	R	R		R						R	A
MEA04.05 Define the work program for the assurance initiative.	R		R	R		R						R	A
MEA04.06 Execute the assurance initiative, focusing on design effectiveness.	R		R	R		R	R	R	R	R	R	R	A
MEA04.07 Execute the assurance initiative, focusing on operating effectiveness.	R		R	R		R	R	R	R	R	R	R	A
MEA04.08 Report and follow up on the assurance initiative.	R		R	R		R						R	A
MEA04.09 Follow up on recommendations and actions.	R	R	A	R		R		R				R	R

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	Inputs		Outputs	
	From	Description	Description	To
MEA04.01 Ensure that assurance providers are independent and qualified.			Results of assurance provider evaluations	Internal
MEA04.02 Develop risk-based planning of assurance initiatives.	BAI01.05	Program audit plans	Assurance plans	All APO; All BAI; All DSS; All MEA; EDM01.03
	DSS01.02	Independent assurance plans	Assessment criteria	Internal
			High-level assessments	Internal
MEA04.03 Determine the objectives of the assurance initiative.	MEA04.02	Assurance plans	Assurance objectives and expected benefits	Internal
MEA04.04 Define the scope of the assurance initiative.	APO11.03	Root causes of failure to deliver quality	Assurance review practices	Internal
	APO12.06	Risk-related root causes	Engagement plan	Internal
	DSS06.01	Root cause analyses and recommendations		
	MEA03.04	Reports of noncompliance issues and root causes	Assurance review scope	Internal

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
MEA04.05 Define the work program for the assurance initiative.	**From**	**Description**	**Description**	**To**
	APO12.04	Risk analysis and risk profile reports for stakeholders	Refined scope	Internal
			Detailed assurance work program	MEA04.06
MEA04.06 Execute the assurance initiative, focusing on design effectiveness.	APO12.06	Risk-related root causes	Documented design of internal controls	MEA04.07
	DSS06.01	Root cause analyses and recommendations		
	MEA04.05	Detailed assurance work program		
MEA04.07 Execute the assurance initiative, focusing on operating effectiveness.	DSS02.02	Incident and service request log	Control effectiveness testing	MEA04.08; MEA04.09
	DSS02.05	Incident resolutions		
	DSS03.05	Problem resolution monitoring reports		
	DSS05.02	Results of penetration tests		
	DSS05.05	Access logs		
	DSS06.01	Root cause analyses and recommendations		
	MEA04.06	Documented design of internal controls		
MEA04.08 Report and follow up on the assurance initiative.	MEA03.03	Identified compliance gaps	Assurance review report	All APO; All BAI; All DSS; All MEA; EDM05.03
	MEA04.07	Control effectiveness testing	Assurance review results	All APO; All BAI; All DSS; All MEA; EDM05.03; MEA04.09
MEA04.09 Follow up on recommendations and actions.	MEA04.07	Control effectiveness testing	Remedial actions	All APO; All BAI; All DSS; All MEA
	MEA04.08	Assurance review results		
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
No related guidance for this component				

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
A number of core principles, described by the Institute of Internal Auditors®, support the effectiveness and efficiency of the (internal) audit function. These principles include, among others, the importance of independence, effective communication skills, proactiveness, etc.	Core Principles for the Professional Practice of Internal Auditing, The Institute of Internal Auditors	cfr. IIA website—Standards & Guidance - Core Principles
Risk management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.3. Risk Management

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Assurance guide	Provides guidance on performing assurance activities. Enables efficient and effective development of I&T assurance initiatives, including planning, scoping and executing assurance reviews, based on well-accepted assurance approaches. Provides assurance steps to test the control design, test the outcome of the operational effectiveness of the control, and document control weaknesses and their impact.		
Internal audit charter	Provides independence to undertake audit reviews and report findings and recommendations directly to top management. The internal audit function should be a separate entity reporting either to the chief executive officer or chief operating officer. With respect to I&T, the charter should stipulate that the function is responsible for reviewing both general and application controls to determine whether the controls have been designed in accordance with management direction, established standards and procedures, and known legal requirements, and whether the controls are operating effectively to provide reliability and security over the data being processed (i.e., confidentiality, integrity and availability). The charter should stipulate that the internal audit function is responsible for reviewing the design, development and implementation of new systems or major modifications of existing systems.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Create a culture that embraces internal audit and assurance findings and recommendations, based on root cause analysis. Leaders must ensure that internal audit and assurance are involved in strategic initiatives and recognize the need for (and value of) audit and assurance reports.		
Ensure an ethical culture of internal auditing through an appropriate code of ethics.	Code of Ethics, The Institute of Internal Auditors	cfr. IIA website—Standards & Guidance—Code of Ethics

G. Component: Services, Infrastructure and Applications
• Assurance engagement tools • Event log auditing tools • Third-party assurance provisioning services

Appendices

5.1 Appendix A: Goals Cascade—Mapping Tables

The mapping tables in Appendix A inform the goals cascade. The first table maps alignment goals to enterprise goals; the second table maps governance and management objectives to alignment goals. The "P" in the table refers to primary and the "S" refers to secondary.

5.1.1 Mapping Table: Enterprise Goals—Alignment Goals

Figure 5.1—Mapping Enterprise Goals and Alignment Goals

		EG01	EG02	EG03	EG04	EG05	EG06	EG07	EG08	EG09	EG10	EG11	EG12	EG13
		Portfolio of competitive products and services	Managed business risk	Compliance with external laws and regulations	Quality of financial information	Customer-oriented service culture	Business service continuity and availability	Quality of management information	Optimization of internal business process functionality	Optimization of business process costs	Staff skills, motivation and productivity	Compliance with internal policies	Managed digital transformation programs	Product and business innovation
AG01	I&T compliance and support for business compliance with external laws and regulations		S	P								S		
AG02	Managed I&T-related risk		P				S							
AG03	Realized benefits from I&T-enabled investments and services portfolio	S				S			S	S			P	
AG04	Quality of technology-related financial information				P			P		P				
AG05	Delivery of I&T services in line with business requirements	P				S	S		S				S	
AG06	Agility to turn business requirements into operational solutions	P				S			S				S	S
AG07	Security of information, processing infrastructure and applications, and privacy		P				P							
AG08	Enabling and supporting business processes by integrating applications and technology	P				P			S		S		P	S
AG09	Delivering programs on time, on budget and meeting requirements and quality standards	P				S			S	S			P	S
AG10	Quality of I&T management information				P			P		S				
AG11	I&T compliance with internal policies		S	P								P		
AG12	Competent and motivated staff with mutual understanding of technology and business					S					P			
AG13	Knowledge, expertise and initiatives for business innovation	P		S									S	P

5.1.2 Mapping Table: Alignment Goals—Governance and Management Objectives

Figure—5.2 Mapping Governance and Management Objectives to Alignment Goals

		AG01	AG02	AG03	AG04	AG05	AG06	AG07	AG08	AG09	AG10	AG11	AG12	AG13
		I&T compliance and support for business compliance with external laws and regulations	Managed I&T-related risk	Realized benefits from I&T-enabled investments and services portfolio	Quality of technology-related financial information	Delivery of I&T services in line with business requirements	Agility to turn business requirements into operational solutions	Security of information, processing infrastructure and applications, and privacy	Enabling and supporting business processes by integrating applications and technology	Delivering programs on time, on budget and meeting requirements and quality standards	Quality of I&T management information	I&T compliance with internal policies	Competent and motivated staff with mutual understanding of technology and business	Knowledge, expertise and initiatives for business innovation
EDM01	Ensured governance framework setting and maintenance	P	S	P					S			S		
EDM02	Ensured benefits delivery			P		S	S		S					S
EDM03	Ensured risk optimization	S	P					P				S		
EDM04	Ensured resource optimization			S		S	S		S	P			S	
EDM05	Ensured stakeholder engagement				S						P	S		
APO01	Managed I&T management framework	S	S	P		S		S	S	S	S	P		
APO02	Managed strategy			S		S	S		P				S	S
APO03	Managed enterprise architecture			S		S	P	S	P					
APO04	Managed innovation			S			P		S				S	P
APO05	Managed portfolio			P		P	S		S	S				
APO06	Managed budget and costs			S	P					P	S			
APO07	Managed human resources			S		S				S			P	P
APO08	Managed relationships			S		P	P		S	S			P	P
APO09	Managed service agreements					P			S					
APO10	Managed vendors					P	S			S				
APO11	Managed quality			S	S	S				P	P			
APO12	Managed risk		P					P						
APO13	Managed security	S	S					P						
APO14	Managed data	S	S		S			S			P			
BAI01	Managed programs			P			S		S	P				
BAI02	Managed requirements definition			S		P	P		S	P			S	
BAI03	Managed solutions identification and build			S		P	P		S	P				
BAI04	Managed availability and capacity					P		S		S				
BAI05	Managed organizational changes			P		S	S		P	P			S	
BAI06	Managed IT changes		S			S	P		S					
BAI07	Managed IT change acceptance and transitioning		S				P			S				
BAI08	Managed knowledge			S			S		S	S			P	P
BAI09	Managed assets				P						S			
BAI10	Managed configuration					S		P						
BAI11	Managed projects			P		S	P			P				
DSS01	Managed operations					P			S					
DSS02	Managed service requests and incidents		S			P		S						
DSS03	Managed problems		S			P		S						
DSS04	Managed continuity		S			P		P						
DSS05	Managed security services	S	P			S		P				S		
DSS06	Managed business process controls		S			S		S	P			S		
MEA01	Managed performance and conformance monitoring	S		S		P				S	P	S		
MEA02	Managed system of internal control	S	S		S	S		S		S	S	P		
MEA03	Managed compliance with external requirements	P										S		
MEA04	Managed assurance	S	S		S	S		S			S	P		

5.2 Appendix B: Organizational Structures—Overview and Descriptions

Throughout the detailed guidance in Chapter 4, the organizational structures components draw from the roles and structures outlined in **figure 5.3** (see also section 3.5 for an overview of the organizational structures component).

Across enterprises, the nomenclature applied to each role or structure will likely differ. Based on the descriptions below, each enterprise may identify appropriate roles and structures—given its own business context, organization, and operating environment—and assign levels of accountability and responsibility accordingly.

Figure 5.3—COBIT Roles and Organizational Structures

Role/Structure	Description
Board	Group of the most senior executives and/or nonexecutive directors accountable for governance and overall control of enterprise resources
Executive Committee	Group of senior executives appointed by the board to ensure that the board is involved in, and kept informed of, major decisions (The executive committee is accountable for managing the portfolios of I&T-enabled investments, I&T services and I&T assets; ensuring that value is delivered; and managing risk. The committee is normally chaired by a board member.)
Chief Executive Officer	Highest-ranking officer charged with the total management of the enterprise
Chief Financial Officer	Most senior official accountable for all aspects of financial management, including financial risk and controls and reliable and accurate accounts
Chief Operating Officer	Most senior official accountable for operation of the enterprise
Chief Risk Officer	Most senior official accountable for all aspects of risk management across the enterprise (An I&T risk officer function may be established to oversee I&T-related risk.)
Chief Information Officer	Most senior official responsible for aligning IT and business strategies and accountable for planning, resourcing and managing delivery of I&T services and solutions
Chief Technology Officer	Most senior official tasked with technical aspects of I&T, including managing and monitoring decisions related to I&T services, solutions and infrastructures (This role may also be taken by the CIO.)
Chief Digital Officer	Most senior official tasked with putting into practice the digital ambition of the enterprise or business unit (This role may be taken by the CIO or another member of the executive committee.)
I&T Governance Board	Group of stakeholders and experts accountable for guiding I&T-related matters and decisions, including managing I&T-enabled investments, delivering value and monitoring risk
Architecture Board	Group of stakeholders and experts accountable for guiding enterprise architecture-related matters and decisions and for setting architectural policies and standards
Enterprise Risk Committee	Group of executives accountable for enterprise-level collaboration and consensus required to support enterprise risk management (ERM) activities and decisions (An I&T risk council may be established to consider I&T risk in more detail and advise the enterprise risk committee.)
Chief Information Security Officer	Most senior official accountable for all aspects of security management across the enterprise
Business Process Owner	Individual accountable for performing processes and/or realizing process objectives, driving process improvement and approving process changes
Portfolio Manager	Individual responsible for guiding portfolio management, ensuring selection of correct programs and projects, managing and monitoring programs and projects for optimal value, and realizing long-term strategic objectives effectively and efficiently
Steering (Programs/ Projects) Committee	Group of stakeholders and experts accountable for guiding programs and projects, including managing and monitoring plans, allocating resources, delivering benefits and value, and managing program and project risk
Program Manager	Individual responsible for guiding a specific program, including articulating and following up on goals and objectives of the program and managing risk and impact on the business

Figure 5.3—COBIT Roles and Organizational Structures *(cont.)*	
Role/Structure	**Description**
Project Manager	Individual responsible for guiding a specific project, including coordinating and delegating time, budget, resources and tasks across the project team
Project Management Office	Function responsible for supporting program and project managers and for gathering, assessing and reporting information about the conduct of programs and constituent projects
Data Management Function	Function responsible for supporting enterprise data assets across the data life cycle and managing data strategy, infrastructure and repositories
Head Human Resources	Most senior official accountable for planning and policies regarding human resources in the enterprise
Relationship Manager	Senior individual responsible for overseeing and managing the internal interface and communications between business and I&T functions
Head Architect	Senior individual accountable for the enterprise architecture process
Head Development	Senior individual accountable for I&T–related solution development processes
Head IT Operations	Senior individual accountable for IT operational environments and infrastructure
Head IT Administration	Senior individual accountable for I&T–related records and responsible for supporting I&T–related administrative matters
Service Manager	Individual who manages the development, implementation, evaluation and ongoing maintenance of new and existing products and services for a specific customer (user) or group of customers (users)
Information Security Manager	Individual who manages, designs, oversees and/or assesses an enterprise's information security
Business Continuity Manager	Individual who manages, designs, oversees and/or assesses an enterprise's business continuity capability, to ensure that the enterprise's critical functions continue to operate following disruptive events
Privacy Officer	Individual responsible for monitoring risk and business impact of privacy laws and for guiding and coordinating the implementation of policies and activities that ensure compliance with privacy directives (In some enterprises, the position may be referenced as the data protection officer.)
Legal Counsel	Function responsible for guidance on legal and regulatory matters
Compliance	Function responsible for all guidance on external compliance
Audit	Function responsible for provision of internal audits

5.3 Appendix C: Detailed List of References

The following standards and guidance contribute to the detailed references to the 40 core COBIT® 2019 governance and management objectives.

- CIS® Center for Internet Security®, *The CIS Critical Security Controls for Effective Cyber Defense*, Version 6.1, August 2016
- CMMI® Cybermaturity Platform, 2018
- CMMI® Data Management Maturity (DMM)℠ model, 2014
- 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)
- Information Technology Infrastructure Library (ITIL®) v3, 2011
- Institute of Internal Auditors® (IIA®), "Core Principles for the Professional Practice of Internal Auditing"• *King IV Report on Corporate Governance™*, 2016
- *King IV Report on Corporate Governance™*, 2016
- 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
- *A Guide to the Project Management Body of Knowledge: PMBOK® Guide Sixth Edition*, 2017
- 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

Page intentionally left blank