COBIT® 2019

FRAMEWORK

Introduction and Methodology

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: Introduction and Methodology* (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: Introduction and Methodology
ISBN 978-1-60420-763-7

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, Ph.D., 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, 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
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

Acknowledgments *(cont.)*

Expert Reviewers

Peter Tessin, CISA, CRISC, CISM, CGEIT, Discover, USA
Mark Thomas, CRISC, CGEIT, Escoute, USA
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 9

Chapter 1. Introduction 11
1.1 Enterprise Governance of Information and Technology 11
1.2 Benefits of Information and Technology Governance 11
1.3 COBIT as an I&T Governance Framework 12
1.3.1 What Is COBIT and What Is It Not? 13
1.4 Structure of This Publication 14

Chapter 2. Intended Audience 15
2.1 Governance Stakeholders 15

Chapter 3. COBIT Principles 17
3.1 Introduction 17
3.2 Six Principles for a Governance System 17
3.3 Three Principles for a Governance Framework 18
3.4 COBIT® 2019 18

Chapter 4. Basic Concepts: Governance System and Components 19
4.1 COBIT Overview 19
4.2 Governance and Management Objectives 20
4.3 Components of the Governance System 21
4.4 Focus Areas 22
4.5 Design Factors 23
4.6 Goals Cascade 28
4.6.1 Enterprise Goals 29
4.6.2 Alignment Goals 30

Chapter 5. COBIT Governance and Management Objectives 33
5.1 Purpose 33

Chapter 6. Performance Management in COBIT 37
6.1 Definition 37
6.2 COBIT Performance Management Principles 37
6.3 COBIT Performance Management Overview 37
6.4 Managing Performance of Processes 38
6.4.1 Process Capability Levels 38
6.4.2 Rating Process Activities 39
6.4.3 Focus Area Maturity Levels 39
6.5 Managing Performance of Other Governance System Components 40
6.5.1 Performance Management of Organizational Structures 40
6.5.2 Performance Management of Information Items 41
6.5.3 Performance Management of Culture and Behavior 43

Chapter 7. Designing a Tailored Governance System 45
7.1 Impact of Design Factors 45
7.2 Stages and Steps in the Design Process 47

Chapter 8. Implementing Enterprise Governance of IT 49
8.1 COBIT Implementation Guide Purpose 49
8.2 COBIT Implementation Approach 49

8.2.1 Phase 1—What Are the Drivers? 50
8.2.2 Phase 2—Where Are We Now? 50
8.2.3 Phase 3—Where Do We Want to Be? 51
8.2.4 Phase 4—What Needs to Be Done? 51
8.2.5 Phase 5—How Do We Get There? 51
8.2.6 Phase 6—Did We Get There? 51
8.2.7 Phase 7—How Do We Keep the Momentum Going? 51
8.3 Relationship Between *COBIT® 2019 Design Guide* and *COBIT® 2019 Implementation Guide* 52

Chapter 9. Getting Started With COBIT: Making the Case 53
9.1 Business Case 53
9.2 Executive Summary 53
9.3 Background 54
9.4 Business Challenges 55
9.4.1 Gap Analysis and Goal 55
9.4.2 Alternatives Considered 56
9.5 Proposed Solution 56
9.5.1 Phase 1. Pre-planning 56
9.5.2 Phase 2. Program Implementation 57
9.5.3 Program Scope 57
9.5.4 Program Methodology and Alignment 57
9.5.5 Program Deliverables 58
9.5.6 Program Risk 58
9.5.7 Stakeholders 59
9.5.8 Cost-Benefit Analysis 59
9.5.9 Challenges and Success Factors 60

Chapter 10. COBIT and Other Standards 63
10.1 Guiding Principle 63
10.2 List of Referenced Standards 63

LIST OF FIGURES

Chapter 1. Introduction

Figure 1.1—The Context of Enterprise Governance of Information and Technology....11

Chapter 2. Intended Audience

Figure 2.1—COBIT Stakeholders....15

Chapter 3. COBIT Principles

Figure 3.1—Governance System Principles....17
Figure 3.2—Governance Framework Principles....18

Chapter 4. Basic Concepts: Governance System and Components

Figure 4.1—COBIT Overview....19
Figure 4.2—COBIT Core Model....21
Figure 4.3—COBIT Components of a Governance System....22
Figure 4.4—COBIT Design Factors....23
Figure 4.5—Enterprise Strategy Design Factor....23
Figure 4.6—Enterprise Goals Design Factor....24
Figure 4.7—Risk Profile Design Factors (IT Risk Categories)....24
Figure 4.8—I&T-Related Issues Design Factor....25
Figure 4.9—Threat Landscape Design Factor....25
Figure 4.10—Compliance Requirements Design Factor....26
Figure 4.11—Role of IT Design Factor....26
Figure 4.12—Sourcing Model for IT Design Factor....26
Figure 4.13—IT Implementation Methods Design Factor....27
Figure 4.14—Technology Adoption Strategy Design Factor....27
Figure 4.15—Enterprise Size Design Factor....27
Figure 4.16—COBIT Goals Cascade....28
Figure 4.17—Goals Cascade: Enterprise Goals and Metrics....29
Figure 4.18—Goals Cascade: Alignment Goals and Metrics....30

Chapter 5. COBIT Governance and Management Objectives

Figure 5.1—COBIT Core Model: Governance and Management Objectives and Purpose....33

Chapter 6. Performance Management in COBIT

Figure 6.1—Capability Levels....38
Figure 6.2—Capability Levels for Processes....39
Figure 6.3—Maturity Levels for Focus Areas....40
Figure 6.4—Information Reference Model: Quality Criteria for Information....42

Chapter 7. Designing a Tailored Governance System

Figure 7.1—Impact of Design Factors on a Governance and Management System....45
Figure 7.2—Governance System Design Workflow....47

Chapter 8. Implementing Enterprise Governance of IT

Figure 8.1—COBIT Implementation Road Map....50
Figure 8.2—Connection Points Between *COBIT Design Guide* and *COBIT Implementation Guide*....52

Chapter 9. Getting Started With COBIT: Making the Case

Figure 9.1—Challenges and Planned Actions for Acme Corporation....60

Page intentionally left blank

Chapter 1
Introduction

1.1 Enterprise Governance of Information and Technology

In the light of digital transformation, information and technology (I&T) have become crucial in the support, sustainability and growth of enterprises. Previously, governing boards (boards of directors) and senior management could delegate, ignore or avoid I&T-related decisions. In most sectors and industries, such attitudes are now ill-advised. Stakeholder value creation (i.e., realizing benefits at an optimal resource cost while optimizing risk) is often driven by a high degree of digitization in new business models, efficient processes, successful innovation, etc. Digitized enterprises are increasingly dependent on I&T for survival and growth.

Given the centrality of I&T for enterprise risk management and value generation, a specific focus on enterprise governance of information and technology (EGIT) has arisen over the last three decades. EGIT is an integral part of corporate governance. It is exercised by the board that oversees the definition and implementation of processes, structures and relational mechanisms in the organization that enable both business and IT people to execute their responsibilities in support of business/IT alignment and the creation of business value from I&T-enabled business investments (**figure 1.1**).

Figure 1.1—The Context of Enterprise Governance of Information and Technology

Source: De Haes, Steven; W. Van Grembergen; *Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5*, 2nd ed., Springer International Publishing, Switzerland, 2015, *https://www.springer.com/us/book/9783319145464*

Enterprise governance of information and technology is complex and multifaceted. There is no silver bullet (or ideal way) to design, implement and maintain effective EGIT within an organization. As such, members of the governing boards and senior management typically need to tailor their EGIT measures and implementation to their own specific context and needs. They must also be willing to accept more accountability for I&T and drive a different mindset and culture for delivering value from I&T.

1.2 Benefits of Information and Technology Governance

Fundamentally, EGIT is concerned with value delivery from digital transformation and the mitigation of business risk that results from digital transformation. More specifically, three main outcomes can be expected after successful adoption of EGIT:

- **Benefits realization**—This consists of creating value for the enterprise through I&T, maintaining and increasing value derived from existing I&T[1] investments, and eliminating IT initiatives and assets that are not creating sufficient value. The basic principle of I&T value are delivery of fit-for-purpose services and solutions, on time

[1] Throughout this text, IT is used to refer to the organizational department with main responsibility for technology. I&T as used in this text refers to all the information the enterprise generates, processes and uses to achieve its goals, as well as the technology to support that throughout the enterprise.

and within budget, that generate the intended financial and nonfinancial benefits. The value that I&T delivers should be aligned directly with the values on which the business is focused. IT value should also be measured in a way that shows the impact and contributions of IT-enabled investments in the value creation process of the enterprise.

- **Risk optimization**—This entails addressing the business risk associated with the use, ownership, operation, involvement, influence and adoption of I&T within an enterprise. I&T-related business risk consists of I&T-related events that could potentially impact the business. While value delivery focuses on the *creation* of value, risk management focuses on the *preservation* of value. The management of I&T-related risk should be integrated within the enterprise risk management approach to ensure a focus on IT by the enterprise. It should also be measured in a way that shows the impact and contributions of optimizing I&T-related business risk on preserving value.
- **Resource optimization**—This ensures that the appropriate capabilities are in place to execute the strategic plan and sufficient, appropriate and effective resources are provided. Resource optimization ensures that an integrated, economical IT infrastructure is provided, new technology is introduced as required by the business, and obsolete systems are updated or replaced. Because it recognizes the importance of people, in addition to hardware and software, it focuses on providing training, promoting retention and ensuring competence of key IT personnel. An important resource is data and information, and exploiting data and information to gain optimal value is another key element of resource optimization.

Strategic alignment and performance measurement are of paramount importance and apply overall to all activities to ensure that I&T-related objectives are aligned with the enterprise goals.

In a large case study of an international airline company, EGIT's benefits were demonstrated to include: lower IT-related continuity costs, increased IT-enabled innovation capacity, increased alignment between digital investments and business goals and strategy, increased trust between business and IT, and a shift toward a "value mindset" around digital assets.[2]

Research has shown that enterprises with poorly designed or adopted approaches to EGIT perform worse in aligning business and I&T strategies and processes. As a result, such enterprises are much less likely to achieve their intended business strategies and realize the business value they expect from digital transformation.[3]

From this, it is clear that governance has to be understood and implemented much beyond the often encountered (i.e., narrow) interpretation suggested by the governance, risk and compliance (GRC) acronym. The GRC acronym itself implicitly suggests that compliance and related risk represent the spectrum of governance.

1.3 COBIT as an I&T Governance Framework

Over the years, best-practice frameworks have been developed and promoted to assist in the process of understanding, designing and implementing 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 practices.

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

[2] De Haes, S.; W. van Grembergen; *Enterprise Governance of IT: Achieving Alignment and Value, Featuring COBIT 5*, Springer International Publishing, Switzerland, 2nd ed. 2015, *https://www.springer.com/us/book/9783319145464*

[3] De Haes, Steven; A. Joshi; W. van Grembergen; "State and Impact of Governance of Enterprise IT in Organizations: Key Findings of an International Study," *ISACA® Journal*, vol. 4, 2015, *https://www.isaca.org/Journal/archives/2015/Volume-4/Pages/state-and-impact-of-governance-of-enterprise-it-in-organizations.aspx*. See also *op cit* De Haes and van Grembergen.

1.3.1 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 enterprise information and technology,[4] 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, overall 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 the 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.[5]

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.

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.

[4] Throughout this publication, references to the "framework for the governance of IT" imply the entirety of this description.
[5] These components were termed enablers in COBIT® 5.

1.4 Structure of This Publication

The remainder of this publication contains the following chapters:

- Chapter 2 discusses the target audience for COBIT.
- Chapter 3 explains the principles for governance systems for I&T, and the principles for good governance frameworks.
- Chapter 4 explains the basic concepts and terminology of COBIT® 2019, including the updated core COBIT model with its 40 governance and management objectives.
- Chapter 5 elaborates on the 40 governance and management objectives.
- Chapter 6 explains how performance monitoring in COBIT® 2019 is conceived and, in particular, how Capability Maturity Model Integration (CMMI®)-inspired capability levels are introduced.
- Chapter 7 contains a brief introduction and overview of the workflow of the *COBIT® 2019 Design Guide*.
- Chapter 8 contains a brief introduction and overview of the *COBIT® 2019 Implementation Guide*.
- Chapter 9 contains a detailed example to illustrate making the case for the adoption and implementation of COBIT in an enterprise.
- Chapter 10 lists the standards, frameworks and regulations that have been used during the development of COBIT® 2019.

Chapter 2
Intended Audience

2.1 Governance Stakeholders

The target audience for COBIT is the stakeholders for EGIT and, by extension, stakeholders for corporate governance. These stakeholders and the benefits they can gain from COBIT are shown in **figure 2.1**.

Figure 2.1—COBIT Stakeholders

Stakeholder	Benefit of COBIT
Internal Stakeholders	
Boards	Provides insights on how to get value from the use of I&T and explains relevant board responsibilities
Executive Management	Provides guidance on how to organize and monitor performance of I&T across the enterprise
Business Managers	Helps to understand how to obtain the I&T solutions enterprises require and how best to exploit new technology for new strategic opportunities
IT Managers	Provides guidance on how best to build and structure the IT department, manage performance of IT, run an efficient and effective IT operation, control IT costs, align IT strategy to business priorities, etc.
Assurance Providers	Helps to manage dependency on external service providers, get assurance over IT, and ensure the existence of an effective and efficient system of internal controls
Risk Management	Helps to ensure the identification and management of all IT-related risk
External Stakeholders	
Regulators	Helps to ensure the enterprise is compliant with applicable rules and regulations and has the right governance system in place to manage and sustain compliance
Business Partners	Helps to ensure that a business partner's operations are secure, reliable and compliant with applicable rules and regulations
IT Vendors	Helps to ensure that an IT vendor's operations are secure, reliable and compliant with applicable rules and regulations

A certain level of experience and a thorough understanding of the enterprise are required to benefit from the COBIT framework. Such experience and understanding allow users to customize core COBIT guidance—which is generic in nature—into tailored and focused guidance for the enterprise, taking into account the enterprise's context.

The target audience includes those responsible during the whole life cycle of the governance solution, from design to execution to assurance. Indeed, assurance providers may apply the logic and workflow developed in this publication to create a well substantiated assurance program for the enterprise.

Page intentionally left blank

Chapter 3
COBIT Principles

3.1 Introduction

COBIT® 2019 was developed based on two sets of principles:

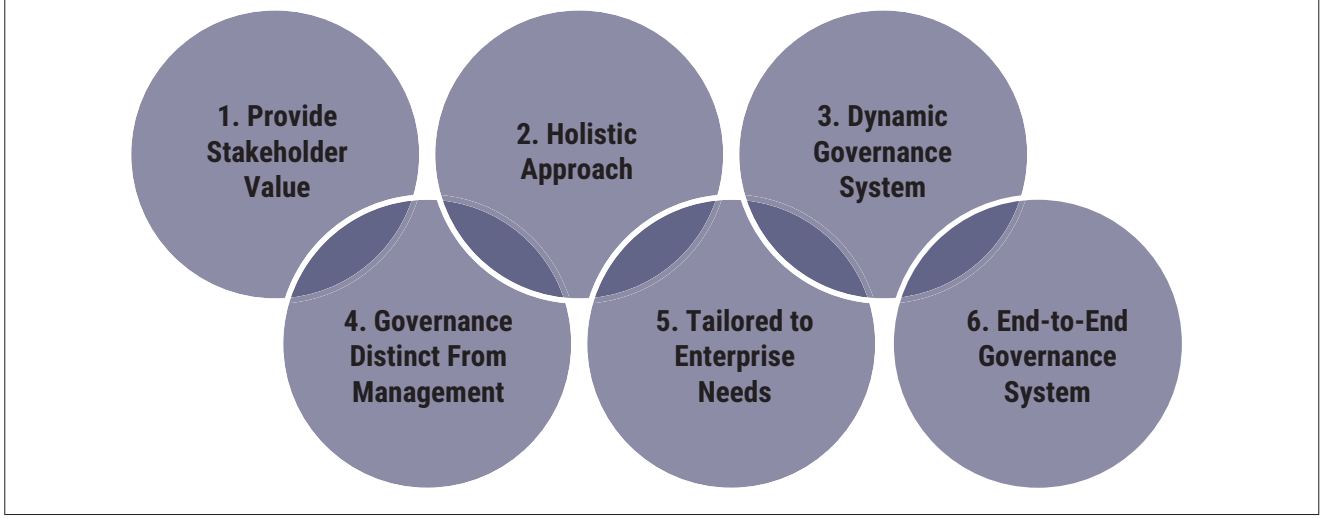
- Principles that describe the core requirements of a **governance system** for enterprise information and technology
- Principles for a **governance framework** that can be used to build a governance system for the enterprise

3.2 Six Principles for a Governance System

The six principles for a governance system are (**figure 3.1**):

1. Each enterprise needs a governance system to satisfy stakeholder needs and to generate value from the use of I&T. Value reflects a balance among benefits, risk and resources, and enterprises need an actionable strategy and governance system to realize this value.
2. A governance system for enterprise I&T is built from a number of components that can be of different types and that work together in a holistic way.
3. A governance system should be dynamic. This means that each time one or more of the design factors are changed (e.g., a change in strategy or technology), the impact of these changes on the EGIT system must be considered. A dynamic view of EGIT will lead toward a viable and future-proof EGIT system.
4. A governance system should clearly distinguish between governance and management activities and structures.
5. A governance system should be tailored to the enterprise's needs, using a set of design factors as parameters to customize and prioritize the governance system components.
6. A governance system should cover the enterprise end to end, focusing not only on the IT function but on all technology and information processing the enterprise puts in place to achieve its goals, regardless where the processing is located in the enterprise.[6]

Figure 3.1—Governance System Principles



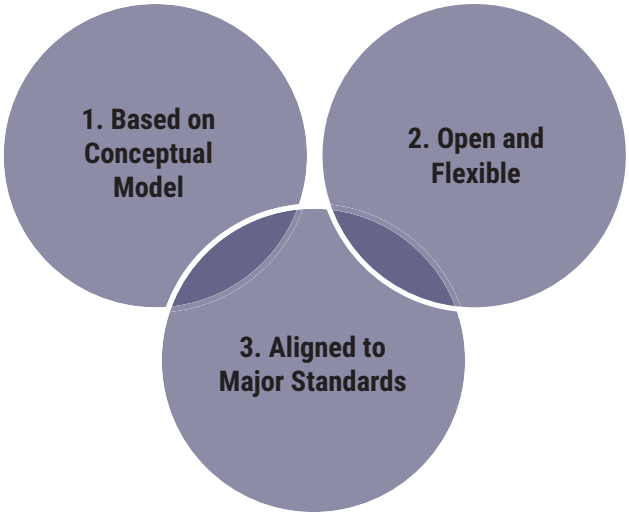
[6] Huygh, T.; S. De Haes; "Using the Viable System Model to Study IT Governance Dynamics: Evidence from a Single Case Study," *Proceedings of the 51st Hawaii International Conference on System Sciences*, 2018, *https://scholarspace.manoa.hawaii.edu/bitstream/10125/50501/1/paper0614.pdf*

3.3 Three Principles for a Governance Framework

The three principles for a governance framework are (**figure 3.2**):

1. A governance framework should be based on a conceptual model, identifying the key components and relationships among components, to maximize consistency and allow automation.
2. A governance framework should be open and flexible. It should allow the addition of new content and the ability to address new issues in the most flexible way, while maintaining integrity and consistency.
3. A governance framework should align to relevant major related standards, frameworks and regulations.

Figure 3.2—Governance Framework Principles



3.4 COBIT® 2019

COBIT® 2019 improves on prior versions of COBIT in the following areas:

- **Flexibility and openness**—The definition and use of design factors allow COBIT to be tailored for better alignment with a user's particular context. The COBIT open architecture enables adding new focus areas (see section 4.4) or modifying existing ones, without direct implications for the structure and content of the COBIT core model.
- **Currency and relevance**—The COBIT model supports referencing and alignment to concepts originating in other sources (e.g., the latest IT standards and compliance regulations).
- **Prescriptive application**—Models such as COBIT can be descriptive and prescriptive. The COBIT conceptual model is constructed and presented such that its instantiation (i.e., the application of tailored COBIT governance components) is perceived as a prescription for a tailored IT governance system.
- **Performance management of IT**—The structure of the COBIT performance management model is integrated into the conceptual model. The maturity and capability concepts are introduced for better alignment with CMMI.

COBIT guidance uses the terms governance of enterprise information and technology, enterprise governance of information and technology, governance of IT and IT governance interchangeably.

Chapter 4
Basic Concepts: Governance System and Components

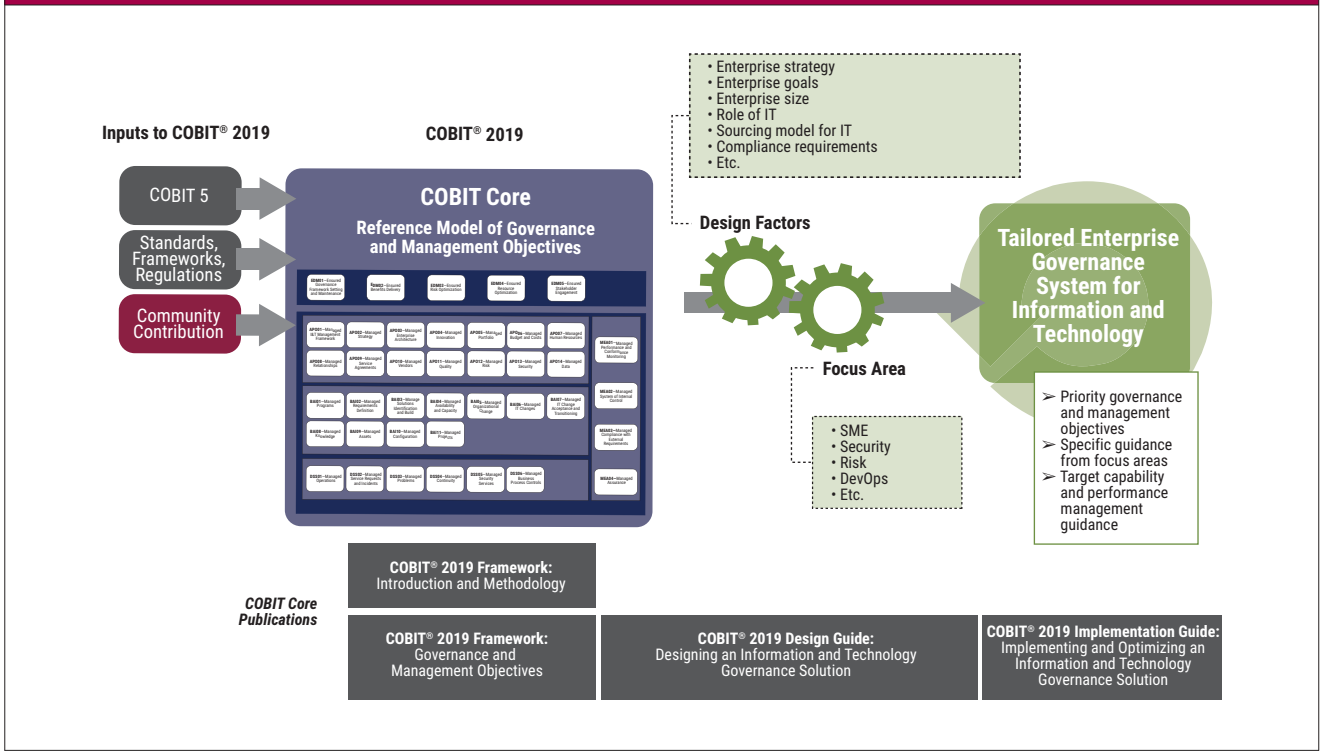
4.1 COBIT Overview

The COBIT® 2019 product family is open-ended and designed for customization. The following publications are currently available:[7]

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

Figure 4.1—COBIT Overview



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

The content identified as focus areas in **figure 4.1** will contain more detailed guidance on specific themes.[8]

COBIT® 2019 is based on COBIT® 5 and other authoritative sources. COBIT is aligned to a number of related standards and frameworks. The list of these standards is included in Chapter 10. The analysis of related standards and COBIT's alignment to them underly COBIT's established position of being the umbrella I&T governance framework.

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.

4.2 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:

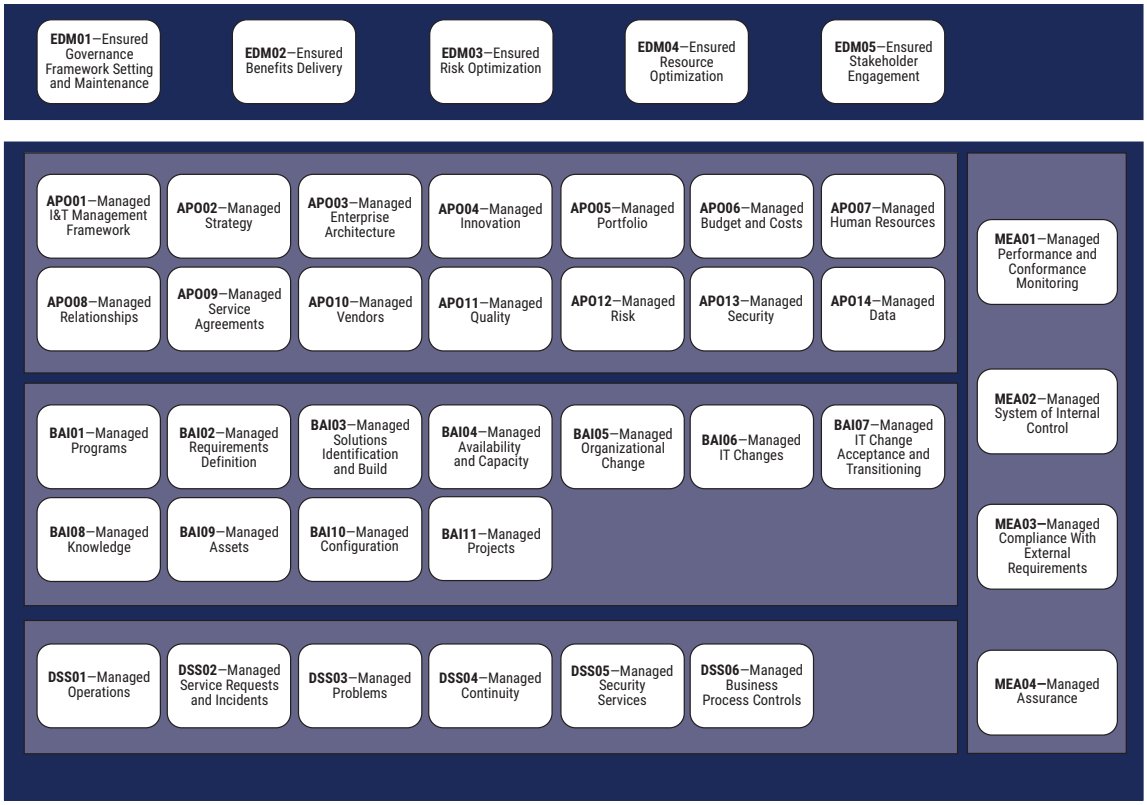
- A governance or management objective **always relates to one process** (with an identical or similar name) and a series of related components of other types to help achieve the objective.
- A governance objective relates to a governance process (depicted in the dark blue background in **figure 4.2**), while a management objective relates to a management process (depicted on the lighter blue background in **figure 4.2**). 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 objective 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.

[8] 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 4.2—COBIT Core Model



4.3 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 4.3**).
  - **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 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 4.3—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 4.2**) 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).

4.4 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.[9] Focus areas may contain a combination of generic governance components and variants.

[9] 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.

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.

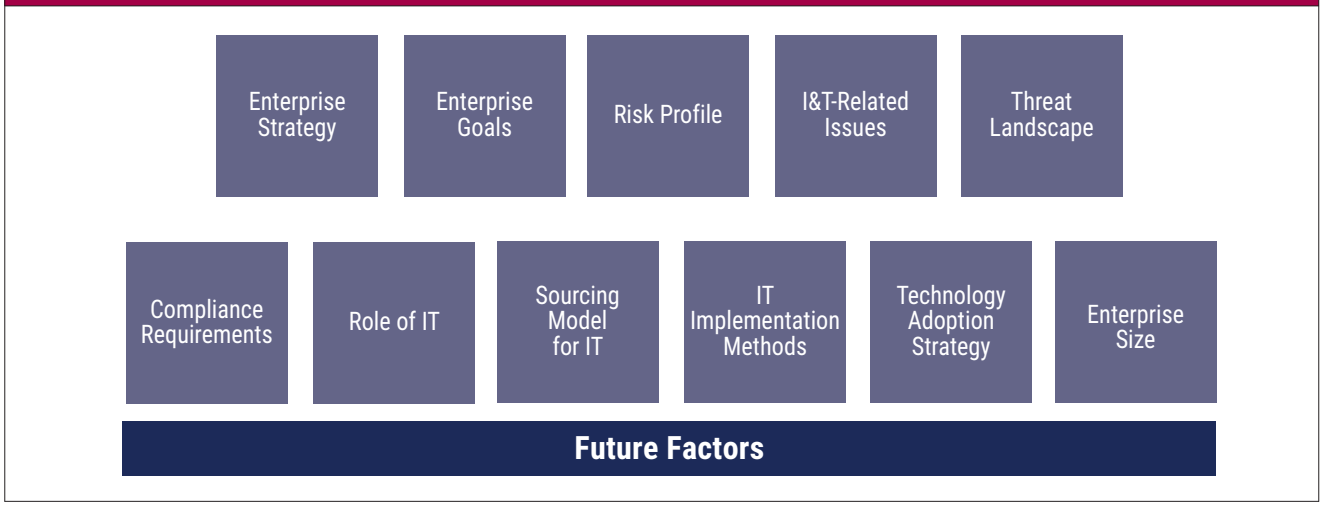
4.5 Design Factors

Design factors are factors that can influence the design of an enterprise's governance system and position it for success in the use of I&T.

The potential impacts design factors can have on the governance system are noted in section 7.1. More information and detailed guidance on how to use the design factors for designing a governance system can be found in the *COBIT® 2019 Design Guide*.

Design factors include any combination of the following (**figure 4.4**):

Figure 4.4—COBIT Design Factors



1. **Enterprise strategy**—Enterprises can have different strategies, which can be expressed as one or more of the archetypes shown in **figure 4.5**. Organizations typically have a primary strategy and, at most, one secondary strategy.

Figure 4.5—Enterprise Strategy Design Factor

Strategy Archetype	Explanation
Growth/Acquisition	The enterprise has a focus on growing (revenues).[10]
Innovation/Differentiation	The enterprise has a focus on offering different and/or innovative products and services to their clients.[11]
Cost Leadership	The enterprise has a focus on short-term cost minimization.[12]
Client Service/Stability	The enterprise has a focus on providing stable and client-oriented service.[13]

[10] Corresponds with prospector in the Miles-Snow typology. See "Miles and Snow's Typology of Defender, Prospector, Analyzer, and Reactor," Elibrary, *https://ebrary.net/3737/management/miles_snows_typology_defender_prospector_analyzer_reactor*.

[11] See Reeves, Martin; Claire Love, Philipp Tillmanns, "Your Strategy Needs a Strategy," *Harvard Business Review*, September 2012, *https://hbr.org/2012/09/your-strategy-needs-a-strategy*, specifically regarding visionary and shaping.

[12] Corresponds to cost leadership; see University of Cambridge, "Porter's Generic Competitive Strategies (ways of competing)," Institute for Manufacturing (IfM) Management Technology Policy, *https://www.ifm.eng.cam.ac.uk/research/dstools/porters-generic-competitive-strategies/*. Also corresponds to operational excellence; see Treacy, Michael; Fred Wiersema, "Customer Intimacy and Other Value Disciplines," *Harvard Business Review*, January/February 1993, *https://hbr.org/1993/01/customer-intimacy-and-other-value-disciplines*

[13] Corresponds with defenders in the Miles-Snow typology. See *op cit* "Miles and Snow's Typology of Defender, Prospector, Analyzer, and Reactor."

2. **Enterprise goals** supporting the enterprise strategy—Enterprise strategy is realized by the achievement of (a set of) enterprise goals. These goals are defined in the COBIT framework, structured along the balanced scorecard (BSC) dimensions, and include the elements shown in **figure 4.6.**

Figure 4.6—Enterprise Goals Design Factor		
Reference	**Balanced Scorecard (BSC) Dimension**	**Enterprise Goal**
EG01	Financial	Portfolio of competitive products and services
EG02	Financial	Managed business risk
EG03	Financial	Compliance with external laws and regulations
EG04	Financial	Quality of financial information
EG05	Customer	Customer-oriented service culture
EG06	Customer	Business-service continuity and availability
EG07	Customer	Quality of management information
EG08	Internal	Optimization of internal business process functionality
EG09	Internal	Optimization of business process costs
EG10	Internal	Staff skills, motivation and productivity
EG11	Internal	Compliance with internal policies
EG12	Growth	Managed digital transformation programs
EG13	Growth	Product and business innovation

Section 4.6 includes more information on the COBIT goals cascade, which is the detailed elaboration of this design factor.

3. **Risk profile** of the enterprise and current issues in relation to I&T—The risk profile identifies the sort of I&T-related risk to which the enterprise is currently exposed and indicates which areas of risk are exceeding the risk appetite. The risk categories[14] listed in **figure 4.7** merit consideration.

Figure 4.7—Risk Profile Design Factor (IT Risk Categories)	
Reference	**Risk Category**
1	IT investment decision making, portfolio definition and maintenance
2	Program and projects lifecycle management
3	IT cost and oversight
4	IT expertise, skills and behavior
5	Enterprise/IT architecture
6	IT operational infrastructure incidents
7	Unauthorized actions
8	Software adoption/usage problems
9	Hardware incidents
10	Software failures
11	Logical attacks (hacking, malware, etc.)
12	Third party/supplier incidents
13	Noncompliance
14	Geopolitical issues
15	Industrial action
16	Acts of nature
17	Technology-based innovation
18	Environmental
19	Data and information management

[14] Modified from ISACA, *The Risk IT Practitioner Guide*, USA, 2009

4. **I&T-related issues**—A related method for an I&T risk assessment for the enterprise is to consider which I&T-related issues it currently faces, or, in other words, what I&T-related risk has materialized. The most common of such issues[15] include those in **figure 4.8**.

Figure 4.8—I&T-Related Issues Design Factor	
Reference	**Description**
A	Frustration between different IT entities across the organization because of a perception of low contribution to business value
B	Frustration between business departments (i.e., the IT customer) and the IT department because of failed initiatives or a perception of low contribution to business value
C	Significant IT-related incidents, such as data loss, security breaches, project failure and application errors, linked to IT
D	Service delivery problems by the IT outsourcer(s)
E	Failures to meet IT-related regulatory or contractual requirements
F	Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems
G	Substantial hidden and rogue IT spending, that is, IT spending by user departments outside the control of the normal IT investment decision mechanisms and approved budgets
H	Duplications or overlaps between various initiatives, or other forms of wasted resources
I	Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction
J	IT-enabled changes or projects frequently failing to meet business needs and delivered late or over budget
K	Reluctance by board members, executives or senior management to engage with IT, or a lack of committed business sponsorship for IT
L	Complex IT operating model and/or unclear decision mechanisms for IT-related decisions
M	Excessively high cost of IT
N	Obstructed or failed implementation of new initiatives or innovations caused by the current IT architecture and systems
O	Gap between business and technical knowledge, which leads to business users and information and/or technology specialists speaking different languages
P	Regular issues with data quality and integration of data across various sources
Q	High level of end-user computing, creating (among other problems) a lack of oversight and quality control over the applications that are being developed and put in operation
R	Business departments implementing their own information solutions with little or no involvement of the enterprise IT department[16]
S	Ignorance of and/or noncompliance with privacy regulations
T	Inability to exploit new technologies or innovate using I&T

5. **Threat landscape**—The threat landscape under which the enterprise operates can be classified as shown in **figure 4.9**.

Figure 4.9—Threat Landscape Design Factor	
Threat Landscape	**Explanation**
Normal	The enterprise is operating under what are considered normal threat levels.
High	Due to its geopolitical situation, industry sector or particular profile, the enterprise is operating in a high-threat environment.

[15] See also Section 3.3.1 Typical Pain Points, in ISACA, *COBIT® 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution*, USA, 2018.
[16] This issue is related to end-user computing, which often stems from dissatisfaction with IT solutions and services.

6. **Compliance requirements**—The compliance requirements to which the enterprise is subject can be classified according to the categories listed in **figure 4.10**.

Figure 4.10—Compliance Requirements Design Factor	
Regulatory Environment	**Explanation**
Low compliance requirements	The enterprise is subject to a minimal set of regular compliance requirements that are lower than average.
Normal compliance requirements	The enterprise is subject to a set of regular compliance requirements that are common across different industries.
High compliance requirements	The enterprise is subject to higher-than-average compliance requirements, most often related to industry sector or geopolitical conditions.

7. **Role of IT**—The role of IT for the enterprise can be classified as indicated in **figure 4.11**.

Figure 4.11—Role of IT Design Factor	
Role of IT[17]	**Explanation**
Support	IT is not crucial for the running and continuity of the business process and services, nor for their innovation.
Factory	When IT fails, there is an immediate impact on the running and continuity of the business processes and services. However, IT is not seen as a driver for innovating business processes and services.
Turnaround	IT is seen as a driver for innovating business processes and services. At this moment, however, there is not a critical dependency on IT for the current running and continuity of the business processes and services.
Strategic	IT is critical for both running and innovating the organization's business processes and services.

8. **Sourcing model for IT**—The sourcing model the enterprise adopts can be classified as shown in **figure 4.12**.

Figure 4.12—Sourcing Model for IT Design Factor	
Sourcing Model	**Explanation**
Outsourcing	The enterprise calls upon the services of a third party to provide IT services.
Cloud	The enterprise maximizes the use of the cloud for providing IT services to its users.
Insourced	The enterprise provides for its own IT staff and services.
Hybrid	A mixed model is applied, combining the other three models in varying degrees.

[17] The roles included in this table are taken from McFarlan, F. Warren; James L. McKenney; Philip Pyburn; "The Information Archipelago—Plotting a Course," *Harvard Business Review,* January 1993, *https://hbr.org/1983/01/the-information-archipelago-plotting-a-course*.

9. **IT implementation methods**—The methods the enterprise adopts can be classified as noted in **figure 4.13**.

Figure 4.13—IT Implementation Methods Design Factor	
IT Implementation Method	**Explanation**
Agile	The enterprise uses Agile development working methods for its software development.
DevOps	The enterprise uses DevOps working methods for software building, deployment and operations.
Traditional	The enterprise uses a more classic approach to software development (waterfall) and separates software development from operations.
Hybrid	The enterprise uses a mix of traditional and modern IT implementation, often referred to as "bimodal IT."

10. **Technology adoption strategy**—The technology adoption strategy can be classified as listed in **figure 4.14**.

Figure 4.14—Technology Adoption Strategy Design Factor	
Technology Adoption Strategy	**Explanation**
First mover	The enterprise generally adopts new technologies as early as possible and tries to gain first-mover advantage.
Follower	The enterprise typically waits for new technologies to become mainstream and proven before adopting them.
Slow adopter	The enterprise is very late with adoption of new technologies.

11. **Enterprise size**—Two categories, as shown in **figure 4.15**, are identified for the design of an enterprise's governance system.[18]

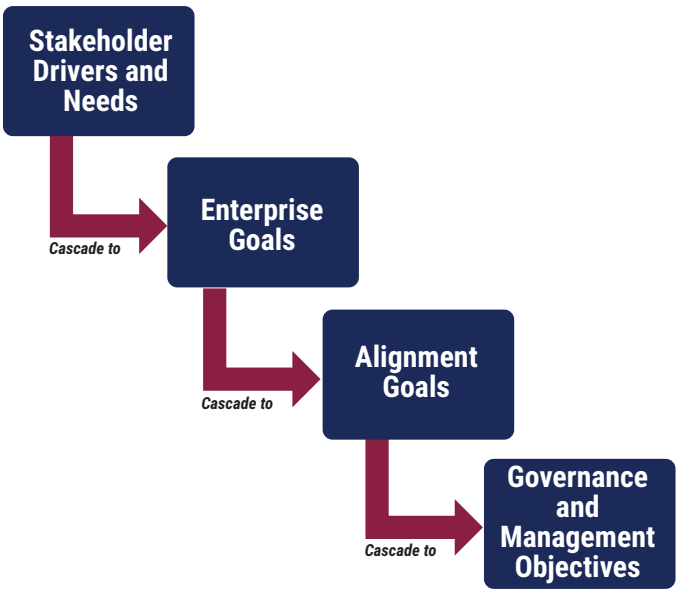
Figure 4.15—Enterprise Size Design Factor	
Enterprise Size	**Explanation**
Large enterprise (Default)	Enterprise with more than 250 full-time employees (FTEs)
Small and medium enterprise	Enterprise with 50 to 250 FTEs

[18] Micro-enterprises, i.e., enterprises with fewer than 50 staff members, are not considered in this publication.

4.6 Goals Cascade

Stakeholder needs have to be transformed into an enterprise's actionable strategy. The goals cascade (**figure 4.16**) supports enterprise goals, which is one of the key design factors for a governance system. It supports prioritization of management objectives based on prioritization of enterprise goals.

Figure 4.16—COBIT Goals Cascade



The goals cascade further supports translation of enterprise goals into priorities for alignment goals. The goals cascade has been updated thoroughly in COBIT® 2019:

- Enterprise goals have been consolidated, reduced, updated and clarified.
- Alignment goals emphasize the alignment of all IT efforts with business objectives.[19] This updated term also seeks to avoid the frequent misunderstanding that these goals indicate purely internal objectives of the IT department within an enterprise. Like enterprise goals, alignment goals have been consolidated, reduced, updated and clarified where necessary.

[19] Alignment goals were called IT-related goals in COBIT 5.

4.6.1 Enterprise Goals

Stakeholder needs cascade to enterprise goals. **Figure 4.17** shows the set of 13 enterprise goals along with a number of accompanying example metrics.

Figure 4.17—Goals Cascade: Enterprise Goals and Metrics

Reference	BSC Dimension	Enterprise Goal	Example Metrics
EG01	Financial	Portfolio of competitive products and services	• Percent of products and services that meet or exceed targets in revenues and/or market share • Percent of products and services that meet or exceed customer satisfaction targets • Percent of products and services that provide competitive advantage • Time-to-market for new products and services
EG02	Financial	Managed business risk	• Percent of critical business objectives and services covered by risk assessment • Ratio of significant incidents that were not identified in risk assessments vs. total incidents • Appropriate frequency of update of risk profile
EG03	Financial	Compliance with external laws and regulations	• Cost of regulatory noncompliance, including settlements and fines • Number of regulatory noncompliance issues causing public comment or negative publicity • Number of noncompliance matters noted by regulators or supervisory authorities • Number of regulatory noncompliance issues relating to contractual agreements with business partners
EG04	Financial	Quality of financial information	• Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of enterprise financial information • Cost of regulatory noncompliance with finance-related regulations
EG05	Customer	Customer-oriented service culture	• Number of customer service disruptions • Percent of business stakeholders satisfied that customer service delivery meets agreed levels • Number of customer complaints • Trend of customer satisfaction survey results
EG06	Customer	Business service continuity and availability	• Number of customer service or business process interruptions causing significant incidents • Business cost of incidents • Number of business processing hours lost due to unplanned service interruptions • Percent of complaints as a function of committed service-availability targets
EG07	Customer	Quality of management information	• Degree of board and executive management satisfaction with decision-making information • Number of incidents caused by incorrect business decisions based on inaccurate information • Time to provide supporting information to enable effective business decisions • Timeliness of management information

Figure 4.17—Goals Cascade: Enterprise Goals and Metrics *(cont.)*			
Reference	**BSC Dimension**	**Enterprise Goal**	**Example Metrics**
EG08	Internal	Optimization of internal business process functionality	• Satisfaction levels of board and executive management with business process capabilities • Satisfaction levels of customers with service delivery capabilities • Satisfaction levels of suppliers with supply chain capabilities
EG09	Internal	Optimization of business process costs	• Ratio of cost vs. achieved service levels • Satisfaction levels of board and executive management with business processing costs
EG10	Internal	Staff skills, motivation and productivity	• Staff productivity compared to benchmarks • Level of stakeholder satisfaction with staff expertise and skills • Percent of staff whose skills are insufficient relative to competencies required for their roles • Percent of satisfied staff
EG11	Internal	Compliance with internal policies	• Number of incidents related to noncompliance with policy • Percent of stakeholders who understand policies • Percent of policies supported by effective standards and working practices
EG12	Growth	Managed digital transformation programs	• Number of programs on time and within budget • Percent of stakeholders satisfied with program delivery • Percent of business transformation programs stopped • Percent of business transformation programs with regular reported status updates
EG13	Growth	Product and business innovation	• Level of awareness and understanding of business innovation opportunities • Stakeholder satisfaction with levels of product and innovation expertise and ideas • Number of approved product and service initiatives resulting from innovative ideas

4.6.2 Alignment Goals

Enterprise goals cascade to alignment goals. **Figure 4.18** contains the set of alignment goals and example metrics.

Figure 4.18—Goals Cascade: Alignment Goals and Metrics			
Reference	**IT BSC Dimension**	**Alignment Goal**	**Metrics**
AG01	Financial	I&T compliance and support for business compliance with external laws and regulations	• Cost of IT noncompliance, including settlements and fines, and the impact of reputational loss • Number of IT-related noncompliance issues reported to the board or causing public comment or embarrassment • Number of noncompliance issues relating to contractual agreements with IT service providers
AG02	Financial	Managed I&T-related risk	• Appropriate frequency of update of risk profile • Percent of enterprise risk assessments including I&T-related risk • Number of significant I&T-related incidents that were not identified in a risk assessment

Figure 4.18—Goals Cascade: Alignment Goals and Metrics *(cont.)*			
Reference	**IT BSC Dimension**	**Alignment Goal**	**Metrics**
AG03	Financial	Realized benefits from I&T-enabled investments and services portfolio	• Percent of I&T-enabled investments for which claimed benefits in the business case are met or exceeded • Percent of I&T services for which expected benefits (as stated in the service level agreements) are realized
AG04	Financial	Quality of technology-related financial information	• Satisfaction of key stakeholders regarding the level of transparency, understanding and accuracy of IT financial information • Percent of I&T services with defined and approved operational costs and expected benefits
AG05	Customer	Delivery of I&T services in line with business requirements	• Percent of business stakeholders satisfied that IT service delivery meets agreed service levels • Number of business disruptions due to IT service incidents • Percent of users satisfied with the quality of IT service delivery
AG06	Customer	Agility to turn business requirements into operational solutions	• Level of satisfaction of business executives with IT's responsiveness to new requirements • Average time-to-market for new I&T-related services and applications • Average time to turn strategic I&T objectives into an agreed and approved initiative • Number of critical business processes supported by up-to-date infrastructure and applications
AG07	Internal	Security of information, processing infrastructure and applications, and privacy	• Number of confidentiality incidents causing financial loss, business disruption or public embarrassment • Number of availability incidents causing financial loss, business disruption or public embarrassment • Number of integrity incidents causing financial loss, business disruption or public embarrassment
AG08	Internal	Enabling and supporting business processes by integrating applications and technology	• Time to execute business services or processes • Number of I&T-enabled business programs delayed or incurring additional cost due to technology integration issues • Number of business process changes that need to be delayed or reworked because of technology integration issues • Number of applications or critical infrastructures operating in silos and not integrated
AG09	Internal	Delivery of programs on time, on budget and meeting requirements and quality standards	• Number of programs/projects on time and within budget • Number of programs needing significant rework due to quality defects • Percent of stakeholders satisfied with program/project quality
AG10	Internal	Quality of I&T management information	• Level of user satisfaction with quality and timeliness and availability of I&T-related management information, taking into account available resources • Ratio and extent of erroneous business decisions in which erroneous or unavailable I&T-related information was a key factor • Percentage of information meeting quality criteria

Figure 4.18—Goals Cascade: Alignment Goals and Metrics *(cont.)*			
Reference	**IT BSC Dimension**	**Alignment Goal**	**Metrics**
AG11	Internal	I&T compliance with internal policies	• Number of incidents related to noncompliance with IT-related policies • Number of exceptions to internal policies • Frequency of policy review and update
AG12	Learning and Growth	Competent and motivated staff with mutual understanding of technology and business	• Percent of I&T-savvy business people (i.e., those having the required knowledge and understanding of I&T to guide, direct, innovate and see opportunities of I&T for their domain of expertise) • Percent of business-savvy IT people (i.e., those having the required knowledge and understanding of relevant business domains to guide, direct, innovate and see opportunities of I&T for the business domain) • Number or percentage of business people with technology management experience
AG13	Learning and Growth	Knowledge, expertise and initiatives for business innovation	• Level of business executive awareness and understanding of I&T innovation possibilities • Number of approved initiatives resulting from innovative I&T ideas • Number of innovation champions recognized/awarded

Chapter 5
COBIT Governance and Management Objectives

5.1 Purpose

In section 4.2, **figure 4.2**, the COBIT core model was presented, including the 40 governance and management objectives. **Figure 5.1** lists all the governance and management objectives, each with its purpose statement. The purpose statement is a further elaboration—a next level of detail—of each governance and management objective.

Figure 5.1—COBIT Core Model: Governance and Management Objectives and Purpose

Reference	Name	Purpose
EDM01	Ensured governance framework setting and maintenance	Provide a consistent approach, integrated and aligned with the enterprise governance approach. I&T-related decisions must be 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.
EDM02	Ensured benefits delivery	Secure optimal value from I&T-enabled initiatives, services and assets; cost-effective 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.
EDM03	Ensured risk optimization	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.
EDM04	Ensured resource optimization	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.
EDM05	Ensured stakeholder engagement	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.
APO01	Managed I&T management framework	Implement a consistent management approach for enterprise governance requirements to be met, covering governance components such as management processes; organizational structures; roles and responsibilities; reliable and repeatable activities; information items; policies and procedures; skills and competencies; culture and behavior; and services, infrastructure and applications.
APO02	Managed strategy	Support the digital transformation strategy of the organization and deliver the desired value through a road map of incremental changes. Use a holistic I&T approach, ensuring that each initiative is clearly connected to an overarching strategy. Enable change in all different aspects of the organization, from channels and processes to data, culture, skills, operating model and incentives.
APO03	Managed enterprise architecture	Represent the different building blocks that make up the enterprise and its interrelationships, as well as the principles guiding their design and evolution over time, to enable a standard, responsive and efficient delivery of operational and strategic objectives.
APO04	Managed innovation	Achieve competitive advantage, business innovation, improved customer experience, and improved operational effectiveness and efficiency by exploiting I&T developments and emerging technologies.

Figure 5.1—COBIT Core Model: Governance and Management Objectives and Purpose *(cont.)*		
Reference	**Name**	**Purpose**
APO05	Managed portfolio	Optimize the performance of the overall portfolio of programs in response to individual program, product and service performance and changing enterprise priorities and demand.
APO06	Managed budget and costs	Foster a partnership between IT and enterprise stakeholders to enable the effective and efficient use of I&T-related resources and provide transparency and accountability of the cost and business value of solutions and services. Enable the enterprise to make informed decisions regarding the use of I&T solutions and services.
APO07	Managed human resources	Optimize human-resources capabilities to meet enterprise objectives.
APO08	Managed relationships	Enable the right knowledge, skills and behaviors to create improved outcomes, increased confidence, mutual trust and effective use of resources that stimulate a productive relationship with business stakeholders.
APO09	Managed service agreements	Ensure that I&T products, services and service levels meet current and future enterprise needs.
APO10	Managed vendors	Optimize available I&T capabilities to support the I&T strategy and road map, minimize the risk associated with nonperforming or noncompliant vendors, and ensure competitive pricing.
APO11	Managed quality	Ensure consistent delivery of technology solutions and services to meet the quality requirements of the enterprise and satisfy stakeholder needs.
APO12	Managed risk	Integrate the management of I&T-related enterprise risk with overall enterprise risk management (ERM) and balance the costs and benefits of managing I&T-related enterprise risk.
APO13	Managed security	Keep the impact and occurrence of information security incidents within the enterprise's risk appetite levels.
APO14	Managed data	Ensure effective utilization of the critical data assets to achieve enterprise goals and objectives.
BAI01	Managed programs	Realize desired business value and reduce the risk of unexpected delays, costs and value erosion. To do so, improve communications to and involvement of business and end users, ensure the value and quality of program deliverables and follow-up of projects within the programs, and maximize program contribution to the investment portfolio.
BAI02	Managed requirements definition	Create optimal solutions that meet enterprise needs while minimizing risk.
BAI03	Managed solutions identification and build	Ensure agile and scalable delivery of digital products and services. Establish timely and cost-effective solutions (technology, business processes and workflows) capable of supporting enterprise strategic and operational objectives.
BAI04	Managed availability and capacity	Maintain service availability, efficient management of resources and optimization of system performance through prediction of future performance and capacity requirements.
BAI05	Managed organizational change	Prepare and commit stakeholders for business change and reduce the risk of failure.
BAI06	Managed IT changes	Enable fast and reliable delivery of change to the business. Mitigate the risk of negatively impacting the stability or integrity of the changed environment.
BAI07	Managed IT change acceptance and transitioning	Implement solutions safely and in line with the agreed expectations and outcomes.

Figure 5.1—COBIT Core Model: Governance and Management Objectives and Purpose *(cont.)*		
Reference	**Name**	**Purpose**
BAI08	Managed knowledge	Provide the knowledge and management information required to support all staff in the governance and management of enterprise I&T and allow for informed decision making.
BAI09	Managed assets	Account for all I&T assets and optimize the value provided by their use.
BAI10	Managed configuration	Provide sufficient information about service assets to enable the service to be effectively managed. Assess the impact of changes and deal with service incidents.
BAI11	Managed projects	Realize defined project outcomes and reduce the risk of unexpected delays, costs and value erosion by improving communications to and involvement of business and end users. Ensure the value and quality of project deliverables and maximize their contribution to the defined programs and investment portfolio.
DSS01	Managed operations	Deliver I&T operational product and service outcomes as planned.
DSS02	Managed service requests and incidents	Achieve increased productivity and minimize disruptions through quick resolution of user queries and incidents. Assess the impact of changes and deal with service incidents. Resolve user requests and restore service in response to incidents.
DSS03	Managed problems	Increase availability, improve service levels, reduce costs, improve customer convenience and satisfaction by reducing the number of operational problems, and identify root causes as part of problem resolution.
DSS04	Managed continuity	Adapt rapidly, continue business operations, and maintain availability of resources and information at a level acceptable to the enterprise in the event of a significant disruption (e.g., threats, opportunities, demands).
DSS05	Managed security services	Minimize the business impact of operational information security vulnerabilities and incidents.
DSS06	Managed business process controls	Maintain information integrity and the security of information assets handled within business processes in the enterprise or its outsourced operation.
MEA01	Managed performance and conformance monitoring	Provide transparency of performance and conformance and drive achievement of goals.
MEA02	Managed system of internal control	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.
MEA03	Managed compliance with external requirements	Ensure that the enterprise is compliant with all applicable external requirements.
MEA04	Managed assurance	Enable the organization to design and develop efficient and effective assurance initiatives, providing guidance on planning, scoping, executing and following up on assurance reviews, using a road map based on well-accepted assurance approaches.

Page intentionally left blank

Chapter 6
Performance Management in COBIT

6.1 Definition

Performance management is an essential part of a governance and management system. "Performance management" represents a general term for all activities and methods. It expresses how well the governance and management system and all the components of an enterprise work, and how they can be improved to achieve the required level. It includes concepts and methods such as capability levels and maturity levels. COBIT uses the term COBIT performance management (CPM) to describe these activities, and the concept is an integral part of the COBIT framework.

6.2 COBIT Performance Management Principles

COBIT® 2019 is based on the following principles:

1. The CPM should be simple to understand and use.
2. The CPM should be consistent with, and support, the COBIT conceptual model. It should enable management of the performance of all types of components of the governance system; it must be possible to manage the performance of processes as well as the performance of other types of components (e.g., organizational structures or information), if users wish to do so.
3. The CPM should provide reliable, repeatable and relevant results.
4. The CPM must be flexible, so it can support the requirements of different organizations with different priorities and needs.
5. The CPM should support different types of assessment, from self-assessments to formal appraisals or audits.

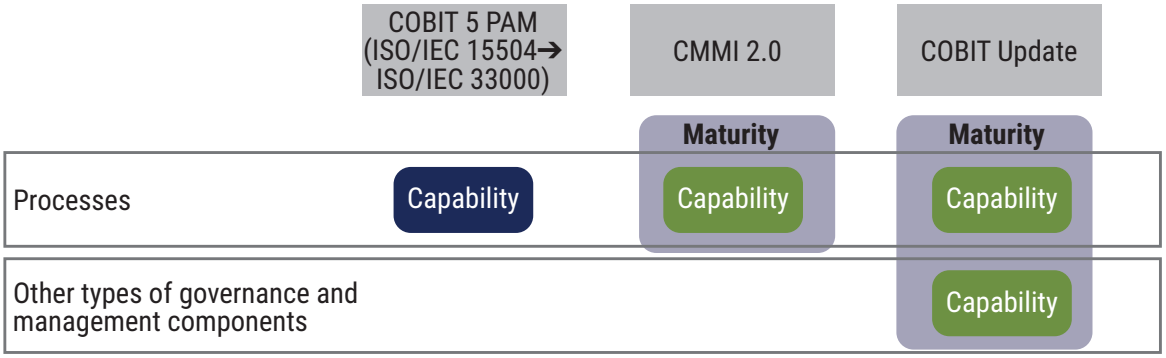
6.3 COBIT Performance Management Overview

The CPM model (**figure 6.1**) largely aligns to and extends CMMI® Development V2.0[20] concepts:

- Process activities are associated to capability levels. This is included in the *COBIT® 2019 Framework: Governance and Management Objectives* guide.
- Other governance and management component types (e.g., organizational structures, information) may also have capability levels defined for them in future guidance.
- Maturity levels are associated with focus areas (i.e., a collection of governance and management objectives and underlying components) and will be achieved if all required capability levels are achieved.

[20] CMMI® Development V2.0, CMMI Institute, USA, 2018, *https://cmmiinstitute.com/model-viewer/dashboard*

Figure 6.1—Capability Levels



If enterprises desire to continue using the COBIT 5 process capability model based on International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 15504 (now ISO/IEC 33000, in which capability levels have very different meanings), they have all required information to do so in *COBIT® 2019 Framework: Governance and Management Objectives*. No separate process assessment model (PAM) publications are necessary, nor will they be provided with COBIT® 2019.

In COBIT® 2019, the explicit process outcomes or process goals are replaced by the process practices themselves. This results in the following situation for an ISO/IEC33000 evaluation:

1. Process outcomes are now linked to the process practices on a one-to-one basis (i.e., the process outcomes are the successful completion of the process practices). Note: the process practices are formulated as practices, and the outcomes can be derived from there. Example: APO01.01 *Design the management system for enterprise I&T* has as process outcome APO01.01: *A management system for enterprise I&T is designed*.
2. Base practices are equal to the COBIT® 2019 process practices for each governance and management objective.
3. Work products are equal to the Information Flows and Items under component C in each governance/management objective.

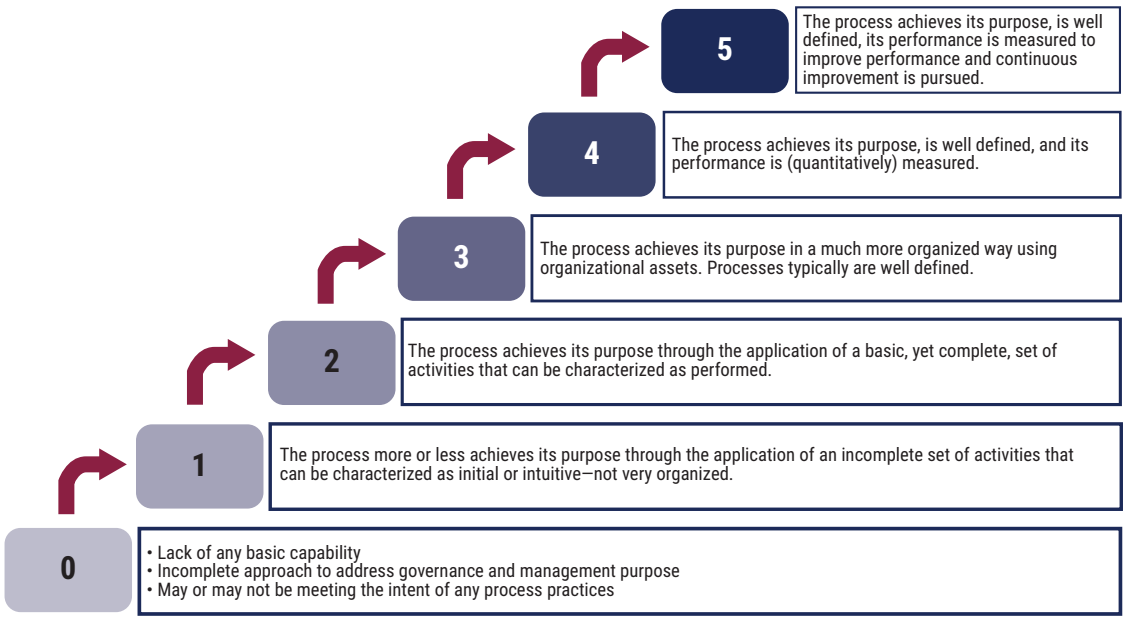
Thus, the mapping of outcomes to base practices and work products is all done by definition in COBIT® 2019.

6.4 Managing Performance of Processes

6.4.1 Process Capability Levels

COBIT® 2019 supports a CMMI-based process capability scheme. The process within each governance and management objective can operate at various capability levels, ranging from 0 to 5. The capability level is a measure of how well a process is implemented and performing. **Figure 6.2** depicts the model, the increasing capability levels and the general characteristics of each.

Figure 6.2—Capability Levels for Processes



The COBIT core model assigns capability levels to all process activities, enabling clear definition of the processes and required activities for achieving the different capability levels. See *COBIT® 2019 Framework: Governance and Management Objectives* for more detail.

6.4.2 Rating Process Activities

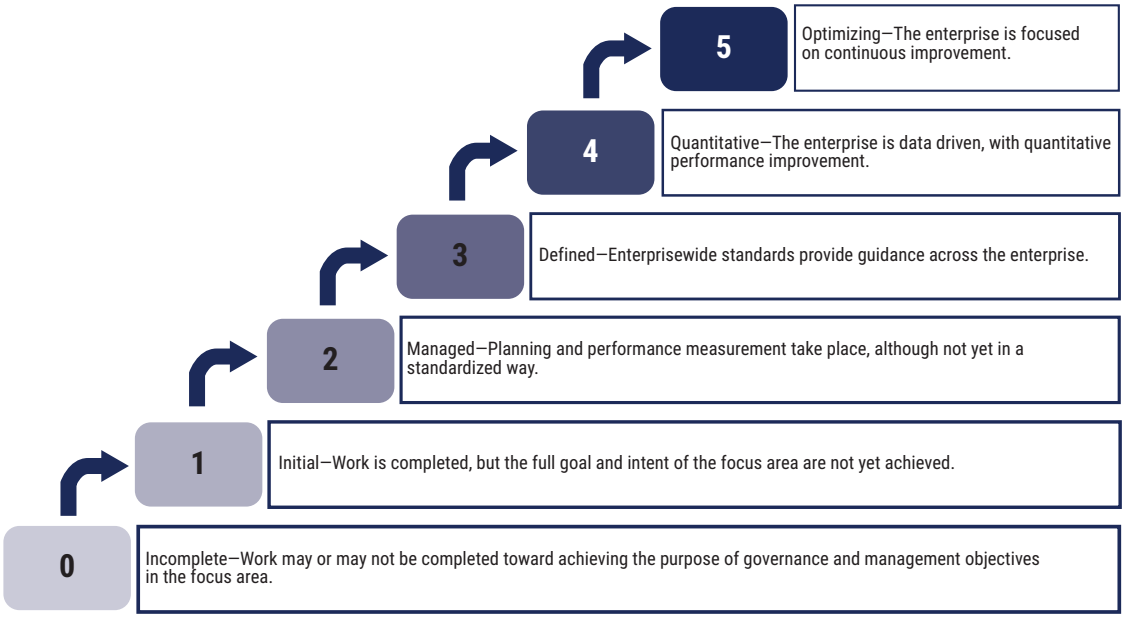
A capability level can be achieved to varying degrees, which can be expressed by a set of ratings. The range of available ratings depends on the context in which the performance assessment is made:

- Some formal methods leading to independent certification use a binary pass/fail set of ratings.
- Less formal methods (often used in performance-improvement contexts) work better with a larger range of ratings, such as the following set:
  - *Fully*—The capability level is achieved for more than 85 percent. (This remains a judgment call, but it can be substantiated by the examination or assessment of the components of the enabler, such as process activities, process goals or organizational structure good practices.)
  - *Largely*—The capability level is achieved between 50 percent and 85 percent.
  - *Partially*—The capability level is achieved between 15 percent and 50 percent.
  - *Not*—The capability level is achieved less than 15 percent.

6.4.3 Focus Area Maturity Levels

Sometimes a higher level is required for expressing performance without the granularity applicable to individual process capability ratings. Maturity levels can be used for that purpose. COBIT® 2019 defines maturity levels as a performance measure at the focus area level, as shown in **figure 6.3**.

Figure 6.3—Maturity Levels for Focus Areas



Maturity levels are associated with focus areas (i.e., a collection of governance and management objectives and underlying components) and a certain maturity level is achieved if all the processes contained in the focus area achieve that particular capability level.

6.5 Managing Performance of Other Governance System Components

6.5.1 Performance Management of Organizational Structures

Although no generally accepted or formal method exists for assessing organizational structures, they can be less formally assessed according to the following criteria. For each criterion, a number of subcriteria can be defined, linked to the various capability levels. The criteria are:

- Successful execution of those process practices for which the organizational structure (or role) has accountability or responsibility (an A or an R, respectively, in a responsible-accountable-consulted-informed [RACI] chart)
- Successful application of a number of good practices for organizational structures, such as:
  - Operating principles
    - The organizational structure is formally established.
    - The organizational structure has a clear, documented and well-understood mandate.
    - Operating principles are documented.
    - Regular meetings take place as defined in the operating principles.
    - Meeting reports/minutes are available and meaningful.
  - Composition
    - The organizational structure is formally established.

  - Span of control
    - The organizational structure has a clear, documented and well-understood mandate.
    - Operating principles are documented.
    - Regular meetings take place as defined in the operating principles.
    - Meeting reports/minutes are available and are meaningful.
  - Level of authority and decision rights
    - Decision rights of the organizational structure are defined and documented.
    - Decision rights of the organizational structure are respected and complied with (also a culture/behavior issue).
  - Delegation of authority
    - Delegation of authority is implemented in a meaningful way.
  - Escalation procedures
    - Escalation procedures are defined and applied.
- Successful application of a number of organizational structure management practices (nonfunctional practices arising from an organizational structure point of view):
  - Objectives for the performance of the organizational structures are identified.
  - Performance of the organizational structure is planned and monitored.
  - Performance of the organizational structure is adjusted to meet plans.
  - Resources and information necessary for the organizational structure are identified, made available, allocated and used.
  - Interfaces between the organizational structure and other stakeholders are managed to ensure both effective communication and clear assignment of responsibility.
  - Regular evaluations result in the required continuous improvement of the organizational structure—in its composition, mandate or any other parameter.

As for the processes, low capability levels require a subset of these criteria to be satisfied, and higher capability levels require all criteria to be satisfied. But, as already indicated, no generally accepted scheme exists for assessing organizational structures. However, this does not prevent an enterprise from defining its own capability scheme for organizational structures.

6.5.2 Performance Management of Information Items

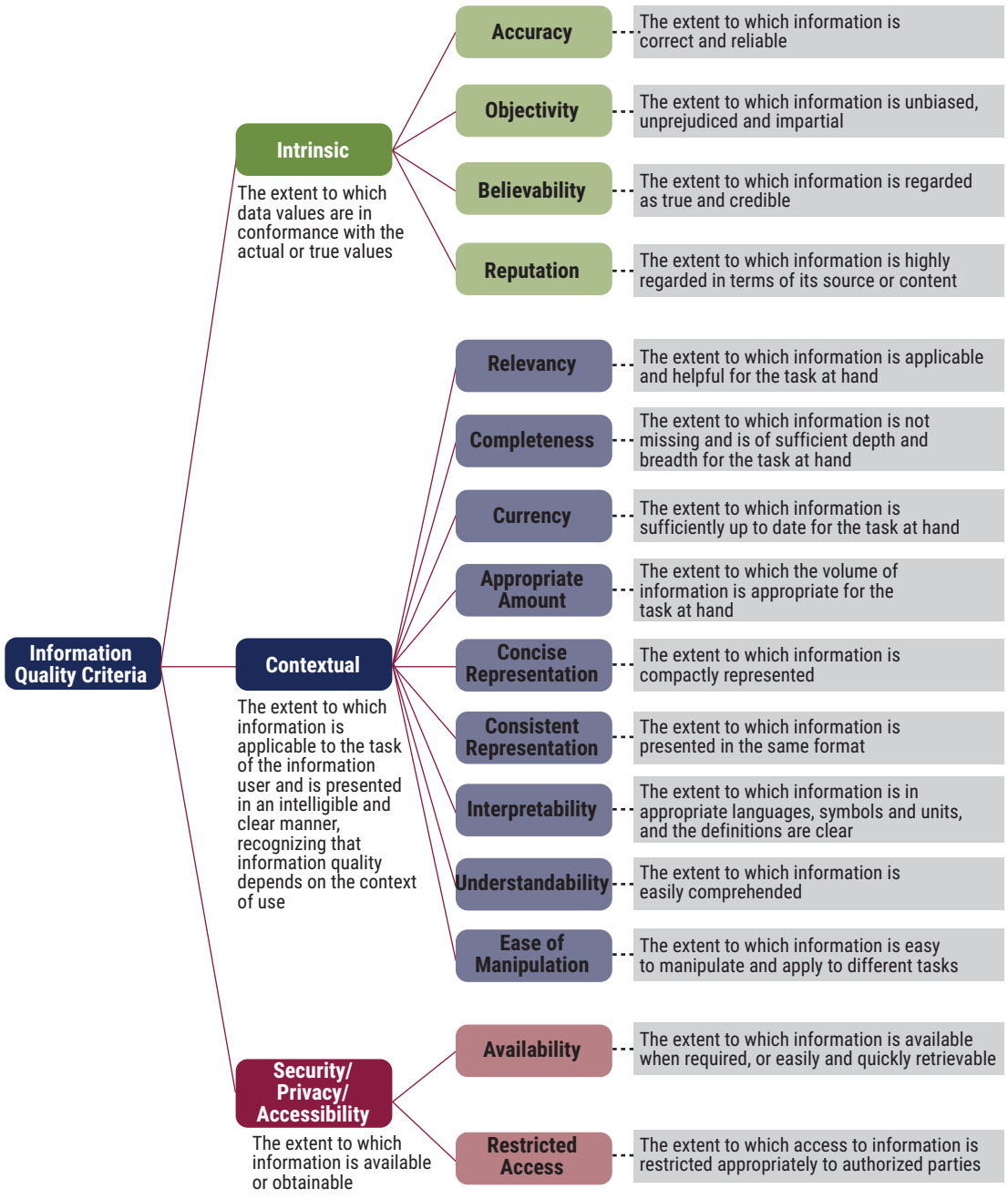
The information item component for a governance system of I&T is more or less equivalent to the process work products as described in *COBIT® 2019 Framework: Governance and Management Objectives*.

Although no generally accepted or formal method exists for assessing information items, they can be less formally assessed according to the information reference model first presented in *COBIT® 5: Enabling Information*.[21]

This model defines three main quality criteria for information and 15 subcriteria, as illustrated in **figure 6.4**.

[21] See ISACA, *COBIT® 5: Enabling Information*, section 3.1.2 Goals, USA, 2013 , *http://www.isaca.org/COBIT/Pages/COBIT-5-Enabling-Information-product-page.aspx*

Figure 6.4—Information Reference Model: Quality Criteria for Information



An information item can be assessed by considering the extent to which the relevant quality criteria, as defined in **figure 6.4**, are achieved.

6.5.3 Performance Management of Culture and Behavior

For the culture and behavior governance component, it should be possible to define a set of desirable (and/or undesirable) behaviors for good governance and management of IT, and to assign different levels of capability to each.

COBIT® 2019 Framework: Governance and Management Objectives defines aspects of the culture and behavior component for most objectives. From there, it is possible to assess the extent to which these conditions or behaviors are met.

Focus area content, which will contain a more detailed set of desired behaviors, will be developed going forward. The user is advised to consult *isaca.org/cobit* for the latest status and available focus area guidance.

Page intentionally left blank

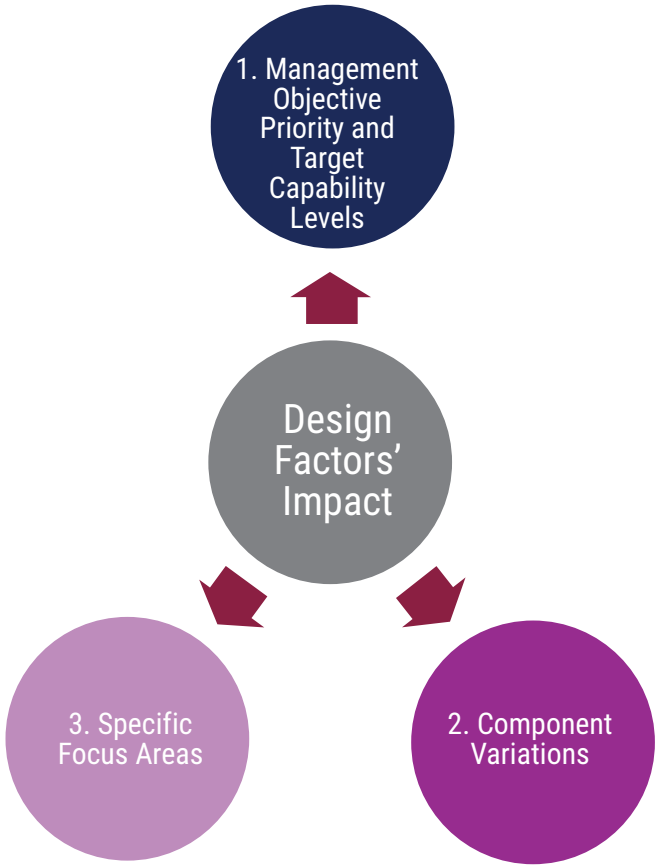
Chapter 7
Designing a Tailored Governance System

7.1 Impact of Design Factors

This section provides a high-level overview of the potential impact of design factors on a governance system for enterprise I&T. It also describes, at a high level, a workflow for designing a tailored governance system for the enterprise. More information on these subjects can be found in the *COBIT® 2019 Design Guide*.

Design factors influence in different ways the tailoring of the governance system of an enterprise. This publication distinguishes three different types of impact, illustrated in **figure 7.1**.

Figure 7.1—Impact of Design Factors on a Governance and Management System



1. **Management objective priority/selection**—The COBIT core model contains 40 governance and management objectives, each consisting of the process and a number of related components. They are intrinsically equivalent; there is no natural order of priority among them. However, design factors can influence this equivalence and make some governance and management objectives more important than others, sometimes to the extent that some governance and management objectives may become negligible. In practice, this higher importance translates into setting higher target capability levels for important governance and management objectives.

Example: When an enterprise identifies the most relevant enterprise goal(s) from the enterprise goal list and applies the goals cascade, this will lead to a selection of priority management objectives. For example, when EG01 *Portfolio of competitive products and services* is ranked as very high by an enterprise, this will make management objective APO05 *Managed portfolio* an important part of this enterprise's governance system.

Example: An enterprise that is very risk averse will give more priority to management objectives that aspire to govern and manage risk and security. Governance and management objectives EDM03 *Ensured risk optimization*, APO12 *Managed risk,* APO13 *Managed security* and DSS05 *Managed security services* will become important parts of that enterprise's governance system and will have higher target capability levels defined for them.

Example: An enterprise operating within a high threat landscape will require highly capable security-related processes: APO13 *Managed security* and DSS05 *Managed security services.*

Example: An enterprise in which the role of IT is strategic and crucial to the success of the business will require high involvement of IT-related roles in organizational structures, a thorough understanding of business by IT professionals (and vice versa), and a focus on strategic processes such as APO02 *Managed strategy* and APO08 *Managed relationships*.

2. **Components variation**—Components are required to achieve governance and management objectives. Some design factors can influence the importance of one or more components or can require specific variations.

Example: Small and medium-sized enterprises might not need the full set of roles and organizational structures as laid out in the COBIT core model, but may use a reduced set instead. This reduced set of governance and management objectives and the included components is defined in the Small and Medium Enterprise focus area.[22]

Example: An enterprise which operates in a highly regulated environment will attribute more importance to *documented work products and policies and procedures* and to some roles, e.g. the compliance officer function.

Example: An enterprise that uses DevOps in solution development and operations will require specific activities, organizational structures, culture, etc., focused on BAI03 *Managed solutions identification and build* and DSS01 *Managed operations*.

3. **Need for specific focus areas**—Some design factors, such as threat landscape, specific risk, target development methods and infrastructure set-up, will drive the need for variation of the core COBIT model content to a specific context.

Example: Enterprises adopting a DevOps approach will require a governance system that has a variant of several generic COBIT processes, described in the DevOps focus area guidance[23] for COBIT.

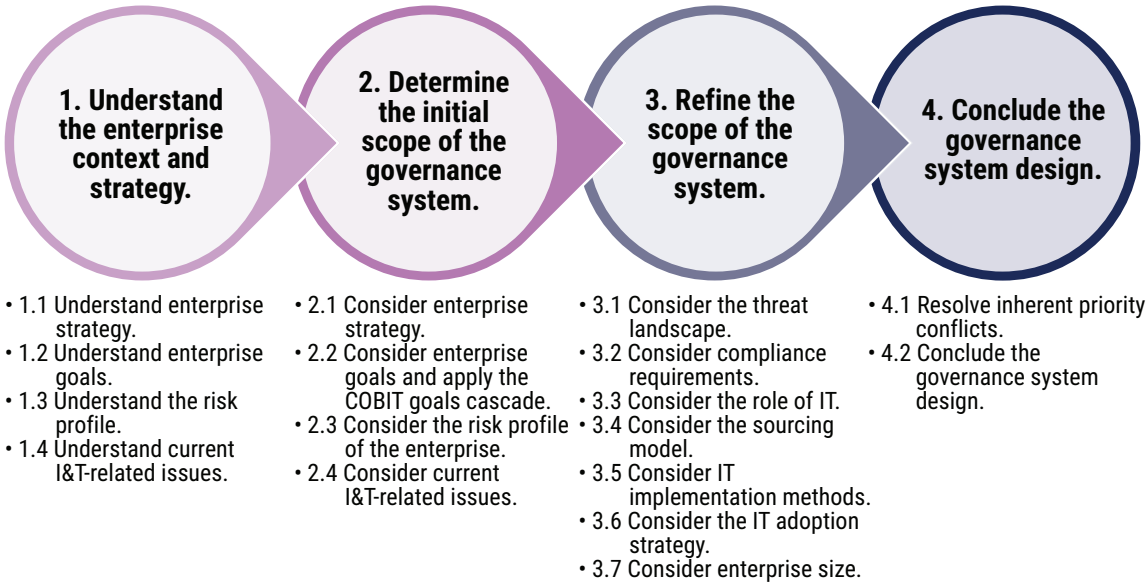
Example: Small and medium enterprises have less staff, fewer IT resources, and shorter and more direct reporting lines, and differ in many more aspects from large enterprises. For that reason, their governance system for I&T will have to be less onerous, compared to large enterprises. This is described in the SME focus area guidance of COBIT.[24]

[22] At the time of publication of *COBIT® 2019 Framework: Introduction and Methodology,* the small and medium enterprise focus area content was in development and not yet released.
[23] At the time of publication of *COBIT® 2019 Framework: Introduction and Methodology,* the DevOps focus area content was in development and not yet released.
[24] At the time of publication of *COBIT® 2019 Framework: Introduction and Methodology,* the small and medium enterprise focus area content was in development and not yet released.

7.2 Stages and Steps in the Design Process

Figure 7.2 illustrates the proposed flow for designing a tailored governance system.

Figure 7.2—Governance System Design Workflow



The different stages and steps in the design process, as illustrated in **figure 7.2**, will result in recommendations for prioritizing governance and management objectives or related governance system components, for target capability levels, or for adopting specific variants of a governance system component.

Some of these steps or substeps may result in conflicting guidance, which is inevitable when considering a larger number of design factors, the overall generic nature of the design factor guidance and the mapping tables used.

It is recommended to put all guidance obtained during the different steps on a design canvas and—in the last stage of the design process—resolve (to the degree possible) the conflicts among the elements on the design canvas and conclude. There is no magic formula. The final design will be a case-by-case decision, based on all the elements on the design canvas. By following these steps, enterprises will realize a governance system that is tailored to their needs.

Page intentionally left blank

Chapter 8
Implementing Enterprise Governance of IT

8.1 COBIT Implementation Guide Purpose

The *COBIT® 2019 Implementation Guide* emphasizes an enterprisewide view of governance of I&T. This guide recognizes that I&T are pervasive in enterprises and that it is neither possible nor good practice to separate business and IT-related activities. The governance and management of enterprise I&T should, therefore, be implemented as an integral part of enterprise governance, covering the full end-to-end business and IT functional areas of responsibility.

One of the common reasons why some governance system implementations fail is that they are not initiated and then managed properly as programs to ensure that benefits are realized. Governance programs need to be sponsored by executive management, be properly scoped and define objectives that are attainable. This enables the enterprise to absorb the pace of change as planned. Program management is, therefore, addressed as an integral part of the implementation life cycle.

It is also assumed that while a program and project approach is recommended to effectively drive improvement initiatives, the goal is also to establish a normal business practice and sustainable approach to governing and managing enterprise I&T just like any other aspect of enterprise governance. For this reason, the implementation approach is based on empowering business and IT stakeholders and role players to take ownership of IT-related governance and management decisions and activities by facilitating and enabling change. The implementation program is closed when the process for focusing on IT-related priorities and governance improvement is generating a measurable benefit, and the program has become embedded in ongoing business activity.

More information on these subjects can also be found in the *COBIT® 2019 Implementation Guide*.

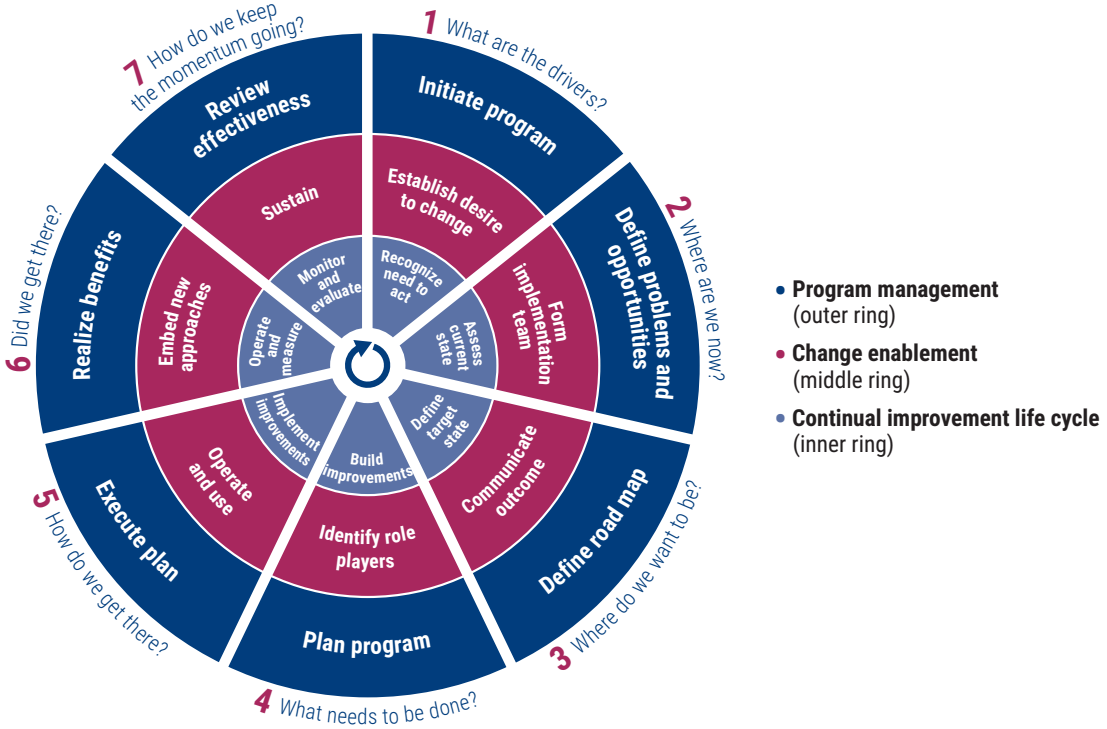
8.2 COBIT Implementation Approach

There are seven phases that comprise the COBIT implementation approach:

- What are the drivers?
- Where are we now?
- Where do we want to be?
- What needs to be done?
- How do we get there?
- Did we get there?
- How do we keep the momentum going?

The COBIT implementation approach is summarized in **figure 8.1**.

Figure 8.1—COBIT Implementation Road Map



8.2.1 Phase 1—What Are the Drivers?

Phase 1 of the implementation approach identifies current change drivers and creates at executive management levels a desire to change that is then expressed in an outline of a business case. A change driver is an internal or external event, condition or key issue that serves as a stimulus for change. Events, trends (industry, market or technical), performance shortfalls, software implementations and even the goals of the enterprise can all act as change drivers.

Risk associated with implementation of the program itself is described in the business case and managed throughout the life cycle. Preparing, maintaining and monitoring a business case are fundamental and important disciplines for justifying, supporting and then ensuring successful outcomes for any initiative, including improvement of the governance system. They ensure a continuous focus on the benefits of the program and their realization.

8.2.2 Phase 2—Where Are We Now?

Phase 2 aligns I&T-related objectives with enterprise strategies and risk, and prioritizes the most important enterprise goals, alignment goals and processes. The *COBIT® 2019 Design Guide* provides several design factors to help with the selection.

Based on the selected enterprise and IT-related goals and other design factors, the enterprise must identify critical governance and management objectives and underlying processes that are of sufficient capability to ensure successful outcomes. Management needs to know its current capability and where deficiencies may exist. This can be achieved by a process capability assessment of the current status of the selected processes.

8.2.3 Phase 3—Where Do We Want to Be?

Phase 3 sets a target for improvement followed by a gap analysis to identify potential solutions.

Some solutions will be quick wins and others more challenging, long-term tasks. Priority should be given to projects that are easier to achieve and likely to give the greatest benefit. Longer-term tasks should be broken down into manageable pieces.

8.2.4 Phase 4—What Needs to Be Done?

Phase 4 describes how to plan feasible and practical solutions by defining projects supported by justifiable business cases and a change plan for implementation. A well-developed business case can help ensure that the project's benefits are identified and continually monitored.

8.2.5 Phase 5—How Do We Get There?

Phase 5 provides for implementing the proposed solutions via day-to-day practices and establishing measures and monitoring systems to ensure that business alignment is achieved, and performance can be measured.

Success requires engagement, awareness and communication, understanding and commitment of top management, and ownership by the affected business and IT process owners.

8.2.6 Phase 6—Did We Get There?

Phase 6 focuses on sustainable transition of the improved governance and management practices into normal business operations. It further focuses on monitoring achievement of the improvements using the performance metrics and expected benefits.

8.2.7 Phase 7—How Do We Keep the Momentum Going?

Phase 7 reviews the overall success of the initiative, identifies further governance or management requirements and reinforces the need for continual improvement. It also prioritizes further opportunities to improve the governance system.

Program and project management is based on good practices and provides for checkpoints at each of the seven phases to ensure that the program's performance is on track, the business case and risk are updated, and planning for the next phase is adjusted as appropriate. It is assumed that the enterprise's standard approach would be followed.

Further guidance on program and project management can also be found in COBIT management objectives BAI01 *Managed programs* and BAI11 *Managed projects*. Although reporting is not mentioned explicitly in any of the phases, it is a continual thread through all of the phases and iterations.

8.3 Relationship Between *COBIT® 2019 Design Guide* and *COBIT® 2019 Implementation Guide*

The workflow explained in the *COBIT® 2019 Design Guide* has the following connection points with the *COBIT® 2019 Implementation Guide*. The *COBIT® 2019 Design Guide* elaborates a set of tasks defined in the *COBIT® 2019 Implementation Guide*. **Figure 8.2** gives a high-level overview of these connection points. More detailed information can be found in the *COBIT® 2019 Design Guide*.

Figure 8.2—Connection Points Between *COBIT Design Guide* and *COBIT Implementation Guide*

COBIT Implementation Guide		*COBIT Design Guide*
Phase 1—What are the drivers? (Continuous improvement [CI] tasks)	→	**Step 1**—Understand the enterprise context and strategy.
Phase 2—Where are we now? (CI tasks)	→	**Step 2**—Determine the initial scope of the governance system. **Step 3**—Refine the scope of the governance system. **Step 4**—Conclude the governance system design.
Phase 3—Where do we want to be? (CI tasks)	→	**Step 4**—Conclude the governance system design.

Chapter 9
Getting Started With COBIT: Making the Case

9.1 Business Case

Common business practice dictates preparing a business case to analyze and justify the initiation of a large project and/or financial investment. This example is provided as a nonprescriptive, generic guide to encourage preparation of a business case to justify investment in an EGIT implementation program. Every enterprise has its own reasons for improving EGIT and its own approach to preparing business cases. This can range from a detailed approach with an emphasis on quantified benefits to a more high-level and qualitative perspective. Enterprises should follow existing internal business case and investment justification approaches, if they exist. This example and the guidance in this publication in provided to help focus on the issues that should be addressed in a business case.

> *The example scenario is Acme Corporation, a large multinational enterprise with a mixture of traditional, well-established business units as well as new Internet-based businesses adopting the very latest technologies. Many of the business units have been acquired and exist in various countries with different local political, cultural and economic environments. The central group's executive management team has been influenced by the latest enterprise governance guidance, including COBIT, which they have used centrally for some time. They want to make sure that rapid expansion and adoption of advanced IT will deliver the value expected; they also intend to manage significant new risk. They have, therefore, mandated enterprisewide adoption of a uniform EGIT approach. This approach includes involvement by the audit and risk functions and internal annual reporting by business unit management of the adequacy of controls in all entities.*

Although the example is derived from actual situations, it does not reflect a specific, existing enterprise.

9.2 Executive Summary

This business case outlines the scope of the proposed EGIT program for Acme Corporation based on COBIT.

A proper business case is needed to ensure that the Acme Corporation board and the business units buy in to the initiative and identify the potential benefits. Acme Corporation will monitor the business case to ensure that the expected benefits are realized.

The scope, in terms of business entities that make up Acme Corporation, is all inclusive. It is acknowledged that some form of prioritization will be applied across all entities for initial coverage by the EGIT program due to limited program resources.

Various stakeholders have an interest in the outcomes of the EGIT program, from the Acme Corporation board of directors to local management at each entity, as well as external stakeholders such as shareholders and government agencies.

Consideration needs to be given to some significant challenges, as well as risk, in the implementation of the EGIT program on the required global scale. One of the more challenging aspects is the entrepreneurial nature of many of the Internet businesses, as well as the decentralized, or federated, business model that exists within Acme Corporation.

The EGIT program will be achieved by focusing on the capability of the Acme processes and other components of the governance system in relation to those that are defined in COBIT, relevant to each business unit. The relevant and prioritized governance and management objectives that will receive focus at each entity will be identified through a

facilitated workshop approach by the members of the EGIT program. The objectives will start with the strategy and enterprise goals of each unit, as well as the IT-related business risk scenarios that apply to the specific business unit.

The objective of the EGIT program is to ensure that an adequate governance system, including governance structures, is in place and to increase the level of capability and adequacy of the relevant IT processes. The expectation is that as the capability of an IT process increases, so too will its efficiencies and quality. Simultaneously, the associated risk will proportionally decrease. In this way, real business benefits can be realized by each business unit.

Once the process of assessing the capability level within each business unit has been established, it is anticipated that self-assessments will continue within each business unit as normal business practice.

The EGIT program will be delivered in two distinct phases. The first phase is a development phase, in which the team will develop and test the approach and tool set that will be used across the Acme Corporation. At the end of phase 1, the results will be presented to group management for final approval. Once the final approval has been obtained, in the form of an approved business case, the EGIT program will be rolled out across the entity in the agreed manner (implementation, phase 2).

It must be noted that it is not the responsibility of the EGIT program to implement the remedial actions identified at each business unit. The EGIT program will merely consolidate and report progress as supplied by each unit.

The final challenge that will need to be met by the EGIT program is that of reporting the results in a sustainable manner going forward. This aspect will take time and a significant amount of discussion and development. This discussion and development should result in an enhancement to the existing corporate reporting mechanisms and scorecards.

An initial budget for the development phase of the EGIT program has been prepared. The budget is detailed in a separate schedule. A detailed budget will also be completed for phase 2 of the project and submitted for approval by group management.

9.3 Background

EGIT is an integral part of overall enterprise governance and is focused on IT performance and the management of risk attributable to the enterprise's dependencies on IT.

IT is integrated into the operations of Acme Corporation businesses. For many, the Internet is at the core of their operations. EGIT, therefore, follows the management structure of the group: a decentralized format. Management of each subsidiary/business unit is responsible for ensuring that proper processes are implemented relevant to EGIT.

Annually, the management of each significant subsidiary company is required to submit a formal written report to the appropriate risk committee, which is a subset of the board of directors. This report will detail the extent to which it has implemented the EGIT policy during the financial year. Significant exceptions are to be reported at each scheduled meeting of the appropriate risk committee.

The board of directors, assisted by the risk and audit committees, will ensure that the group's EGIT performance is assessed, monitored, reported and disclosed in an EGIT statement as part of the enterprise's integrated annual report. The statement will be based on reports obtained from the risk, compliance and internal audit teams and the management of each significant subsidiary company. It will provide both internal and external stakeholders with relevant and reliable information about the quality of the group's EGIT performance.

Internal audit services will provide assurance to management and to the audit committee on the adequacy and effectiveness of EGIT.

IT-related business risk will be reported on and discussed as part of the risk management process in the risk registers presented to the relevant risk committee.

9.4 Business Challenges

Due to the pervasive nature of IT and the pace of technology change, a reliable framework is required to adequately control the full IT environment and avoid control gaps that may expose the enterprise to unacceptable risk.

The intention is not to impede the IT operations of the various operating entities. Instead, it is to improve the risk profile of the entities in a manner that makes business sense and provides increased quality of service and efficiencies, while explicitly achieving compliance not only with the Acme Corporation's group EGIT charter, but also with any other legislative, regulatory and/or contractual requirements.

Some examples of likely pain points include:[25]

- Complicated IT assurance efforts due to the entrepreneurial nature of many of the business units
- Complex IT operating models due to the Internet service-based business models in use
- Geographically dispersed entities made up of diverse cultures and languages
- The decentralized/federated and largely autonomous business control model employed within the group
- Implementation of reasonable levels of IT management, given a highly technical and, at times, volatile IT workforce
- IT's balancing of the enterprise's drive for innovation capabilities and business agility with the need to manage risk and have adequate control
- The setting of risk and tolerance levels for each business unit
- An increasing need to focus on meeting regulatory (privacy) and contractual (Payment Card Industry [PCI]) compliance requirements
- Regular audit findings about poor IT controls and reported problems related to IT quality of service
- Successful and on-time delivery of new and innovative services in a highly competitive market

9.4.1 Gap Analysis and Goal

There is currently no groupwide approach or framework for EGIT or use of IT good practices and standards. Among local business units, there are variable levels of adoption of good practice with regard to EGIT. As a result, very little attention has traditionally been paid to the level of IT process capability. Based on experience, the levels are generally low.

The objective of the EGIT program is, therefore, to increase the level of capability and adequacy of IT-related processes and controls appropriate to each business unit, in a prioritized manner.

The outcome should be that significant risk has been identified and articulated, and management can address the risk and report on its status. As the capability level of each business unit increases, quality and efficiency should increase proportionally as well and the IT-related business risk profile of each entity should decrease.

Ultimately, business value should increase as a result of effective EGIT.[26]

[25] This enumeration is a subset of the one in section 4.5 (Design Factors) and is also discussed in the *COBIT® 2019 Implementation Guide*.
[26] Empirical research exists to support the statement. For example, see *op cit* De Haes, Joshi and van Grembergen.

9.4.2 Alternatives Considered

Many IT frameworks exist, each intended to control specific aspects of IT. The COBIT framework is regarded by many as the world's leading EGIT and control framework. It has already been implemented by some subsidiaries of Acme Corporation.

COBIT was chosen by Acme as the preferred framework for EGIT implementation and should, therefore, be adopted by all subsidiaries.

COBIT does not have to be implemented in its entirety; only those areas relevant to the specific subsidiary or business unit need to be implemented, taking into account the following:

1. The development stage of each entity in the business life cycle
2. The business objectives of each entity
3. The importance of IT for the business unit
4. The IT-related business risk faced by each entity
5. Legal and contractual requirements
6. Any other pertinent reasons

If a specific subsidiary or business unit has already implemented another framework, or an implementation is planned in the future, the implementation should be mapped to COBIT for reasons of reporting, audit and clarity of internal control.

9.5 Proposed Solution

The EGIT program is being planned in two distinct phases.

9.5.1 Phase 1. Pre-planning

Phase 1 of the EGIT program is the development stage. During this stage of the program, the following steps are undertaken:

1. The core team structure is finalized among the stakeholders and participants on the project.
2. The core team completes COBIT foundation training.
3. Workshops with the core team are conducted to define an approach for the group.
4. An online community is created within Acme Corporation to act as a repository for knowledge sharing.
5. All stakeholders and their needs are identified.
6. Current committee structures, roles and responsibilities, decision rules, and reporting arrangements are clarified and realigned, if required.
7. A business case for the EGIT program is developed and maintained, as a foundation for the successful implementation of the program.
8. A communication plan is created for guiding principles, policies and expected benefits throughout the program.
9. The assessment and reporting tools for use during the life of the program and beyond are developed.
10. The approach is tested at one local entity. This activity is for ease of logistics and to facilitate the refinement of the approach and tools.
11. The refined approach is piloted at one of the foreign entities. This is to understand and quantify the difficulties of running the EGIT program assessment phase under more challenging business conditions.

12. The final business case and approach are presented, including a roll-out plan to Acme Corporation executive management for approval.

9.5.2 Phase 2. Program Implementation

The EGIT program is designed to start an ongoing program of continual improvement, based on a facilitated, iterative life cycle by following these steps:

1. Determine the drivers for improving EGIT, from both an Acme Corporation group perspective and at the business unit level.
2. Determine the current status of EGIT.
3. Determine the desired state of EGIT (both short- and long-term).
4. Determine what needs to be implemented at the business unit level to enable local business objectives, and thereby align with group expectations.
5. Implement the identified and agreed improvement projects at the local business unit level.
6. Realize and monitor the benefits.
7. Sustain the new way of working by keeping the momentum going.

9.5.3 Program Scope

The EGIT program will cover:

1. All of the group entities. However, the entities will be prioritized for interaction due to limited program resources.
2. The method of prioritization. It will need to be agreed with Acme Corporation management, but could be done on the following basis:
   a. Size of investment
   b. Earnings/contribution to the group
   c. Risk profile from a group perspective
   d. A combination of these criteria
3. The list of entities to be covered during the current financial year. This should be finalized and agreed with Acme Corporation management.

9.5.4 Program Methodology and Alignment

The EGIT program will achieve its mandate by using a facilitated, interactive workshop approach with all the entities.

The approach starts with the business objectives and the objective owners, typically the CEO and chief financial officer (CFO). This approach should ensure that the program outcomes are closely aligned to the expected business outcomes and priorities.

Once the business objectives have been covered, the focus shifts to IT operations, typically under the control of the chief technology officer (CTO) or chief information officer (CIO). At the IT operations level, further details of the IT-related business risk and objectives are considered.

The business and IT objectives, as well as the IT-related business risk, are then combined in a tool (based on COBIT guidance) that will provide a set of focus areas within the COBIT processes for consideration by the business unit. In this fashion, the business unit can prioritize its remediation efforts to address the areas of IT risk.

9.5.5 Program Deliverables

As mentioned earlier, an overall goal of the EGIT program is to embed the good practices of EGIT into the continuing operations of the various group entities.

Specific outcomes will be produced by the EGIT program to enable Acme Corporation to gauge the delivery of the intended outcomes. These include the following:

1. The EGIT program will facilitate internal knowledge sharing via the intranet platform and leverage existing relationships with vendors to the advantage of the individual business units.
2. Detailed reports on each facilitation with the business units will be created derived from the EGIT program assessment tool. The reports will include:
   a. The current prioritized business objectives, and consequent IT objectives, based on COBIT
   b. The IT-related risk identified by the business unit in a standardized format, and the agreed focus areas for attention by the business unit based on COBIT processes and practices and other recommended components
3. Overall progress reports on the intended coverage of the Acme Corporation business units by the EGIT program will be created.
4. Consolidated group reporting will cover:
   a. Progress from business units engaged with their agreed implementation projects based on monitoring agreed performance metrics
   b. Consolidated IT risk view across the Acme Corporation entities
   c. Specific requirements of the risk committee(s)
5. Financial reporting on the program budget vs. actual amount spent will be generated.
6. Benefit monitoring and reporting against business-unit-defined value objectives and metrics will be created.

9.5.6 Program Risk

The following are considered potential types of risk to the successful initiation and ongoing success of the Acme Corporation EGIT program. Risk will be mitigated by focusing on change enablement and will be monitored and addressed continually via program reviews and a risk register. These types of risk are:

1. Management commitment and support for the program, both at the group level as well as the local business unit level
2. Demonstrating actual value delivery and benefits to each local entity through the adoption of the program. The local entities should want to adopt the process for the value it will deliver, rather than doing it because of the policy in place.
3. Local management's active participation in the implementation of the program
4. Identifying key stakeholders at each entity for participation in the program
5. Business insight within the IT management ranks
6. Successful integration with any governance or compliance initiatives that exist within the group
7. The appropriate committee structures to oversee the program. For example, the progress of the EGIT program overall could become an agenda item of the IT executive committee. Local equivalents would also need to be constituted. This could be replicated geographically, as well as at the local holding company level, where appropriate.

9.5.7 Stakeholders

The following have been identified as stakeholders in the outcome of the EGIT program:

1. Risk committee
2. IT executive committee
3. Governance team
4. Compliance staff
5. Regional management
6. Local entity-level executive management (including IT management)
7. Internal audit services

A final structure containing the individual names of stakeholders will be compiled and published after consultation with group management.

The EGIT program needs the identified stakeholders to provide the following:

1. Guidance as to the overall direction of the EGIT program. This includes decisions on significant governance-related topics defined in a group RACI chart according to COBIT guidance. It further includes setting priorities, agreeing on funding and approving value objectives.
2. Acceptance of the deliverables and monitoring the expected benefits of the EGIT program

9.5.8 Cost-Benefit Analysis

The program should identify the expected benefits and monitor to ensure that real business value is being generated from the investment. Local management should motivate and sustain the program. Sound EGIT should result in benefits that will be set as specific targets for each business unit and monitored and measured during implementation to ensure that they are realized. The benefits include:

1. Maximizing the realization of business opportunities through IT, while mitigating IT-related business risk to acceptable levels, thus ensuring that risk is responsibly weighed against opportunity in all business initiatives
2. Support of the business objectives by key investments and optimum returns on those investments, thus aligning IT initiatives and objectives directly with business strategy
3. Legislative, regulatory and contractual compliance as well as internal policy and procedural compliance
4. A consistent approach to measuring and monitoring progress, efficiency and effectiveness
5. Improved quality of service delivery
6. Lowered cost of IT operations and/or increased IT productivity by accomplishing more work consistently in less time and with fewer resources

Central costs will include the time required for group program management, external advisory resources and initial training courses. These central costs have been estimated for phase 1. The cost of assessment workshops for individual business unit management and process owners (attendance, venue, facilitators and other related costs) will be funded locally and an estimate provided. Specific project improvement initiatives for each business unit will be estimated in phase 2 and considered on a case-by-case basis and overall. This will enable the group to maximize efficiency and standardization.

9.5.9 Challenges and Success Factors

Figure 9.1 summarizes the challenges that could affect the EGIT program during the implementation period of the program and the critical success factors that should be addressed to ensure a successful outcome.

Figure 9.1—Challenges and Planned Actions for Acme Corporation

Challenge	Critical Success Factor—Actions Planned
Inability to gain and sustain support for improvement objectives	• Mitigate through committee structures within the group (to be agreed and constituted).
Communication gap between IT and the business	• Involve all stakeholders.
Cost of improvements outweighing perceived benefits	• Focus on benefit identification.
Lack of trust and good relationships between IT and the enterprise	• Foster open and transparent communication about performance, with links to corporate performance management. • Focus on business interfaces and service mentality. • Publish positive outcomes and lessons learned to help establish and maintain credibility. • Ensure the CIO maintains credibility and leadership in building trust and relations. • Formalize governance roles and responsibilities in the business so accountability for decisions is clear. • Identify and communicate evidence of real issues, risk that needs to be avoided and benefits to be gained (in business terms) relating to proposed improvements. • Focus on change enablement planning.
Lack of understanding of the Acme environment by those responsible for the EGIT program	• Apply a consistent assessment methodology.
Various levels of complexity (technical, organizational, operating model)	• Treat the entities on a case-by-case basis. Benefit from lessons learned and sharing knowledge.
Understanding of EGIT frameworks, procedures and practices	• Train and mentor.
Resistance to change	• Ensure that implementation of the life cycle also includes change enablement activities.
Adoption of improvements	• Enable local empowerment at the entity level.
Difficulty in integrating EGIT with the governance models of outsourcing partners	• Involve suppliers/third parties in EGIT activities. • Incorporate conditions and right to audit in contracts.
Failure to realize EGIT implementation commitments	• Manage expectations. • Keep it simple, realistic and practical. • Break down the overall project into small achievable projects, building experience and benefits.
Trying to do too much at once; IT tackling overly complex and/or difficult problems	• Apply program and project management principles. • Use milestones. • Prioritize 80/20 tasks (80 percent of the benefit with 20 percent of the effort) and be careful about sequencing in the correct order. Capitalize on quick wins. • Build trust/confidence. Have skills and experience to keep it simple and practical. • Reuse what is there as a base.
IT in fire-fighting mode and/or not prioritizing well and unable to focus on EGIT	• Apply good leadership skills. • Gain commitment and drive from top management so people are made available to focus on EGIT. • Address root causes in the operational environment (external intervention, management prioritizing IT). • Apply tighter discipline over/management of business requests. • Obtain external assistance.

Figure 9.1—Challenges and Planned Actions for Acme Corporation *(cont.)*	
Challenge	**Critical Success Factor—Actions Planned**

Absence of required IT skills and competencies, such as understanding of the business, processes, soft skills	• Focus on change enablement planning:
	  ■ Development
	  ■ Training
	  ■ Coaching
	  ■ Mentoring
	  ■ Feedback into recruitment process
	  ■ Cross-training

Improvements not adopted or applied	• Use a case-by-case approach with agreed principles for the local entity. It must be practical to implement.
Benefits difficult to show or prove	• Identify performance metrics.
Loss of interest and momentum	• Build group-level commitment, including communication.

Page intentionally left blank

Chapter 10
COBIT and Other Standards

10.1 Guiding Principle

One of the guiding principles applied throughout the development of COBIT® 2019 was to maintain the positioning of COBIT as an umbrella framework. This means that COBIT continues to align with a number of relevant standards, frameworks and/or regulations.

In this context, alignment means that COBIT does not contradict any guidance in the related standards. At the same time, it is important to remember that COBIT does not copy the contents of these related standards. Instead, it usually provides equivalent statements or references to related guidance.

10.2 List of Referenced Standards

Standards and guidance used during the development of the COBIT® 2019 update include:

- CIS® Center for Internet Security®, *The CIS Critical Security Controls for Effective Cyber Defense,* Version 6.1, August 2016
- Cloud standards and good practices:
  - Amazon Web Services (AWS®)
  - *Security Considerations for Cloud Computing*, ISACA
  - *Controls and Assurance in the Cloud: Using COBIT® 5*, ISACA
- CMMI® Cybermaturity Platform, 2018
- CMMI® Data Management Maturity (DMM)℠ model, 2014
- CMMI® Development V2.0, CMMI Institute, USA, 2018
- Committee of Sponsoring Organizations (COSO) Enterprise Risk Management (ERM) Framework, June 2017
- European Committee for Standardization (CEN), *e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework*, EN 16234-1:2016
- HITRUST® Common Security Framework, version 9, September 2017
- Information Security Forum (ISF), *The Standard of Good Practice for Information Security 2016*
- International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) standards
  - ISO/IEC 20000-1:2011(E)
  - ISO/IEC 27001:2013/Cor.2:2015(E)
  - ISO/IEC 27002:2013/Cor.2:2015(E)
  - ISO/IEC 27004:2016(E)
  - ISO/IEC 27005:2011(E)
  - ISO/IEC 38500:2015(E)
  - ISO/IEC 38502:2017(E)
- Information Technology Infrastructure Library (ITIL®) v3, 2011
- Institute of Internal Auditors® (IIA®), "Core Principles for the Professional Practice of Internal Auditing"
- *King IV Report on Corporate Governance™*, 2016

- US National Institute of Standards and Technology (NIST) standards:
  - *Framework for Improving Critical Infrastructure Cybersecurity* V1.1, April 2018
  - Special Publication 800-37, Revision 2 (Draft), May 2018
  - Special Publication 800-53, Revision 5 (Draft), August 2017
- "Options for Transforming the IT Function Using Bimodal IT," *MIS Quarterly Executive* (white paper)
- *A Guide to the Project Management Body of Knowledge: PMBOK® Guide, Sixth Edition*, 2017
- PROSCI® 3-Phase Change Management Process
- Scaled Agile Framework for Lean Enterprises (SAFe®)
- Skills Framework for the Information Age (SFIA®) V6, 2015
- The Open Group IT4IT™ Reference Architecture, version 2.0
- The Open Group Standard TOGAF® version 9.2, 2018
- The TBM Taxonomy, The TBM Council