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 enterprise governance of information and technology (EGIT), 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, enterprise governance of information and technology (EGIT), 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

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
Bart Peeters, 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
Andre Pitkowski, CRISC, CGEIT, CRMA-IIA, OCTAVE, SM, APIT Consultoria de Informatica Ltd., Brazil
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

Acknowledgments *(cont.)*

Expert Reviewers (cont.)

John Thorp, CMC, ISP, ITCP, The Thorp Network, Canada
Greet Volders, CGEIT, COBIT Assessor, Voquals N.V., Belgium
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, CISM, Clyde Consulting LLC, USA, Chair
Brennan Baybeck, CISA, CRISC, CISM, CISSP, Oracle Corporation, USA, Vice-Chair
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

LIST OF FIGURES

Chapter 1. Introduction to COBIT® 2019

Chapter 3. Structure of COBIT Governance and Management Objectives

Appendices

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.

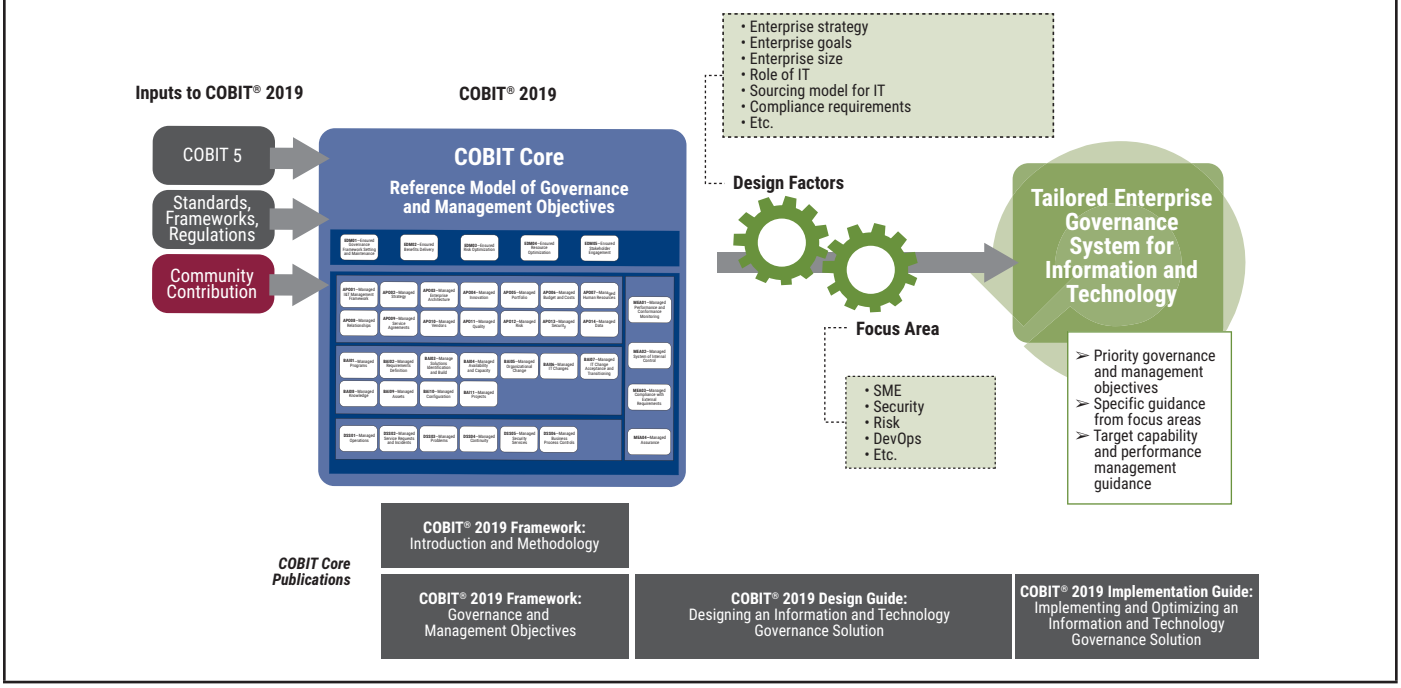
1.2 Overview of COBIT® 2019

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:

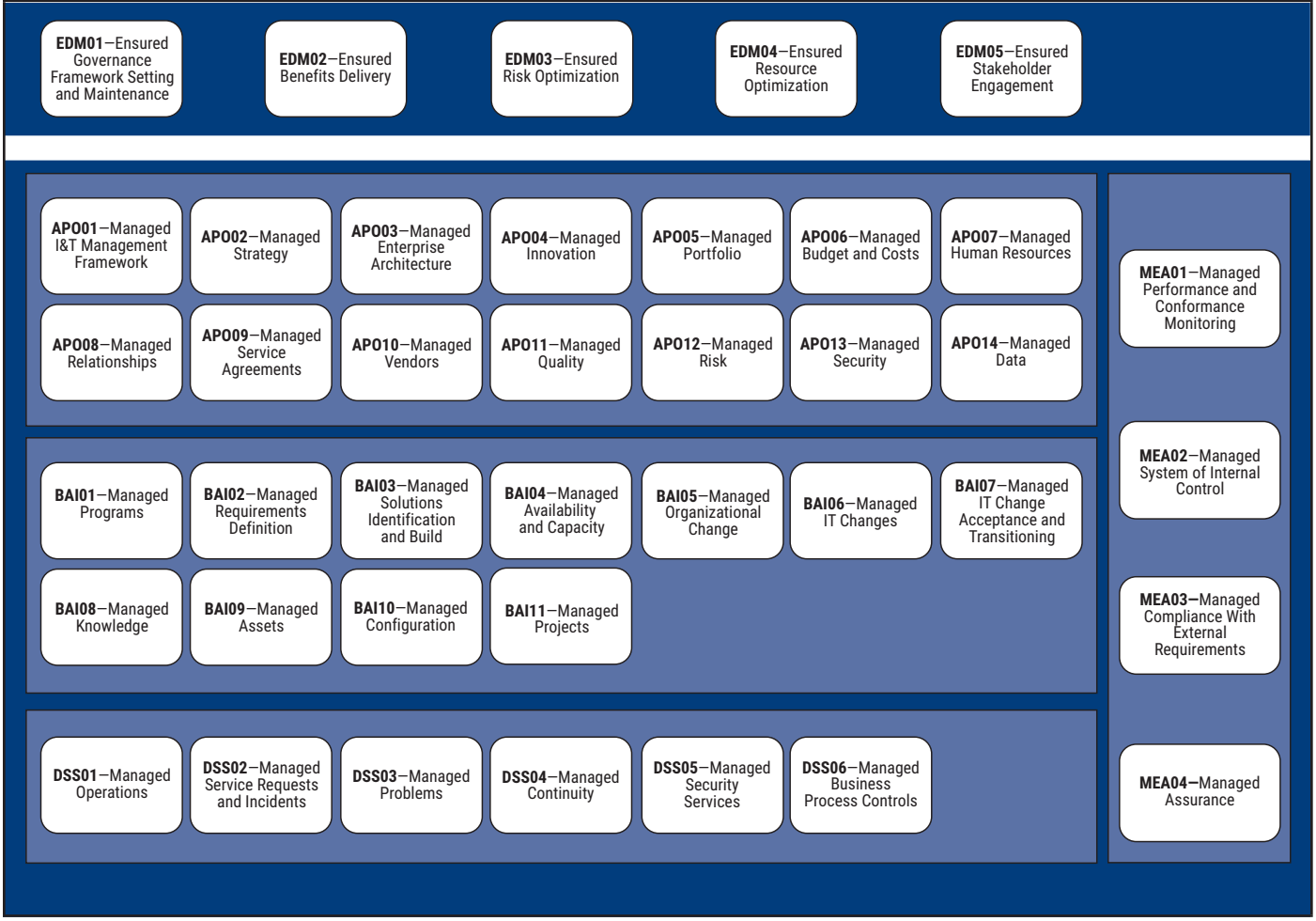
- A governance or management objective **always relates to one process** (with an identical or similar name) and a series of related components of other types to help achieve the objective.
- A governance objective relates to a governance process (depicted on the dark blue background in **figure 1.2**), 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

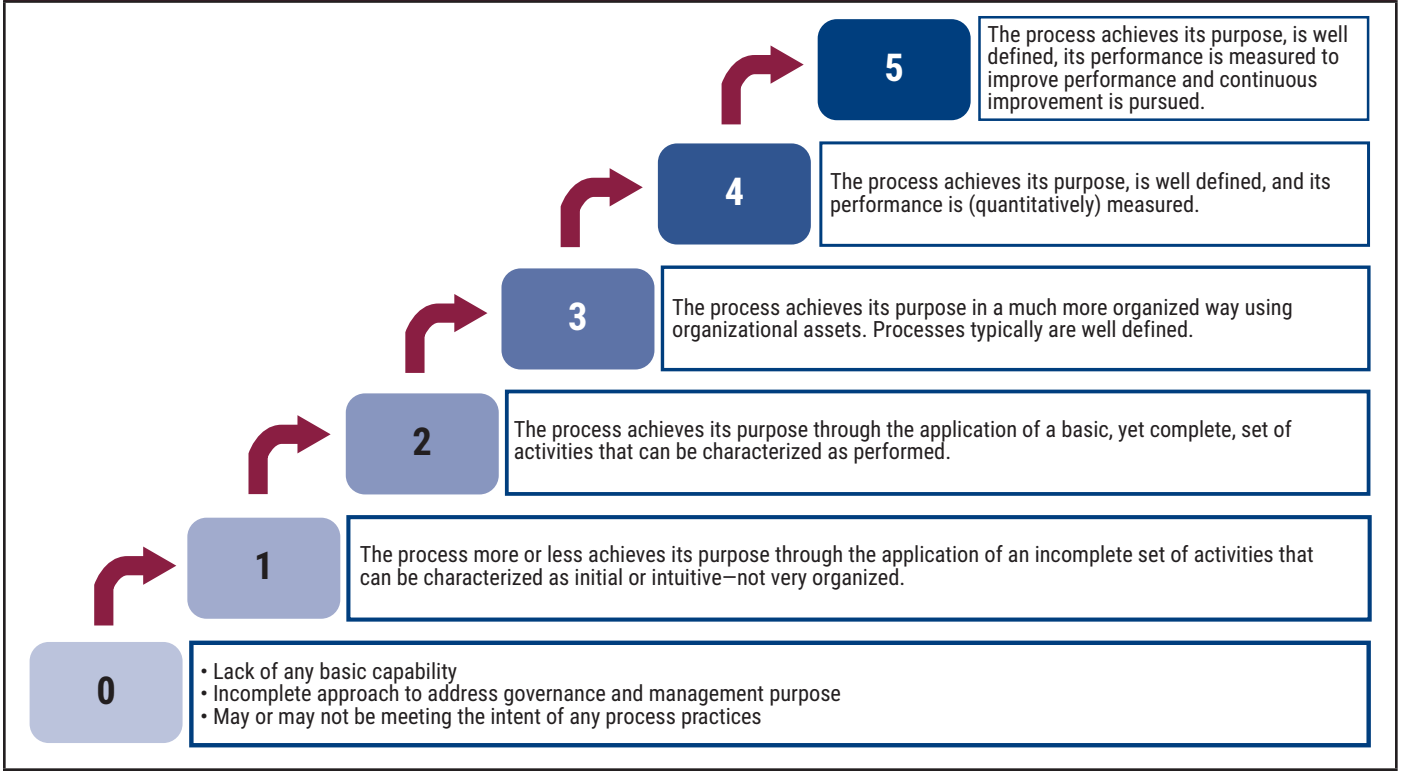
A. Component: Process	
Governance/Management Practice	**Example Metrics**
<REF> <NAME> <DESCRIPTION>	<METRIC>

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	
EDM04.01 Evaluate resource management.	**From**	**Description**	**Description**	**To**
	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