COBIT® 2019

DESIGN GUIDE

Designing an Information and Technology Governance Solution

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 Design Guide: Designing an Information and Technology Governance Solution* (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 Design Guide: Designing an Information and Technology Governance Solution
ISBN 978-1-60420-765-1

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
Floris Ampe, CISA, CRISC, CGEIT, CIA, ISO27000, PRINCE2, TOGAF, PwC, Belgium
Graciela Braga, CGEIT, Auditor and Advisor, Argentina
James L. Golden, Golden Consulting Associates, USA
J. Winston Hayden, CISA, CRISC, CISM, CGEIT, South Africa
Abdul Rafeq, CISA, CGEIT, FCA, Managing Director, Wincer Infotech Limited, India
Jo Stewart-Rattray, CISA, CRISC, CISM, CGEIT, FACS CP, BRM Holdich, Australia

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 (Pty) Ltd, 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.

Page intentionally left blank

TABLE OF CONTENTS

List of Figures 11

Part I. Design Process 15

Chapter 1. Introduction and Purpose 15
1.1 Governance Systems 15
1.2 Structure of This Publication 15
1.3 Target Audience for This Publication 16
1.4 Related Guidance: *COBIT® 2019 Implementation Guide* 16

Chapter 2. Basic Concepts: Governance System and Components 17
2.1 Introduction 17
2.2 Governance and Management Objectives 18
2.3 Components of the Governance System 20
2.4 Focus Areas 20
2.5 Capability Levels 20
2.6 Design Factors 21
2.6.1 Why is There no Industry Sector Design Factor? 28

Chapter 3. Impact of Design Factors 29
3.1 Impact of Design Factors 29

Chapter 4. Designing a Tailored Governance System 31
4.1 Introduction 31
4.2 Step 1: Understand the Enterprise Context and Strategy 32
4.2.1 Understand Enterprise Strategy 32
4.2.2 Understand Enterprise Goals 32
4.2.3 Understand the Risk Profile 33
4.2.4 Understand Current I&T-Related Issues 33
4.2.5 Conclusion 33
4.3 Step 2: Determine the Initial Scope of the Governance System 33
4.3.1 Translating Design Factors into Governance and Management Priorities 34
4.3.2 Consider Enterprise Strategy (Design Factor 1) 34
4.3.3 Consider Enterprise Goals and Apply the COBIT Goals Cascade (Design Factor 2) 35
4.3.4 Consider the Risk Profile of the Enterprise (Design Factor 3) 36
4.3.5 Consider Current I&T-Related Issues of the Enterprise (Design Factor 4) 36
4.3.6 Conclusion 36
4.4 Step 3: Refine the Scope of the Governance System 37
4.4.1 Consider the Threat Landscape (Design Factor 5) 37
4.4.2 Consider Compliance Requirements (Design Factor 6) 38
4.4.3 Consider the Role of IT (Design Factor 7) 38
4.4.4 Consider the Sourcing Model for IT (Design Factor 8) 39
4.4.5 Consider IT Implementation Methods (Design Factor 9) 39
4.4.6 Consider the Technology Adoption Strategy (Design Factor 10) 40
4.4.7 Consider Enterprise Size (Design Factor 11) 41
4.4.8 Conclusion 41
4.5 Step 4: Resolve Conflicts and Conclude the Governance System Design 41
4.5.1 Resolve Inherent Priority Conflicts 42
4.5.1.1 Purpose 42
4.5.1.2 Resolution Strategies 42
4.5.1.3 Resolution Approach 43

4.5.2 Conclude the Governance System Design....43
4.5.2.1 Concluding the Design....43
4.5.2.2 Sustaining the Governance System....44

Chapter 5. Connecting With the *COBIT® 2019 Implementation Guide*....45

5.1 Purpose of the *COBIT® 2019 Implementation Guide*....45
5.2 COBIT Implementation Approach....45
5.2.1 Phase 1—What Are the Drivers?....46
5.2.2 Phase 2—Where Are We Now?....46
5.2.3 Phase 3—Where Do We Want to Be?....47
5.2.4 Phase 4—What Needs to Be Done?....47
5.2.5 Phase 5—How Do We Get There?....47
5.2.6 Phase 6—Did We Get There?....47
5.2.7 Phase 7—How Do We Keep the Momentum Going?....47
5.3 Relationship Between *COBIT Design Guide* and *COBIT Implementation Guide*....47

Part II. Execution and Examples....51

Chapter 6. The Governance System Design Toolkit....51

6.1 Introduction....51
6.2 Toolkit Basics....51
6.3 Step 1 and Step 2: Determine the Initial Scope of the Governance System....52
6.3.1 Enterprise Strategy (Design Factor 1)....52
6.3.2 Enterprise Goals and Applying the COBIT Goals Cascade (Design Factor 2)....53
6.3.3 Risk Profile of the Enterprise (Design Factor 3)....54
6.3.4 Current I&T-Related Issues of the Enterprise (Design Factor 4)....55
6.3.5 Conclusion....56
6.4 Step 3: Refine the Scope of the Governance System....58
6.4.1 Threat Landscape (Design Factor 5)....59
6.4.2 Compliance Requirements (Design Factor 6)....60
6.4.3 Role of IT (Design Factor 7)....61
6.4.4 Sourcing Model for IT (Design Factor 8)....62
6.4.5 IT Implementation Methods (Design Factor 9)....63
6.4.6 Technology Adoption Strategy (Design Factor 10)....64
6.4.7 Enterprise Size (Design Factor 11)....65
6.4.8 Conclusion....65

Chapter 7. Examples....67

7.1 Introduction....67
7.2 Example 1: Manufacturing Enterprise....67
7.2.1 Step 1: Understand the Enterprise Context and Strategy....67
7.2.2 Step 2: Determine the Initial Scope of the Governance System....71
7.2.3 Step 3: Refine the Scope of the Governance System....80
7.2.4 Step 4: Conclude the Governance Solution Design....89
7.2.4.1 Governance and Management Objectives....89
7.2.4.2 Other Components....91
7.2.4.3 Specific Focus Area Guidance....91
7.3 Example 2: Medium-Sized Innovative Company....92
7.3.1 Step 1: Understand the Enterprise Context and Strategy....92
7.3.2 Step 2: Determine the Initial Scope of the Governance System....96
7.3.3 Step 3: Refine the Scope of the Governance System....105
7.3.4 Step 4: Conclude the Governance Solution Design....115
7.3.4.1 Governance and Management Objectives....115
7.3.4.2 Other Components....117
7.3.4.3 Specific Focus Area Guidance....118
7.4 Example 3: High-Profile Government Agency....118
7.4.1 Step 1: Understand the Enterprise Context and Strategy....119
7.4.2 Step 2: Determine the Initial Scope of the Governance System....123

7.4.3 Step 3: Refine the Scope of the Governance System....131
7.4.4 Step 4: Conclude the Governance Solution Design....132
7.4.4.1 Governance and Management Objectives....132
7.4.4.2 Other Components....134
7.4.4.3 Specific Focus Area Guidance....135
Appendices....137
Appendix A: Mapping Table—Enterprise Strategies to Governance and Management Objectives....137
Appendix B: Mapping Table—Enterprise Goals to Alignment Goals....139
Appendix C: Mapping Table—Alignment Goals to Governance and Management Objectives....140
Appendix D: Mapping Table—IT Risk to Governance and Management Objectives....141
Appendix E: Mapping Table—IT-Related Issues to Governance and Management Objectives....143
Appendix F: Mapping Table—Threat Landscape to Governance and Management Objectives....145
Appendix G: Mapping Table—Compliance Requirements to Governance and Management Objectives....146
Appendix H: Mapping Table—Role of IT to Governance and Management Objectives....147
Appendix I: Mapping Table—Sourcing Model for IT to Governance and Management Objectives....148
Appendix J: Mapping Table—IT Implementation Methods to Governance and Management Objectives....149
Appendix K: Mapping Table—Technology Adoption Strategies to Governance and Management Objectives....150

Page intentionally left blank

LIST OF FIGURES

Part I. Design Process

Chapter 2. Basic Concepts: Governance System and Components

Figure 2.1—COBIT Overview 17
Figure 2.2—COBIT Core Model 19
Figure 2.3—Capability Levels for Processes 21
Figure 2.4—COBIT Design Factors 22
Figure 2.5—Enterprise Strategy Design Factor 22
Figure 2.6—Enterprise Goals Design Factor 22
Figure 2.7—Risk Profile Design Factor (IT Risk Categories) 23
Figure 2.8—I&T-Related Issues Design Factor 26
Figure 2.9—Threat Landscape Design Factor 26
Figure 2.10—Compliance Requirements Design Factor 27
Figure 2.11—Role of IT Design Factor 27
Figure 2.12—Sourcing Model for IT Design Factor 27
Figure 2.13—IT Implementation Methods Design Factor 27
Figure 2.14—Technology Adoption Strategy Design Factor 28
Figure 2.15—Enterprise Size Design Factor 28

Chapter 3. Impact of Design Factors

Figure 3.1—Impact of Design Factors on Governance System 29

Chapter 4. Designing a Tailored Governance System

Figure 4.1—Governance System Design Workflow 31
Figure 4.2—Governance and Management Objectives Priority Mapped to Enterprise Strategy Design Factor 34
Figure 4.3—Governance and Management Objectives Priority Mapped to Threat Landscape Design Factor 37
Figure 4.4—Governance and Management Objectives Priority Mapped to Compliance Requirements Design Factor 38
Figure 4.5—Governance and Management Objectives Priority Mapped to Role of IT Design Factor 38
Figure 4.6—Governance and Management Objectives Priority Mapped to Sourcing Model for IT Design Factor 39
Figure 4.7—Governance and Management Objectives Priority Mapped to IT Implementation Methods Design Factor 40
Figure 4.8—Governance and Management Objectives Priority Mapped to Technology Adoption Strategy Design Factor 40
Figure 4.9—Governance and Management Objectives Priority Mapped to Enterprise Size Design Factor 41
Figure 4.10—Governance System Design Step 4—Conclusion 42

Chapter 5. Connecting With the COBIT® 2019 Implementation Guide

Figure 5.1—COBIT Implementation Roadmap 46
Figure 5.2—Connection Points Between COBIT Design Guide and COBIT Implementation Guide 48

Part II. Execution and Examples

Chapter 7. Examples

Figure 7.1—Example 1, Step 1.1: Enterprise Strategy 67
Figure 7.2—Example 1, Step 1.2: Enterprise Goals 68
Figure 7.3—Example 1, Step 1.3: Risk Profile 69
Figure 7.4—Example 1, Step 1.4: I&T-Related Issues 70
Figure 7.5—Example 1, Step 2.1: Enterprise Strategy 71
Figure 7.6—Example 1, Step 2.1: Resulting Governance/Management Objectives Importance for Design Factor 1 Enterprise Strategy 72
Figure 7.7—Example 1, Step 2.2: Enterprise Goals 73
Figure 7.8—Example 1, Step 2.2: Resulting Governance/Management Objectives Importance for Design Factor 2 Enterprise Goals 74
Figure 7.9—Example 1, Step 2.3: Risk Profile 75

Figure 7.10—Example 1, Step 2.3: Resulting Governance/Management Objectives Importance for Design Factor 3 Risk Profile 76
Figure 7.11—Example 1, Step 2.4: I&T-Related Issues 77
Figure 7.12—Example 1, Step 2.4: Resulting Governance/Management Objectives Importance for Design Factor 4 I&T-Related Issues 78
Figure 7.13—Example 1, Step 2.5: Initial Design Summary of Governance and Management Objectives Importance....79
Figure 7.14—Example 1 Tailored Version of Governance System 80
Figure 7.15—Example 1, Step 3.1: Threat Landscape 82
Figure 7.16—Example 1, Step 3.1: Resulting Governance/Management Objectives Importance for Design Factor 5 Threat Landscape....82
Figure 7.17—Example 1, Step 3.2: Compliance Requirements 83
Figure 7.18—Example 1, Step 3.2: Resulting Governance/Management Objectives Importance for Design Factor 6 Compliance Requirements....84
Figure 7.19—Example 1, Step 3.3: Role of IT 84
Figure 7.20—Example 1, Step 3.3: Resulting Governance/Management Objectives Importance for Design Factor 7 Role of IT ...85
Figure 7.21—Example 1, Step 3.4: Sourcing Model for IT 86
Figure 7.22—Example 1, Step 3.4: Resulting Governance/Management Objectives Importance for Design Factor 8 Sourcing Model for IT....86
Figure 7.23—Example 1, Step 3.5: IT Implementation Methods....87
Figure 7.24—Example 1, Step 3.5: Resulting Governance/Management Objectives Importance for Design Factor 9 IT Implementation Methods 87
Figure 7.25—Example 1, Step 3.6: Technology Adoption Strategy....88
Figure 7.26—Example 1, Step 3.6: Resulting Governance/Management Objectives Importance for Design Factor 10 Technology Adoption Strategy 88
Figure 7.27—Example 1, Step 4: Governance and Management Objectives Importance (All Design Factors)....89
Figure 7.28—Example 1, Governance and Management Objectives and Target Process Capability Levels....90
Figure 7.29—Example 2, Step 1.1: Enterprise Strategy 92
Figure 7.30—Example 2, Step 1.2: Enterprise Goals 93
Figure 7.31—Example 2, Step 1.3: Risk Profile....94
Figure 7.32—Example 2, Step 1.4: I&T-Related Issues 95
Figure 7.33—Example 2, Step 2.1: Enterprise Strategy 96
Figure 7.34—Example 2, Step 2.1: Resulting Governance/Management Objectives Importance for Design Factor 1 Enterprise Strategy 97
Figure 7.35—Example 2, Step 2.2: Enterprise Goals 98
Figure 7.36—Example 2, Step 2.2: Resulting Governance/Management Objectives Importance for Design Factor 2 Enterprise Goals 99
Figure 7.37—Example 2, Step 2.3: Risk Profile....100
Figure 7.38—Example 2, Step 2.3: Resulting Governance/Management Objectives Importance for Design Factor 3 Risk Profile....101
Figure 7.39—Example 2, Step 2.4: I&T-Related Issues 102
Figure 7.40—Example 2, Step 2.4: Resulting Governance/Management Objectives Importance for Design Factor 4 I&T-Related Issues 103
Figure 7.41—Example 2, Step 2.5: Initial Design Summary of Governance and Management Objectives Importance....104
Figure 7.42—Governance System Scope Refinement Table Applied to Example 2 105
Figure 7.43—Example 2, Step 3.1: Threat Landscape 107
Figure 7.44—Example 2, Step 3.1: Resulting Governance/Management Objectives Importance for Design Factor 5 Threat Landscape....107
Figure 7.45—Example 2, Step 3.2: Compliance Requirements 109
Figure 7.46—Example 2, Step 3.2: Resulting Governance/Management Objectives Importance for Design Factor 6 Compliance Requirements....109
Figure 7.47—Example 2, Step 3.3: Role of IT 110
Figure 7.48—Example 2, Step 3.3: Resulting Governance/Management Objectives Importance for Design Factor 7 Role of IT .110
Figure 7.49—Example 2, Step 3.4: Sourcing Model for IT....112
Figure 7.50—Example 2, Step 3.4: Resulting Governance/Management Objectives Importance for Design Factor 8 Sourcing Model for IT 112
Figure 7.51—Example 2, Step 3.5: IT Implementation Methods....113
Figure 7.52—Example 2, Step 3.5: Resulting Governance/Management Objectives Importance for Design Factor 9 IT Implementation Methods 113
Figure 7.53—Example 2, Step 3.6: Technology Adoption Strategy....114
Figure 7.54—Example 2, Step 3.6: Resulting Governance/Management Objectives Importance for Design Factor 10 Technology Adoption Strategy 114

Figure 7.55—Example 2, Step 4.1: Governance and Management Objectives Importance (All Design Factors)....115
Figure 7.56—Example 2 Governance and Management Objectives with Target Process Capability Levels....116
Figure 7.57—Example 3, Step 1.1: Enterprise Strategy....119
Figure 7.58—Example 3, Step 1.2: Enterprise Goals....120
Figure 7.59—Example 3, Step 1.3: Risk Profile....121
Figure 7.60—Example 3, Step 1.4: I&T-Related Issues....122
Figure 7.61—Example 3, Step 2.1: Enterprise Strategy....123
Figure 7.62—Example 3, Step 2.1: Resulting Governance/Management Objectives Importance for Design Factor 1 Enterprise Strategy....123
Figure 7.63—Example 3, Step 2.2: Enterprise Goals....124
Figure 7.64—Example 3, Step 2.2: Resulting Governance/Management Objectives Importance for Design Factor 2 Enterprise Goals....125
Figure 7.65—Example 3, Step 2.3: Risk Profile....126
Figure 7.66—Example 3, Step 2.3: Resulting Governance/Management Objectives Importance for Design Factor 3 Risk Profile....127
Figure 7.67—Example 3, Step 2.4: I&T-Related Issues....128
Figure 7.68—Example 3, Step 2.4: Resulting Governance/Management Objectives Importance for Design Factor 4 I&T-Related Issues....129
Figure 7.69—Example 3, Step 2.5: Initial Design Summary of Governance and Management Objectives Importance....130
Figure 7.70—Governance System Scope Refinement Table Applied to Example 3....131
Figure 7.71—Example 3, Step 4: Governance and Management Objectives Importance (All Design Factors)....132
Figure 7.72—Example 3 Governance and Management Objectives and Target Process Capability Levels....133
Figure 7.73—Example 3, Step 4: Organizational Structures....135

Appendices....137

Figure A.1—Mapping Enterprise Strategies to Governance and Management Objectives....137
Figure A.2—Mapping Enterprise Goals to Alignment Goals....139
Figure A.3—Mapping Alignment Goals to Governance and Management Objectives....140
Figure A.4—Mapping IT Risk to Governance and Management Objectives....141
Figure A.5—Mapping I&T-Related Issues to Governance and Management Objectives....143
Figure A.6—Mapping Threat Landscape to Governance and Management Objectives....145
Figure A.7—Mapping Compliance Requirements to Governance and Management Objectives....146
Figure A.8—Mapping Role of IT to Governance and Management Objectives....147
Figure A.9—Mapping Sourcing Model for IT to Governance and Management Objectives....148
Figure A.10—Mapping IT Implementation Methods to Governance and Management Objectives....149
Figure A.11—Mapping Technology Adoption Strategy to Governance and Management Objectives....150

Page intentionally left blank

Part I
Design Process

Chapter 1
Introduction and Purpose

1.1 Governance Systems

This publication describes how an enterprise can design a customized governance solution for enterprise information and technology (I&T). An effective and efficient governance system over I&T is the starting point for generating value. This applies to all types and sizes of enterprises. Governance over a complex domain like I&T requires a multitude of components, including processes, organizational structures, information flows and behaviors. All of these elements must work together in a systemic way; therefore, this publication refers to the tailored governance solution that every enterprise should build as the "governance system for enterprise I&T," or "governance system" for short.

There is no unique, one-size-fits-all governance system for enterprise I&T. Every enterprise has its own distinct character and profile, and will differ from other organizations in several critical respects: size of the enterprise, industry sector, regulatory landscape, threat landscape, role of IT for the organization and tactical technology-related choices, among others. All of these aspects—to which COBIT® refers, collectively, as design factors—require organizations to tailor their governance systems to realize the most value out of their use of I&T.

Tailoring means that an enterprise should start from the COBIT® core model, and from there, apply changes to the generic framework based on the relevance and importance of a series of design factors. This process is called "designing the governance system for enterprise I&T."

1.2 Structure of This Publication

This publication contains the following major parts, chapters and appendices:

Part I: Design Process

- Chapter 1 provides an introduction denoting the structure and intended audience.
- Chapter 2 reviews key concepts and definitions from the *COBIT® 2019 Framework: Introduction and Methodology* publication, including the design factor concept.
- Chapter 3 explores the implications of design factors on the design of the governance solution.
- Chapter 4 is the core of the publication. It presents a workflow for designing an enterprise governance solution, taking into account all potential design factors. The workflow consists of four distinct steps, and results in a tailored governance solution.
- Chapter 5 explains how this publication relates to the *COBIT® 2019 Implementation Guide,* and how the two should be used together.

Part II: Execution and Examples

- Chapter 6 introduces the *COBIT® 2019 Design Guide* toolkit—an Excel® tool that facilitates the governance system design workflow.
- Chapter 7 illustrates how the workflow of Chapter 4 may be applied, using the tool.
- Appendices A through K contain various mapping tables used during the design process.

1.3 Target Audience for This Publication

The target audience for this publication includes a range of direct stakeholders in governance over I&T: board members, executive and senior management, and experienced professionals throughout the enterprise, not only from the business and IT, but also from audit, assurance, compliance, security, privacy and risk management disciplines.

Other indirect stakeholders in governance over I&T include customers, users and citizens; they constitute the most important beneficiaries of good governance, even though most will rarely turn to this publication. Their interests are assumed by the direct stakeholders mentioned previously.

A certain level of experience and a thorough understanding of the enterprise are required to benefit from this guide. Such experience and understanding allow users to customize core COBIT® 2019 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 initial design, to execution and assurance. Indeed, assurance providers may apply the logic and workflow developed in this publication to create a well-substantiated assurance program for the enterprise.

1.4 Related Guidance: *COBIT® 2019 Implementation Guide*

The *COBIT® 2019 Implementation Guide* is related to this publication. It describes the road map for continuously improving governance over enterprise I&T. The (initial) design of such a governance system, which is described herein, is part of the initial phases of that road map.

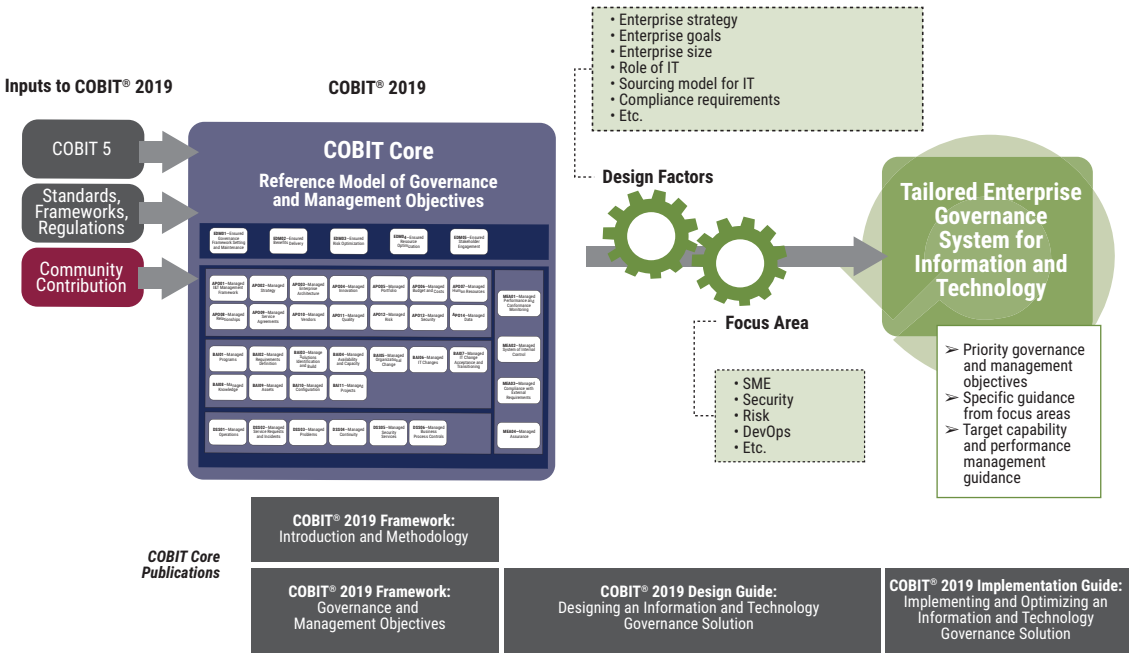
Chapter 5 of this guide elaborates on the links between the two publications, and illustrates how to use them together.

Chapter 2
Basic Concepts: Governance System and Components

2.1 Introduction

Figure 2.1 shows the high-level overview of COBIT® 2019, and how the different publications cover different aspects.

Figure 2.1—COBIT Overview



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 of *COBIT® 2019 Framework: Introduction and Methodology.* 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 COBIT product family is open-ended. At the time of publication of this guide, the following publications are available:

- ***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*.

The content identified as focus areas in **figure 2.1** will contain more detailed guidance on specific themes. 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*.

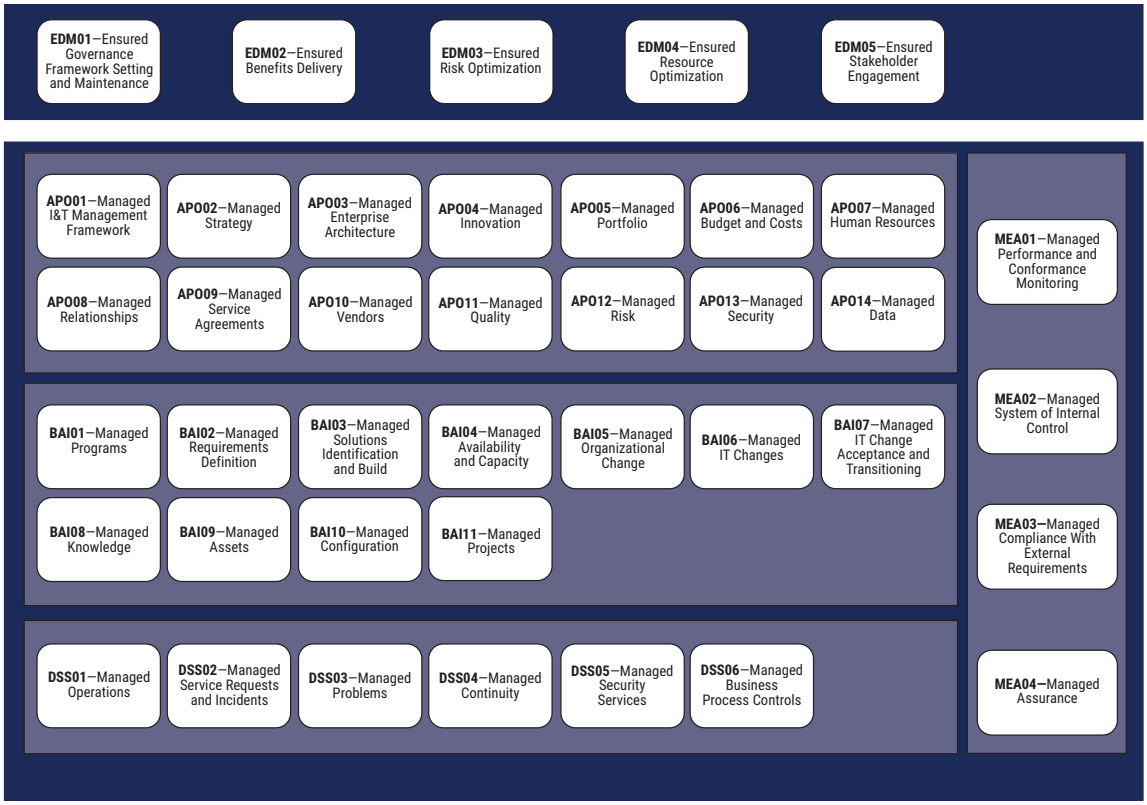
The remainder of this section describes the basic concepts of COBIT® 2019 as they are defined in the COBIT framework publications. The design factors, focus areas and variants concepts will be used to design a tailored governance system for enterprise I&T. A tailored governance system based on COBIT is a system that has taken the generic contents of COBIT and has assigned specific priorities and target capability levels to the governance and management components based on the enterprise's own context and design factor values. When required, specific variants of governance components are also put in place.

2.2 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 2.2**), while a management objective relates to a management process (depicted on the lighter blue background in **figure 2.2**). Boards and executive management are typically accountable for governance processes, while management processes are the domain of senior and middle management.

Figure 2.2—COBIT Core Model



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.

2.3 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.
- 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 2.2**) 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).

2.4 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.[1] Focus areas may contain a combination of generic governance components and variants.

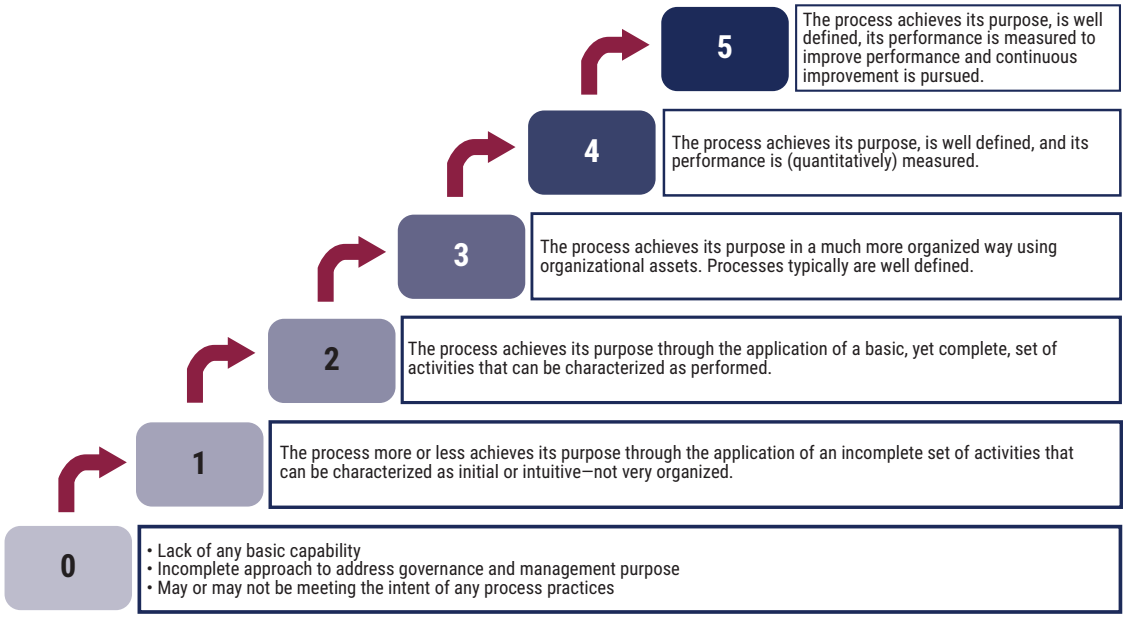
The number of focus areas is virtually unlimited. That is what makes COBIT open-ended. New focus areas can be added as required or as subject matter experts and practitioners contribute to the open-ended COBIT model.

2.5 Capability Levels

COBIT® 2019 supports a Capability Maturity Model Integration (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 for how well a process is implemented and performing. **Figure 2.3** depicts the model, the increasing capability levels and the general characteristics of each.

[1] 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.

Figure 2.3—Capability Levels for Processes



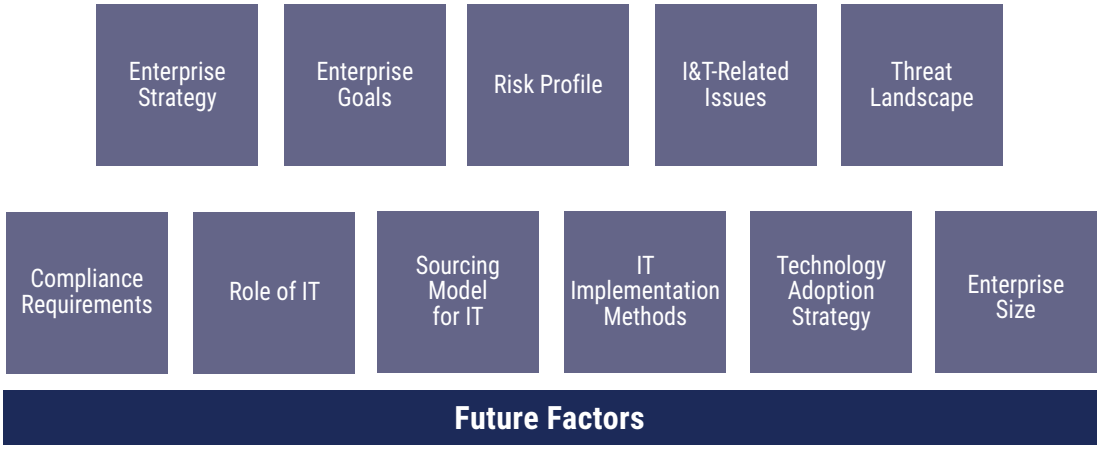
The COBIT core model assigns capability levels to all process activities, allowing to clearly define processes at different capability levels. In this guide we will sometimes refer to 'lower' or 'higher' capability levels. As a convention in this guide, any level at 3 or up is called 'higher,' anything below 3 is called 'lower.'

2.6 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 design factors are listed below and their potential impact on the governance system is discussed in Chapter 3.

Design factors include any combination of the following (**figure 2.4**):

Figure 2.4—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 2.5**. Organizations typically have a primary strategy and, at most, one secondary strategy.

Figure 2.5—Enterprise Strategy Design Factor

Strategy Archetype	Explanation
Growth/Acquisition	The enterprise has a focus on growing (revenues)[2]
Innovation/Differentiation	The enterprise has a focus on offering different and/or innovative products and services to their clients[3]
Cost Leadership	The enterprise has a focus on short-term cost minimization[4]
Client Service/Stability	The enterprise has a focus on providing a stable and client-oriented service.[5]

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 following (**figure 2.6**):

Figure 2.6—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

[2] 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*.

[3] 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.

[4] 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*.

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

Figure 2.6—Enterprise Goals Design Factor *(cont.)*		
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

3. **Risk profile** of the enterprise and current issues in relation to I&T—The risk profile identifies the sort of IT-related risk to which the enterprise is currently exposed and indicates which areas of risk are exceeding the risk appetite.

The risk categories listed in **figure 2.7** merit consideration.[6]

Figure 2.7—Risk Profile Design Factor (IT Risk Categories)		
Reference	**Risk Category**	**Example Risk Scenarios**
1	IT-investment decision making, portfolio definition and maintenance	A. Programs selected for implementation misaligned with corporate strategy and priorities B. Failure of IT-related Investments to support digital strategy of the enterprise C. Selection of wrong software (in terms of cost, performance, features, compatibility, redundancy, etc.) for acquisition and implementation D. Selection of wrong infrastructure (in terms of cost, performance, features, compatibility, etc.) for implementation E. Duplication or important overlaps between different investment initiatives F. Long-term incompatibility between new investment programs and enterprise architecture G. Misallocation, inefficient management and/or competition for resources without alignment to business priorities
2	Program and projects lifecycle management	A. Failure of senior management to terminate failing projects (due to cost explosion, excessive delays, scope creep, changed business priorities) B. Budget overruns for I&T projects C. Lack of quality of I&T projects D. Late delivery of I&T projects E. Failure of third-party outsourcers to deliver projects as per contractual agreements (any combination of exceeded budgets, quality problems, missing functionality, late delivery)
3	IT cost and oversight	A. Extensive dependency on, and use of, user-created, user-defined, user-maintained applications and *ad hoc* solutions B. Excess cost and/or ineffectiveness of I&T-related purchases outside of the I&T procurement process C. Inadequate requirements leading to ineffective Service Level Agreements (SLAs) D. Lack of funds for I&T related investments
4	IT expertise, skills and behavior	A. Lack or mismatch of IT-related skills within IT (e.g., due to new technologies or working methods) B. Lack of business understanding by IT staff that affects service delivery/project quality C. Inability to recruit and retain IT staff D. Recruitment of unsuitable profiles because of lack of due diligence in the recruitment process E. Lack of I&T training F. Overreliance for I&T services on key staff

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

Figure 2.7—Risk Profile Design Factor (IT Risk Categories) *(cont.)*		
Reference	**Risk Category**	**Example Risk Scenarios**
5	Enterprise/IT architecture	A. Complex, inflexible enterprise architecture (EA), obstructing further evolution and expansion, and leading to missed business opportunities B. Failure to timely adopt and exploit new infrastructure or abandon obsolete infrastructure C. Failure to timely adopt and exploit new software (functionality, optimization, etc.) or to abandon obsolete applications D. Undocumented EA leading to inefficiencies and duplications E. Excessive number of exceptions on enterprise architecture standards
6	IT operational infrastructure incidents	A. Accidental damaging of IT equipment B. Errors by IT staff (during backup, during upgrades of systems, during maintenance of systems, etc.) C. Incorrect information input by IT staff or system users D. Destruction of data center (sabotage, etc.) by staff E. Theft of device with sensitive data F. Theft of a key infrastructure component G. Erroneous configuration of hardware components H. Intentional tampering with hardware (security devices, etc.) I. Abuse of access rights from prior roles to access IT infrastructure J. Loss of backup media or backups not checked for effectiveness K. Loss of data by cloud provider L. Operational-service interruption by cloud providers
7	Unauthorized actions	A. Tampering with software B. Intentional modification or manipulation of software leading to incorrect data C. Intentional modification or manipulation of software leading to fraudulent actions D. Unintentional modification of software leading to inaccurate results E. Unintentional configuration and change-management errors
8	Software adoption/ usage problems	A. Nonadoption of new application software by users B. Inefficient use of new software by users
9	Hardware incidents	A. System instability in wake of installing new infrastructure, leading to operational incidents (e.g., BYOD program) B. Inability of systems to handle transaction volumes when user volumes increase C. Inability of systems to handle load when new applications or initiatives are deployed D. Utilities failure (telecom, electricity) E. Hardware failure due to overheating and/or other environmental conditions like humidity F. Damaging of hardware components leading to destruction of data by internal staff G. Loss/disclosure of portable media containing sensitive data (CD, USB-drives, portable disks, etc.) H. Extended resolution time or support delays in case of hardware incidents
10	Software failures	A. Inability to use the software to realize desired outcomes (e.g., failure to make required business model or organizational changes) B. Implementation of immature software (early adopters, bugs, etc.) C. Operational glitches when new software is made operational D. Regular software malfunctioning of critical application software E. Obsolete application software (outdated, poorly documented, expensive to maintain, difficult to extend, not integrated in current architecture, etc.) F. Inability to revert back to former versions in case of operational issues with a new version G. Software-induced corrupted data(base) leading to inaccessible data

Figure 2.7—Risk Profile Design Factor (IT Risk Categories) *(cont.)*		
Reference	**Risk Category**	**Example Risk Scenarios**
11	Logical attacks (hacking, malware, etc.)	A. Unauthorized (internal) users trying to break into systems B. Service interruption due to denial-of-service (DoS) attack C. Website defacement D. Malware attack E. Industrial espionage F. Hacktivism G. Disgruntled employee implements a time bomb which leads to data loss H. Company data stolen through unauthorized access gained by a phishing attack I. Foreign government attacks on critical systems
12	Third-party/supplier incidents	A. Inadequate performance of outsourcer in large-scale, long-term outsourcing arrangement (e.g., through lack of supplier due diligence regarding financial viability, delivery capability and sustainability of supplier's service) B. Accepting unreasonable terms of business from IT suppliers C. Inadequate support and services delivered by vendors, not in line with SLA D. Noncompliance with software license agreements (use and/or distribution of unlicensed software) E. Inability to transfer to alternative suppliers due to overreliance or overdependence on current supplier F. Purchase of IT services (especially cloud services) by the business without consultation /involvement of IT, resulting in inability to integrate the service with in-house services. G. Inadequate or unenforced SLA to obtain agreed services and penalties in case of noncompliance
13	Noncompliance	A. Noncompliance with national or international regulations (e.g., privacy, accounting, manufacturing, environmental, etc.) B. Lack of awareness of potential regulatory changes that may have a business impact C. Operational obstacles caused by regulations D. Failure to comply with internal procedures
14	Geopolitical issues	A. Lack of access due to disruptive incident in other premises B. Government interference and national policies impacting the business C. Targeted action from government-sponsored groups or agencies
15	Industrial action	A. Facilities and building inaccessible because of labor union strike B. Third-party providers unable to provide services because of strike C. Key staff unavailable through industrial action (e.g., transportation or utilities strike)
16	Acts of nature	A. Earthquake destroying or damaging important IT infrastructure B. Tsunami destroying critical premises C. Major storms and tropical cyclone or tornado damaging critical infrastructure D. Major wildfire E. Flooding F. Rising water table leaving critical location unusable G. Rising temperature rendering critical locations uneconomical to operate
17	Technology-based innovation	A. Failure to identify new and important technology trends B. Failure to appreciate the value and potential of new technologies C. Failure to adopt and exploit new technologies in a timely manner (functionality, process optimization, etc.) D. Failure to provide technology support new business models
18	Environmental	A. Environmentally unfriendly equipment (e.g., power consumption, packaging)
19	Data and information management	A. Discovery of sensitive information by unauthorized persons due to inefficient retaining/archiving/disposing of information B. Intentional illicit or malicious modification of data C. Unauthorized disclosure of sensitive information through email or social media D. Loss of IP and/or leakage of competitive information

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[7] include (**figure 2.8**):

Figure 2.8—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, application errors, etc. 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 wasting 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 lack of committed business sponsors 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 implementations of new initiatives or innovations caused by the current IT architecture and system
O	Gap between business and technical knowledge which leads to business users and IT 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 [8]
S	Ignorance and/or noncompliance with security and privacy regulations
T	Inability to exploit new technologies or to innovate using I&T

5. **Threat landscape**—The threat landscape under which the enterprise operates can be classified as shown in **figure 2.9.**

Figure 2.9—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.

[7] 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.

[8] 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 to can be classified according to the categories listed in **figure 2.10.**

Figure 2.10—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 2.11.**

Figure 2.11—Role of IT Design Factor	
Role of IT[9]	**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 of 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 2.12.**

Figure 2.12—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 their own IT staff and services.
Hybrid	A mixed model is applied, combining the three models above in varying degrees.

9. **IT implementation methods**—The methods the enterprise adopts can be classified as noted in **figure 2.13.**

Figure 2.13—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 towards software development (waterfall) and separates software development and operations.
Hybrid	The enterprise uses a mix of traditional and modern IT implementation, often referred to as "bimodal IT."

[9] 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*.

10. **Technology adoption strategy**—The technology adoption strategy can be classified as listed in **figure 2.14.**

Figure 2.14—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 technology to become mainstream and proven before adopting them.
Slow adopter	The enterprise is very late with their adoption of new technologies.

11. **Enterprise size**—Two categories, as shown in **figure 2.15**, are identified for the design of an enterprise's governance system.[10]

Figure 2.15—Enterprise Size Design Factor	
Enterprise Size	**Explanation**
Large enterprise (default)	Enterprises with more than 250 full-time employees (FTEs)
Small and medium enterprise	Enterprise with 50 to 250 FTEs

The impact that design factors have on the design of the governance system is explained in Chapter 3.

2.6.1 Why is There no Industry Sector Design Factor?

Every industry sector has its own unique set of requirements regarding expectations from the use of I&T. However, it is possible to capture the key characteristics of an industry sector by a combination of the design factors listed in the preceding tables. For example:

- The financial sector can be characterized as follows: IT is highly regulated, IT plays a strategic role, it is typically composed of large enterprises and it operates in a high-threat landscape.
- Healthcare providers (e.g., hospitals) typically aim for a combination of client service/stability and innovation strategy, are highly regulated, are subject to a number of specific risk areas (safety, security, privacy, continuity, etc.), operate in a moderate (but increasing) threat landscape, and depend more and more strategically on IT.
- Nonprofit enterprises are typically smaller, and less regulated, have a cost focus, and are not leading innovators in technology adoption.
- Public sector agencies are often large organizations, with client-service and cost-leadership strategies. They have moderate to high risk profiles and are highly regulated by their very nature. The role of IT can vary, from support in conservative agencies, to strategic when it comes to egovernment initiatives. Sourcing models increasingly use outsourced services, whereas they are commonly mainstream followers in technology adoption.

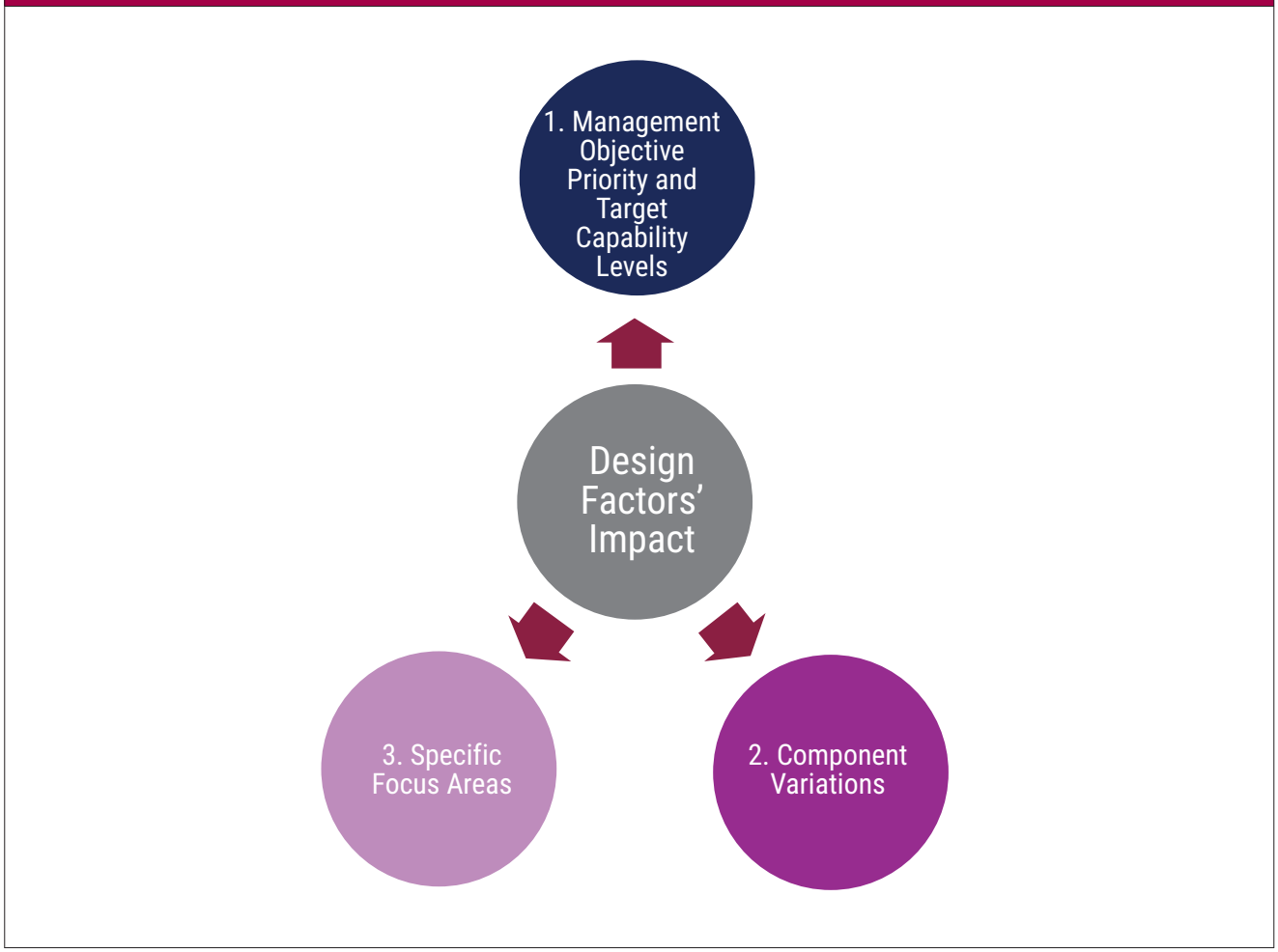
[10] Micro-enterprises, i.e., enterprises with fewer than 50 staff members, are not considered in this publication.

Chapter 3
Impact of Design Factors

3.1 Impact of Design Factors

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 3.1**.

Figure 3.1—Impact of Design Factors on Governance 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. Design factors can mandate specific variations of components or can influence the importance of components.

Example: Small and medium 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.[11]

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 area guidance: some design factors, such as threat landscape, specific risk, target development methods, 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[12] 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.[13]

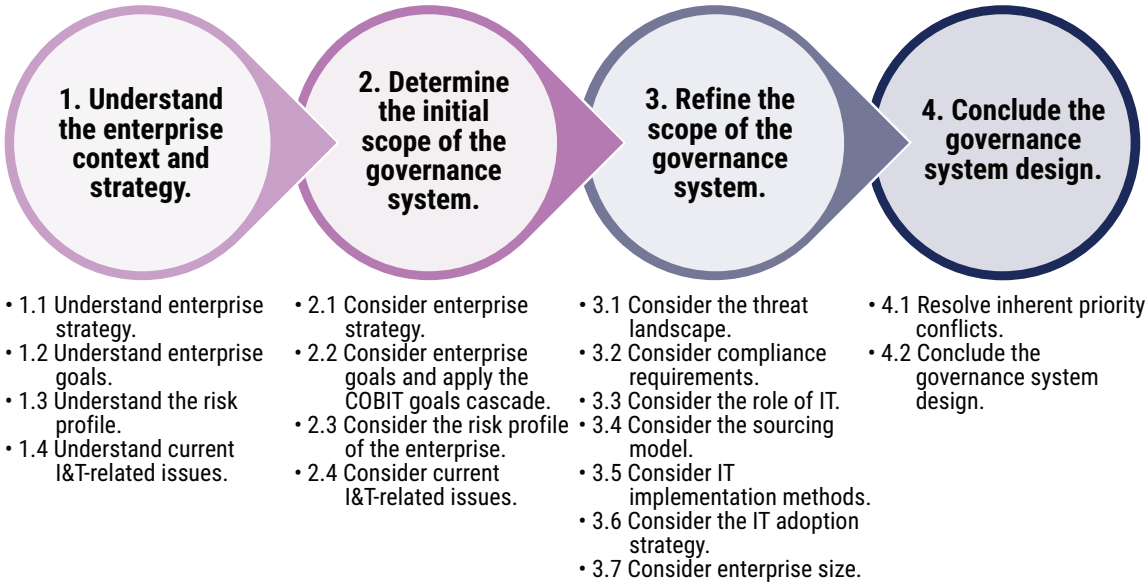
[11] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution,* the small and medium enterprise focus area content was in development and not yet released.
[12] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution,* the DevOps focus area content was in development and not yet released.
[13] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution,* the small and medium enterprise focus area content was in development and not yet released.

Chapter 4
Designing a Tailored Governance System

4.1 Introduction

Figure 4.1 illustrates the proposed flow for designing a tailored governance system. Each step is further discussed in the subsections that follow.

Figure 4.1—Governance System Design Workflow



The different stages and steps in the design process, as illustrated in **figure 4.1**, 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.

Note 1: Before embarking on the design workflow for a governance system, it is important to articulate the unit of analysis. For example, is the intent to design a governance system for a business unit, an enterprise as a whole, a network of enterprises, etc.?[14]

Note 2: The workflow presented in this publication contains four steps. The substeps within each step are not mandatory. For example, an enterprise can decide to design a governance system to address a particular strategy choice (only) or to address certain areas of IT risk (only), without having to run through the full detailed sequence of the workflow.

4.2 Step 1: Understand the Enterprise Context and Strategy

In the first step, the enterprise examines its context, strategy and business environment to achieve a clear understanding across four partially overlapping, interdependent, and often complementary domains. The following subsections outline the critical substeps in Step 1:

- Enterprise strategy
- Enterprise goals and resulting alignment goals
- I&T risk profile
- Current I&T-related issues

4.2.1 Understand Enterprise Strategy

The enterprise must determine which of the archetype enterprise strategies best fit its own enterprise strategy. The archetype enterprise strategies are defined in Section 2.6, Item 1 (see **figure 2.5**).

The mechanism that translates enterprise strategy into a relative rating of importance of governance and management objectives works best when clear choices are made for enterprise strategy archetypes.

It is generally best to identify one primary archetype and select only one secondary archetype. When an enterprise strategy is defined as a mix of equally important strategy archetypes, the governance and management objectives from the COBIT core model tend to become more or less equally important, thus making prioritization difficult.

4.2.2 Understand Enterprise Goals

The enterprise strategy is realized through the achievement of (a set of) enterprise goals. COBIT defines a set of 13 generic enterprise goals; each enterprise can/should prioritize its enterprise goals in alignment with the chosen enterprise strategy. The list of enterprise goals is defined in Section 2.6, Item 2 (see **figure 2.6**).

To translate enterprise goals into a relative rating of importance of governance and management objectives (see the goals cascade, Section 4.3.3), one should make clear choices when selecting enterprise strategy archetypes. It is recommended to identify only a few primary enterprise goals and a limited number of secondary enterprise goals. When all enterprise goals are assigned equally important priorities, the governance and management objectives from the COBIT core model tend to become more or less equally important, thus making prioritization difficult.

[14] Understanding this scope is fully in line with the system design thinking of recursion, which refers to the fact that "any viable enterprise governance of IT system contains, and is contained in, a viable enterprise governance of IT system"; see 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.

4.2.3 Understand the Risk Profile

Another important input to the design of a governance system is to understand the risk profile of the enterprise—that is, to understand which risk scenarios may affect the enterprise, and how to assess their impact and likelihood of materializing.

To achieve this understanding, a high-level risk analysis should be performed, including:

- Identification of relevant risk scenarios (which could be based on the list of risk scenario categories defined in Section 2.6, Item 3; see **figure 2.7**)
- Assessment of impact and likelihood of the scenario materializing, taking into account the current state of risk mitigation controls
- Overall rating of the risk based on the preceding inputs

To be most effective in deciding the appropriate risk profile for governance design purposes, one should make a clear differentiation while assessing I&T risk.

When all IT risk is rated as equally important, the governance and management objectives from the COBIT core model tend to become more or less equally important, thus making prioritization difficult.

4.2.4 Understand Current I&T-Related Issues

Closely related to IT risk are I&T-related issues—also called pain points—from which the enterprise is suffering. (These could be considered risks that have materialized.) IT issues can be identified or reported through risk management, audit, senior management or external stakeholders. A list of common issues is defined in Section 2.5, Item 4 (see **figure 2.8**).

Clear differentiation should be made in rating I&T issues, in order to provide the necessary inputs to determine governance design priorities.

When all I&T-related issues are rated as equally serious, the governance and management objectives from the COBIT core model tend to become more or less equally important, thus making prioritization difficult.

4.2.5 Conclusion

At the end of Step 1, the enterprise will have a clear and consistent view on the enterprise strategy, the enterprise goals, IT-related risk and current I&T issues. In the next step (Section 4.3), this information will be translated into prioritized governance/management objectives for an initial scoping of a customized governance system for the enterprise.

4.3 Step 2: Determine the Initial Scope of the Governance System

To determine the initial scope of the governance system, Step 2 synthesizes information collected during Step 1. Values derived for enterprise strategy, enterprise goals, risk profile and I&T-related issues are translated into a set of prioritized governance components to yield the initial tailored governance system for the enterprise.

4.3.1 Translating Design Factors into Governance and Management Priorities

Step 2 presents a number of relevant design factors and associated descriptive values, whose selection will drive prioritization of governance and management objectives. There are two basic options for this assessment: a qualitative approach and a more quantitative approach.

The **qualitative** approach considers the most relevant governance and management objectives for the values of each design factor. After the initial design and design refinement steps (for the latter, see Section 4.4), a qualitative decision is made on governance and management objectives priorities.

The more **quantitative** approach involves numeric mapping tables created for each design factor. The mapping tables quantify the descriptive values associated with each design factor, in order to indicate their correlation with governance and management objectives.

- Mapping tables in COBIT® 2019 generally contain values between zero (0) and four (4). Four indicates maximum relevance of a governance or management objective with that particular design factor value; zero indicates no relevance.
- Translating design factor values into governance and management objective importance involves a matrix calculation, resulting in a score for each governance and management objective.
- Depending on the actual method preferred, these scores can be further manipulated for presentation purposes (e.g., normalized to certain fixed scales).
- At the end of Steps 2 and 3, the results of several of these calculations need to be consolidated. Again, there is no objectively necessary, fixed method for consolidation; however, it is often best accomplished using a (weighted) summation.

Chapter 7 of this publication includes examples of the quantitative approach. All examples reference an Excel® toolkit that is available from *www.isaca.org/COBIT/Pages/COBIT-2019-Design-Guide.aspx* as a companion to this *COBIT® 2019 Design Guide*.

4.3.2 Consider Enterprise Strategy (Design Factor 1)

For each enterprise strategy archetype, **figure 4.2** lists the most important governance and management objectives, important governance components and relevant focus area guidance. When enterprise strategy is defined as a hybrid strategy, the important governance and management objectives will reflect a combination of elements.

Figure 4.2—Governance and Management Objectives Priority Mapped to Enterprise Strategy Design Factor

Design Factor Value	Governance and Management Objectives Priority	Components	Focus Area Variants

Growth/acquisition	Important management objectives[15] include:
	• APO02, APO03, APO05
	• BAI01, BAI05, BAI11
		Important components:
		• Organizational structures
		  ■ Support the portfolio management role with an investment office
		  ■ Enterprise architect
		• Services, infrastructure and applications
		  ■ Facilitate automation and growth and realize economies of scale
			COBIT core model

[15] 'Important' corresponds to a value of 3 or more in the mapping table of this design factor to governance and management objectives.

Figure 4.2—Governance and Management Objectives Priority Mapped to Enterprise Strategy Design Factor *(cont.)*

Design Factor Value	Governance and Management Objectives Priority	Components	Focus Area Variants
Innovation/ differentiation	Important management objectives include: • APO02, APO04, APO05 • BAI08, BAI11	Important components: • Organizational structures ■ Chief digital officer and/or chief innovation officer • Important influence of culture and behavior component for innovation	COBIT core model
Cost leadership	Important governance and management objectives include: • EDM04 • APO06, APO10	Important components: • Skills and competencies ■ Focus on IT costing and budgeting skills • Important influence of culture and behavior component • Services, infrastructure and applications component (e.g., for automation of controls, improving efficiency)	COBIT core model
Client service/stability	Important governance and management objectives include: • EDM02 • APO08, APO09, APO11 • BAI04 • DSS02, DSS03, DSS04	Important component: • Important influence of culture and behavior component (client centricity)	COBIT core model

4.3.3 Consider Enterprise Goals and Apply the COBIT Goals Cascade (Design Factor 2)

The enterprise strategy is realized by achieving (a set of) enterprise goals. COBIT® 2019 defines 13 generic enterprise goals (see Section 2.6, Item 2 and **figure 2.6**); each enterprise should prioritize these enterprise goals in alignment with the enterprise strategy.

To translate enterprise goals into actionable governance and management objectives:

1. Start with the generic enterprise goals, and determine the most important enterprise goals for the organization. Select the top three to five most important enterprise goals; too many high-priority goals will produce less meaningful goals cascade results.
2. Find the prioritized enterprise goals on the mapping table between enterprise goals and alignment goals (Appendix B). Use the mapping to determine the most important alignment goals.
3. Find the prioritized alignment goals on the mapping table between alignment goals and governance and management objectives (Appendix C). Use the mapping to determine the most important governance and management objectives.

This substep identifies a number of governance and management objectives that have higher importance for the enterprise, based on the prioritized enterprise goals.

Note: This technique is purely mechanical, using mapping tables that are generic in nature. The enterprise must interpret the results with care, or adapt the mapping tables based on its own experience and context. In the workflow described in this guide, this fine-tuning is done in Step 4 *Conclude the governance system design*.

Examples of goals cascade application are included in the toolkit companion to this *COBIT® 2019 Design Guide*.[16]

4.3.4 Consider the Risk Profile of the Enterprise (Design Factor 3)

In Step 1 (see Section 4.2.3 Understand the Risk Profile), the enterprise performed a high-level risk analysis to identify risk categories exceeding the enterprise's risk appetite. Here, the results of the risk analysis are translated into priorities for governance and management objectives. The most common risk response used in risk management is risk mitigation, which requires a number of controls (in risk language) to be implemented, or (in the language of COBIT), governance and management objectives that need to be achieved. Appendix D contains a mapping between the 19 IT risk categories in COBIT® 2019 and the governance and management objectives, expressing the extent to which each governance and management objective can be considered as a control for each risk scenario.

The mapping table in Appendix D relates the risk profile of the enterprise to governance and management objectives and their priorities, using the same technique and scoring method described earlier.

Example: Appendix D illustrates that if IT risk scenario category 1 (RISKCAT01) *IT investment decision making, portfolio definition & maintenance* is a concern, then the following governance and management objectives will be important:

- EDM01, EDM02, EDM04, EDM05
- APO05

4.3.5 Consider Current I&T-Related Issues of the Enterprise (Design Factor 4)

In Step 1 (see Section 4.2.4 Understand Current I&T-Related Issues), the enterprise performed a high-level diagnostic on the I&T-related issues it experiences. Here, the results of this diagnostic are translated into priorities for governance and management objectives.

Appendix E contains a mapping table between I&T issues and COBIT® 2019 governance and management objectives. As Appendix E shows, each I&T-related issue is associated to one or more governance or management objective that can influence the I&T-related issue. The same techniques and scoring mechanisms described earlier can be used.

Example: When the I&T-related issue, "IT-enabled changes or projects frequently failing to meet business needs and delivered late or over budget," is of concern, the following governance and management objectives are important:

- APO03
- BAI01, BAI02, BAI03, BAI05, BAI11

4.3.6 Conclusion

At the end of Step 2, all elements are available to define the initial scope of a customized governance system:

- **Prioritized governance and management objectives** indicate which governance and management objectives should be the focus.
- **Guidance on specific governance components** can potentially also be included in the initial design.

[16] The companion toolkit can be downloaded at *www.isaca.org/COBIT/Pages/COBIT-2019-Design-Guide.aspx*.

The enterprise can choose to elaborate the current initial design and resolve all differences among the various inputs; or, the enterprise can wait until Step 4 of the workflow and combine the different inputs with the scope refinements identified in Step 3.

4.4 Step 3: Refine the Scope of the Governance System

Step 3 identifies refinements to the initial scope of the governance system, based on the remaining set of design factors as defined in Section 2.6. Throughout this chapter, not all design factors may be applicable to each enterprise. Those not applicable can be ignored.

In this step, the governance system designer will:

1. Walk through each design factor (DF) from DF5 *Threat landscape* through DF11 *Enterprise size*.
2. Determine whether or not each design factor is applicable.
3. For applicable design factors, determine which of the potential values—or which combination of potential values—is most applicable to the enterprise. Reference descriptions of the applicable design factor values, along with the mapping tables in Appendices F through K, to determine which refinements to the governance system are associated with these values.

The result of each consideration of a design factor is a ranked list of governance and management objectives, similar to the result from Step 2. Using the mapping tables in Appendices F through K, the same techniques and scales can be used as described earlier.

4.4.1 Consider the Threat Landscape (Design Factor 5)

The following steps should be performed when considering this design factor:

- Decide which combination of values best fits the current situation of the enterprise, as per the defined entries in **figure 4.3**.
- Consider the listed guidance for governance and management objectives, components and focus areas, and include the pertinent information on the design canvas for resolution and conclusion in Step 4.

Figure 4.3—Governance and Management Objectives Priority Mapped to Threat Landscape Design Factor

Design Factor Value	Governance and Management Objectives Priority	Components	Focus Area Variants
High	Important governance and management objectives include: • EDM01, EDM03 • APO01, APO03, APO10, APO12, APO13, APO14 • BAI06, BAI10 • DSS02, DSS04, DSS05, DSS06 • MEA01, MEA03, MEA04	Important organizational structures include: • Security strategy committee • Chief information security officer (CISO) Important culture and behavior aspects include: • Security awareness Information flows include: • Security policy • Security strategy	Information security focus area[17]
Normal	• *As per the initial scope definition*	• *N/A*	COBIT core model

[17] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, the information security focus area content was in development, and not yet released.

4.4.2 Consider Compliance Requirements (Design Factor 6)

The following steps should be performed when considering this design factor:

- Decide which combination of values best fits the current situation of the enterprise, as per the defined entries in **figure 4.4**.
- Consider the listed guidance for governance and management objectives, components and focus areas, and include the pertinent information on the design canvas for resolution and conclusion in Step 4.

Figure 4.4—Governance and Management Objectives Priority Mapped to Compliance Requirements Design Factor

Design Factor Value	Governance and Management Objectives Priority	Components	Focus Area Variants
High	Important governance and management objectives include: • EDM01, EDM03 • APO12 • MEA03, MEA04	Importance of compliance function: • High relevance of documentation (information items) and policies and procedures	COBIT core model
Normal	• *As per the initial scope definition*	• *N/A*	COBIT core model
Low	• *As per the initial scope definition*	• *N/A*	COBIT core model

4.4.3 Consider the Role of IT (Design Factor 7)

The following steps should be performed when considering this design factor:

- Decide which combination of values best fits the current situation of the enterprise, as per the defined entries in **figure 4.5**.
- Consider the listed guidance for governance and management objectives, components and focus areas, and include the pertinent information on the design canvas for resolution and conclusion in Step 4.

Figure 4.5—Governance and Management Objectives Priority Mapped to Role of IT Design Factor

Design Factor Value	Governance and Management Objectives Priority	Components	Focus Area Variants
Support	• *As per the initial scope definition*	• *N/A*	COBIT core model
Factory	Important governance and management objectives include: • EDM03 • DSS01, DSS02, DSS03, DSS04	• *N/A*	Information security focus area[18]
Turnaround	Important governance and management objectives include: • APO02, APO04 • BAI02, BAI03	• *N/A*	DevOps focus area[19]

[18] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, the information security focus area content was in development and not yet released.
[19] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, the DevOps focus area content was in development and not yet released.

Figure 4.5—Governance and Management Objectives Priority Mapped to Role of IT Design Factor *(cont.)*			
Design Factor Value	**Governance and Management Objectives Priority**	**Components**	**Focus Area Variants**

Strategic	Important governance and management objectives include:
	• EDM01, EDM02, EDM03
	• APO02, APO04, APO05, APO12, APO13
	• BAI02, BAI03
	• DSS01, DSS02, DSS03, DSS04, DSS05
		Typical bimodal components include:
		• Organizational structures
		  ■ Chief digital officer
		• Skills and competencies
		  ■ Staff who can work in an ambidextrous environment that combines both exploration and exploitation
		• Processes
		  ■ A portfolio and innovation process that integrates exploration and exploitation of digital transformation opportunities
			Digital transformation focus area[20]

4.4.4 Consider the Sourcing Model for IT (Design Factor 8)

The following steps should be performed when considering this design factor:

- Decide which combination of values best fits the current situation of the enterprise, as per the defined entries in **figure 4.6**.
- Consider the listed guidance for governance and management objectives, components and focus areas, and include the pertinent information on the design canvas for resolution and conclusion in Step 4.

Figure 4.6—Governance and Management Objectives Priority Mapped to Sourcing Model for IT Design Factor			
Design Factor Value	**Governance and Management Objectives Priority**	**Components**	**Focus Area Variants**
Outsourcing	Important management objectives include: • APO09, APO10 • MEA01	• *N/A*	Vendor management focus area[21]
Cloud	Important management objectives include: • APO09, APO10 • MEA01	• *N/A*	Cloud focus area[22]
Insourced	• *As per the initial scope definition*	• *N/A*	COBIT core model
Hybrid	*Combination of guidance for the three specific options*		

4.4.5 Consider IT Implementation Methods (Design Factor 9)

The following steps should be performed when considering this design factor:

- Decide which combination of values best fits the current situation of the enterprise, as per the defined entries in **figure 4.7**.

[20] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, the digital transformation focus area content was being contemplated as a potential future focus area.
[21] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, the vendor management focus area was being contemplated as a potential future focus area.
[22] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, the cloud focus area was being contemplated as a potential future focus area.

- Consider the listed guidance for governance and management objectives, components and focus areas, and include the pertinent information on the design canvas for resolution and conclusion in Step 4.

Figure 4.7—Governance and Management Objectives Priority Mapped to IT Implementation Methods Design Factor

Design Factor Value	Governance and Management Objectives Priority	Components	Focus Area Variants
Agile	Important management objectives include: • BAI02, BAI03, BAI06	• Important and specific roles as identified in the Agile focus area guidance	Agile focus area[23]
DevOps	Important management objectives include: • BAI03	• Important and specific roles as identified in the DevOps focus area guidance	DevOps focus area[24]
Traditional	• *As per the initial scope definition*	• *N/A*	COBIT core model
Hybrid	*Combination of guidance for the three specific options*		

4.4.6 Consider the Technology Adoption Strategy (Design Factor 10)

The following steps should be performed when considering this design factor:

- Decide which combination of values best fits the current situation of the enterprise, as per the defined entries in **figure 4.8**.
- Consider the listed guidance for governance and management objectives, components and focus areas, and include the pertinent information on the design canvas for resolution and conclusion in Step 4.

Figure 4.8—Governance and Management Objectives Priority Mapped to Technology Adoption Strategy Design Factor

Design Factor Value	Governance and Management Objectives Priority	Components	Focus Area Variants
First Mover	Important governance and management objectives include: • EDM01, EDM02 • APO02, APO04, APO05, APO08 • BAI01, BAI02, BAI03, BAI05, BAI07, BAI11 • MEA01	• *N/A*	DevOps focus area[24] Digital transformation focus area[25]
Follower	Important governance and management objectives include: • APO02, APO04 • BAI01	• *N/A*	COBIT core model
Slow Adopter	• *As per the initial scope definition*	• *N/A*	COBIT core model

[23] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, the Agile focus area was being contemplated as a potential future focus area.
[24] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, the DevOps focus area content was in development and not yet released.
[25] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, the digital transformation focus area content was being contemplated as a potential future focus area.

4.4.7 Consider Enterprise Size (Design Factor 11)

The following steps should be performed when considering this design factor:

- Decide which combination of values best fits the current situation of the enterprise, as per the defined entries in **figure 4.9**.
- Consider the listed guidance for governance and management objectives, components and focus areas, and include the pertinent information on the design canvas for resolution and conclusion in Step 4.

Figure 4.9—Governance and Management Objectives Priority Mapped to Enterprise Size Design Factor

Design Factor Value	Governance and Management Objectives Priority	Components	Focus Area Variants
Large	• *As per the initial scope definition*	• *N/A*	COBIT core model
Small/Medium	• *As per the initial scope definition*	• *As applicable in the SME focus area description*	SME focus area[26]

Example: If the enterprise is an SME (e.g., it has 250 or fewer full-time employees [FTEs]), it should use the guidance contained in the SME focus area for the design of its governance system.

4.4.8 Conclusion

At the end of Step 3, the enterprise will have identified a series of potential refinements for the initial governance system and put them all on the canvas for consolidation during Step 4 of the design workflow.

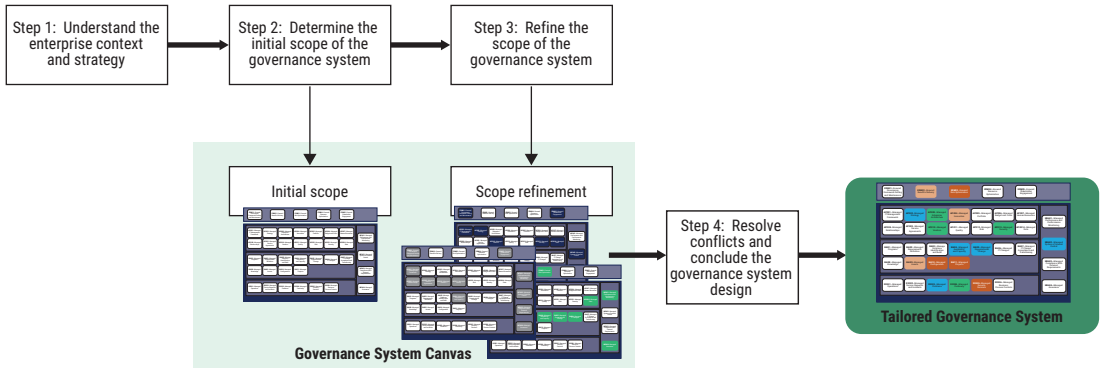
The following refinements are typically expressed similar to outcome from Step 2: prioritized governance and management objectives, important components for the governance system, and specific focus area guidance.

4.5 Step 4: Resolve Conflicts and Conclude the Governance System Design

As the last step in the design process, Step 4 brings together all inputs from previous steps to conclude the governance system design, as depicted in **figure 4.10**. The resulting governance system must reflect careful consideration of all inputs—understanding that these inputs may sometimes conflict.

[26] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution,* the small and medium enterprise focus area content was in development and not yet released.

Figure 4.10—Governance System Design Step 4—Conclusion



4.5.1 Resolve Inherent Priority Conflicts

Step 4 involves reconciling any conflicts in order to finalize the design.

4.5.1.1 Purpose

The following outputs from previous steps will be considered before any conclusion is made:

- Initial design of the governance system, as obtained during Step 2, based on the enterprise strategy, enterprise goals, risk profile and I&T-related issues. This initial design probably reflects some diverging sets of prioritized management objectives.
- Scope refinements obtained in Step 3 through the analysis of remaining design factors and diverging sets of priorities.

4.5.1.2 Resolution Strategies

The workflow described in this guide can be applied to different situations, requiring different strategies for coming to a conclusion. In short, the enterprise needs to analyze the data and results after applying design factors in the context of its goals for implementing a governance program.

Example: If the enterprise has ***one important, ongoing initiative*** (e.g., a major investment in an enterprise application, digital transformation program, etc.) or wants to focus on ***a very specific topic or issue*** (e.g., solving an important security problem, adopting a DevOps approach, aligning to and complying with new privacy regulations, etc.), the enterprise need not apply all steps in the proposed workflow in full detail, but rather, may focus on specific areas of interest.

- In case of an important development investment, the enterprise can consider its enterprise strategy (design factor 1) as an innovation/differentiation strategy, and consequently decide to work only on the governance and management objectives that are emphasized for this design factor.
- In case of new privacy regulations, an enterprise can focus on governance and management objectives that correspond to high compliance requirements (design factor 6). Those objectives are EDM01 *Ensured governance framework setting and maintenance*, EDM03 *Ensured risk optimization*, APO12 *Managed risk*, MEA03 *Managed compliance with external requirements* and MEA04 *Managed assurance*. In addition, the enterprise will need to focus on governance and management objectives that come out of the compliance requirements analysis contained in MEA03.

Example: If the enterprise requires ***a broad, holistic and comprehensive view*** of its governance system, it is recommended that the enterprise apply the full workflow as described in this guide and carefully consider all design factors.

When defining the design of a governance system, the enterprise should review its governance and management objectives, and analyze its current performance level(s) (i.e., capability levels for processes). The enterprise should then take the results of these assessments into account when defining the road map toward the target governance system, looking first of all for quick wins (i.e., those initiatives entailing limited effort, but yielding high benefit).

4.5.1.3 Resolution Approach

There are no universally applicable guidelines for resolving competing or conflicting priorities, valid across all enterprise contexts. However, a few recommendations to approach this are:

- Include all key stakeholders in the discussion on the design of the governance system: board and executive management, business executives, management of the IT function, and risk and assurance management.
- Consider the generic nature of COBIT guidance and the mapping tables, which cannot take into account all specificities of every enterprise. The enterprise can and should be prepared to deviate from some of the identified priorities if it feels there are justified reasons for such deviation.
- Likewise, note that the specific context of the enterprise may well require deviating from the kind of strictly quantitative priorities for governance and management objectives that are generated by generic, preprogrammed computations (e.g., results from mathematical matrix calculations).

4.5.2 Conclude the Governance System Design

4.5.2.1 Concluding the Design

The conclusion of the design phase must result in one design for the governance system for enterprise I&T. This design will include:

- Prioritized governance and management objectives, whereby the:
  - Number of high-priority objectives is kept to a reasonable level.
  - Target capability levels (or equivalent performance requirements for nonprocesses) are defined, with higher target capability levels for the most critical objectives, and lower target capability levels for less critical objectives.
- A variety of target capability levels for processes (or equivalent performance targets for other components). When defining those targets, it is not recommended to aim for the highest rating, because:
  - For some processes or other components, a level five (5) capability is not possible or defined.
  - Very rarely is it cost-effective or justifiable to operate a governance system at this high capability level across all objectives.
  - Many organizations will find it nearly impossible to implement the road map toward such a high capability level governance system within any sort of reasonable time frame.
- A governance component requiring specific attention due to a particular issue or circumstance (e.g., if privacy is of utmost concern to an enterprise, privacy policies and procedures may need extra attention)
- Focus area guidance complementing the core COBIT guidance (when available, necessary and appropriate)

Examples of such a design are included in Chapter 7.

4.5.2.2 Sustaining the Governance System

The result of the last step in the governance design workflow is a well-designed governance system. A governance system, however, is inherently dynamic. Strategies can change, important investment programs are launched, threat landscapes change, technologies change, etc. This means that the governance system should be reviewed on a regular basis, and changes to the system should be made whenever necessary.

This dynamic nature of any governance system also informs the *COBIT® 2019 Implementation Guide*, which outlines a continuous improvement cycle (see also Chapter 5 of this publication).

Chapter 5
Connecting With the *COBIT® 2019 Implementation Guide*

5.1 Purpose of the *COBIT® 2019 Implementation Guide*

The *COBIT® 2019 Implementation Guide* emphasizes an enterprisewide view of governance of I&T, recognizing 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.

When governance system implementations fail, one of the common reasons is that they are not initiated and then managed properly as programs, to ensure that benefits are realized. Governance programs must be sponsored by executive management and properly scoped, and should always define objectives that are attainable. These provisions enable the enterprise to absorb the pace of change as planned. Program management is, therefore, addressed as an integral part of the implementation life cycle.

While a program and project approach is recommended to drive improvement initiatives effectively, the overarching goal is to establish a normal business practice and a sustainable approach to governing and managing enterprise I&T (as with any other aspect of enterprise governance). For this reason, the implementation approach is based on empowering business and IT stakeholders to take ownership of I&T-related governance and management decisions and activities by facilitating and enabling change.

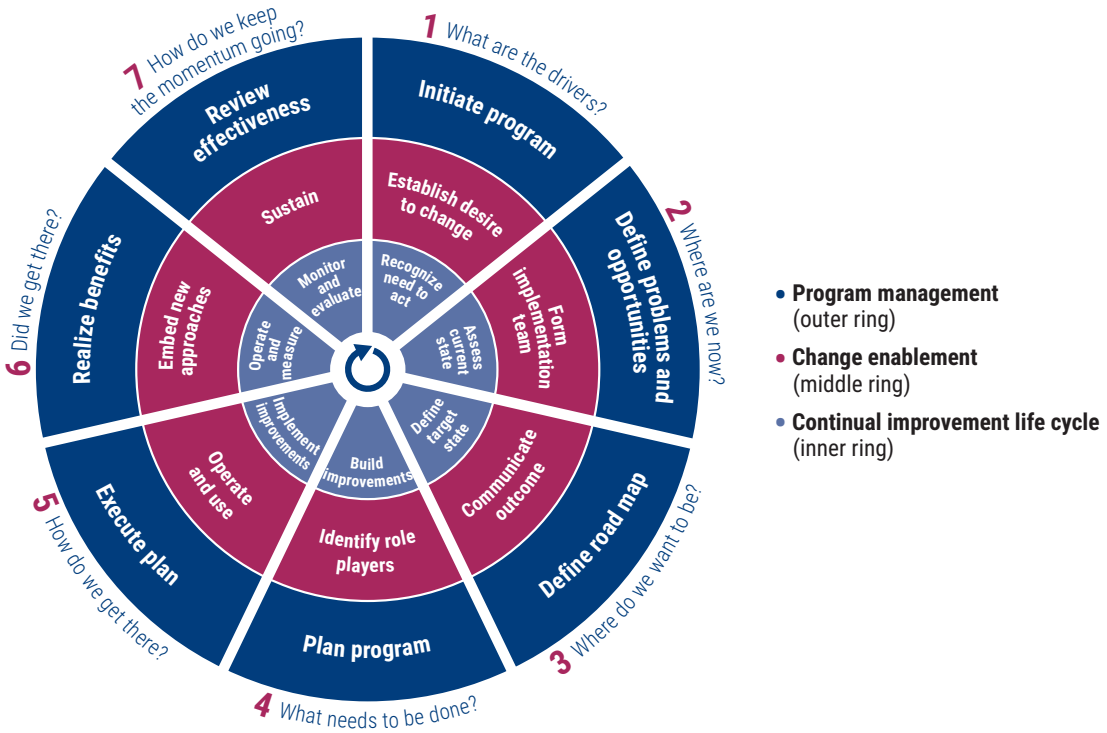
The implementation program closes when the process for focusing on IT-related priorities and governance improvement generates a measurable benefit, and the results of the program have become embedded in ongoing business activity.

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

5.2 COBIT Implementation Approach

The COBIT implementation approach is summarized in **Figure 5.1**.

Figure 5.1—COBIT Implementation Roadmap



5.2.1 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.

5.2.2 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.

5.2.3 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.

5.2.4 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.

5.2.5 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.

5.2.6 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.

5.2.7 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.

5.3 Relationship Between *COBIT Design Guide* and *COBIT Implementation Guide*

The *COBIT® 2019 Design Guide* elaborates on a set of tasks defined in the *COBIT® 2019 Implementation Guide*. **Figure 5.2** describes the connection points between both Guides, and the purpose of this table is that users of the *COBIT® 2019 Implementation Guide* find appropriate additional and more detailed guidance for certain phases and activities in the *COBIT® 2019 Design Guide.*

Figure 5.2—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.**	
1	Identify the current governance context, business IT and IT pain points, events, and symptoms triggering the need to act.	**1.4**	Understand current I&T-related issues.
2	Identify the business and governance drivers and compliance requirements for improving the enterprise governance of I&T (EGIT) and assess current stakeholder needs.	**1.1** **1.2** **1.3**	Understand enterprise strategy. Understand enterprise goals. Understand the risk profile.
3	Identify business priorities and business strategy dependent on IT, including any current significant projects.	**1.1** **1.2** **1.3**	Understand enterprise strategy. Understand enterprise goals. Understand the risk profile.
4	Align with enterprise policies, strategies, guiding principles and any ongoing governance initiatives.	Not exclusively governance design steps, these tasks are more related to change enablement (CE) tasks in the *COBIT Implementation Guide* and are adequately covered there.	
5	Raise executive awareness of IT's importance to the enterprise and the value of EGIT.		
6	Define EGIT policy, objectives, guiding principles and high-level improvement targets.		
7	Ensure that the executives and board understand and approve the high-level approach, and accept the risk of not taking any action on significant issues.		
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.**	
1	Identify key enterprise and supporting IT-related goals.	**2.1** **2.2**	Consider enterprise strategy. Consider enterprise goals and apply the COBIT goals cascade.
2	Establish the significance and nature of IT's contribution (solutions and services) required to support business objectives.	**2.2** **3.3** **3.4** **3.5** **3.6** **3.7**	Consider enterprise goals and apply the COBIT goals cascade. Consider the role of IT. Consider the sourcing model. Consider IT implementation methods. Consider the technology adoption strategy. Consider enterprise size.
3	Identify key governance issues and weaknesses related to the current and required future solutions and services, the enterprise architecture needed to support the IT-related goals, and any constraints or limitations.	**2.4**	Consider current I&T-related issues.
4	Identify and select the processes critical to support IT-related goals and, if appropriate, key management practices for each selected process.	**2.1** **2.2**	Consider enterprise strategy. Consider enterprise goals and apply the COBIT goals cascade.
5	Assess benefit/value enablement risk, program/project delivery risk and service delivery/IT operations risk related to critical IT processes.	**2.3**	Consider the risk profile of the enterprise.
6	Identify and select IT processes critical to ensure that risk is avoided.	**2.3**	Consider the risk profile of the enterprise.
7	Understand the risk acceptance position as defined by management.	**1.3** **2.3**	Understand the risk profile. Consider the risk profile of the enterprise.

Figure 5.2—Connection Points Between *COBIT Design Guide* and *COBIT Implementation Guide* (cont.)

COBIT Implementation Guide		COBIT Design Guide	
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.**	
8	Define the method for executing the assessment.	The assessment method for processes is the method described in the *COBIT® 2019 Framework: Introduction and Methodology* publication (based on CMMI capability levels).	
9	Document understanding of how the current process actually addresses the management practices selected earlier.	**2.1** **2.2** **2.3** **2.4** **3.1** **3.2** **3.3** **3.4** **3.5** **3.6** **3.7**	Consider enterprise strategy. Consider enterprise goals and apply the COBIT goals cascade. Consider the risk profile of the enterprise. Consider current I&T-related issues. Consider the threat landscape. Consider compliance requirements. Consider the role of IT. Consider the sourcing model. Consider IT implementation methods. Consider the technology adoption strategy. Consider enterprise size.
10	Analyze the current level of capability.	**4.1** **4.2**	Resolve inherent priority conflicts. Conclude the governance system design.
11	Define the current process capability rating.	**4.1** **4.2**	Resolve inherent priority conflicts. Conclude the governance system design.
Phase 3—Where do we want to be? (CI tasks)		**Step 4—Conclude the governance system design.**	
1	Define targets for improvement: • Based on enterprise requirements for performance and conformance, decide the initial ideal short- and long-term target capability levels for each process. • To the extent possible, benchmark internally to identify better practices that can be adopted. • To the extent possible, benchmark externally with competitors and peers to help decide the appropriateness of the chosen target level. • Do a "sanity check" of the reasonableness of the targeted level (individually and as a whole), looking at what is achievable and desirable and can have the greatest positive impact within the chosen time frame.	**4.1** **4.2**	Resolve inherent priority conflicts. Conclude the governance system design.
2	Analyze gaps: • Use understanding of current capability (by attribute) and compare it to the target capability level. • Leverage existing strengths wherever possible to deal with gaps and seek guidance from COBIT management practices and activities and other specific good practices and standards such as ITIL, International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27000, The Open Group Architectural Framework (TOGAF®) and the Project Management Body of Knowledge (PMBOK®), to close other gaps. • Look for patterns that indicate root causes to be addressed.	**4.1** **4.2**	Resolve inherent priority conflicts. Conclude the governance system design.
3	Identify potential improvements: • Collate gaps into potential improvements. • Identify unmitigated residual risk and ensure formal acceptance.		

Page intentionally left blank

Part II
Execution and Examples

Chapter 6
The Governance System Design Toolkit

6.1 Introduction

This chapter introduces the *COBIT Design Guide* companion toolkit, an Excel® spreadsheet-based tool that facilitates the application of the governance system design workflow explained in Chapter 4.

The toolkit was used to illustrate the three examples outlined in Chapter 7 of this publication. This introduction should help readers obtain a basic understanding of the toolkit, and appreciate how the results were generated for examples in Chapter 7. The toolkit as downloaded shows the values illustrated in this chapter. To use the tool, change the values to fit the enterprise context.

Note: Many methods exist to quantify and rank priorities for governance and management objectives. In this publication and its accompanying toolkit, one method was selected, but that does not exclude other valuable methods that are capable of delivering reliable results.

6.2 Toolkit Basics

The toolkit consists of an Excel spreadsheet. The spreadsheet contains:

- An introduction and instructions tab that provides basic information about how to use the toolkit
- A canvas tab that consolidates all results of the governance system design workflow
- One tab for each design factor (DF), where:
  - Values can be entered and graphically represented
  - Priority scores for governance and management objectives are calculated and presented in table format and graphically in two diagrams
- Two summary tabs (one after Step 2 and another after Step 3 of the governance system design workflow) that graphically represent the outcomes of each completed step
- Mapping tables for design factors that have input values used by other tabs (these tables are hidden to increase the readability of the spreadsheet)
  - Mapping tables (with the exception of Design Factor 2 *Enterprise goals*) contain values between zero (0) and four (4), indicating the relevance of each governance/management objective for each respective value of the design factor, risk scenario or I&T-related issue.
    - A value of 4 means maximal relevance, while a value of 0 means no relevance.
    - Values reflect averages that were established by an expert panel. The values cannot, and do not, model every given individual situation, and should therefore be used with caution. They can, however, give good, representative indications, and can be considered as directional guidance.
  - The mapping table for Design Factor 2 *Enterprise goals* is slightly different, in that it contains two mapping tables. One table maps from enterprise goals to alignment goals, and the other table maps from alignment goals to governance and management objectives (see Appendices B and C).

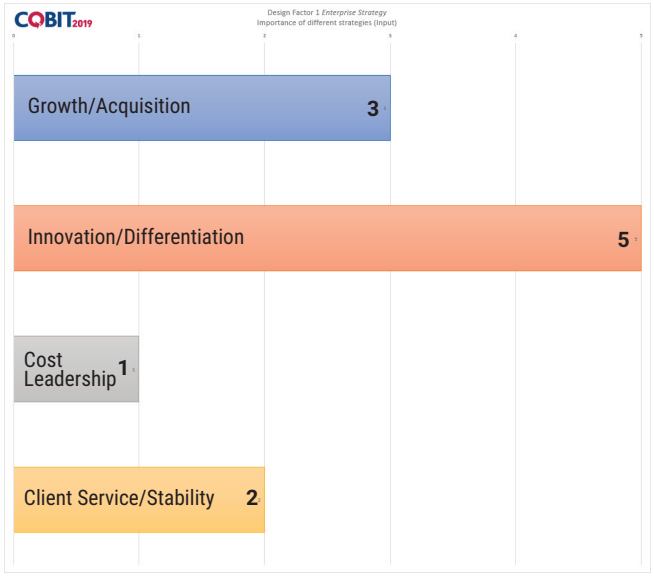
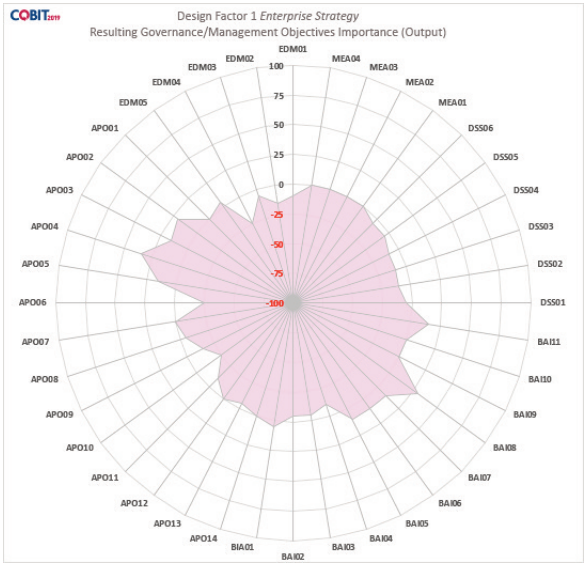
6.3 Step 1 and Step 2: Determine the Initial Scope of the Governance System

In these steps of the governance design workflow, the strategy, goals, risk profile and I&T-related issues of the enterprise are assessed. The steps assess the first four design factors (as defined in Chapter 4) to determine their impact on the initial design of a governance system:

1. Enterprise strategy
2. Enterprise goals (via the goals cascade)
3. IT risk profile
4. I&T-related issues

6.3.1 Enterprise Strategy (Design Factor 1)

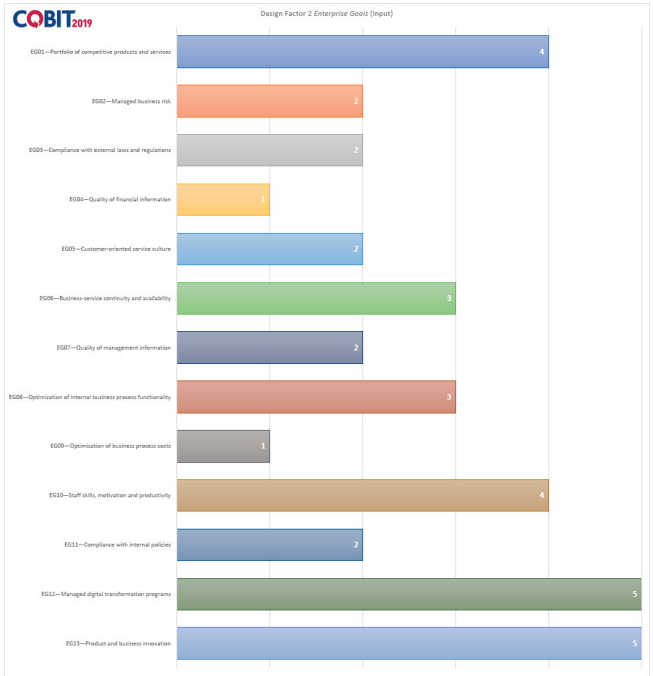
Input	• Each of the four possible values for the enterprise strategy design factor—growth/acquisition, innovation/differentiation, cost leadership, client services/stability—must be rated between 1 (not important) and 5 (most important). • It is recommended to maintain sufficient spread between values.
Calculation	• The toolkit performs a matrix calculation of the entered values for Design Factor 1 *Enterprise strategy* with the mapping table for design factor 1, resulting in a score for each governance/management objective. • The toolkit performs a second matrix calculation of a baseline set of values for design factor 1 with the mapping table for design factor 1, resulting in a baseline score for each governance/management objective. • The toolkit then calculates a relative importance for each governance/management objective as the relative difference between both sets of values, expressed as a percentage and rounded to 5. This number can be positive or negative, indicating that a governance/management objective is more or less important when compared to the baseline score.
Output	• The output section of this tab contains the calculated relative importance of each of the 40 COBIT® 2019 governance and management objectives. • The results are represented in table format, as a bar chart and as a spider diagram.

Sample Input Graph	Sample Output Graph
	

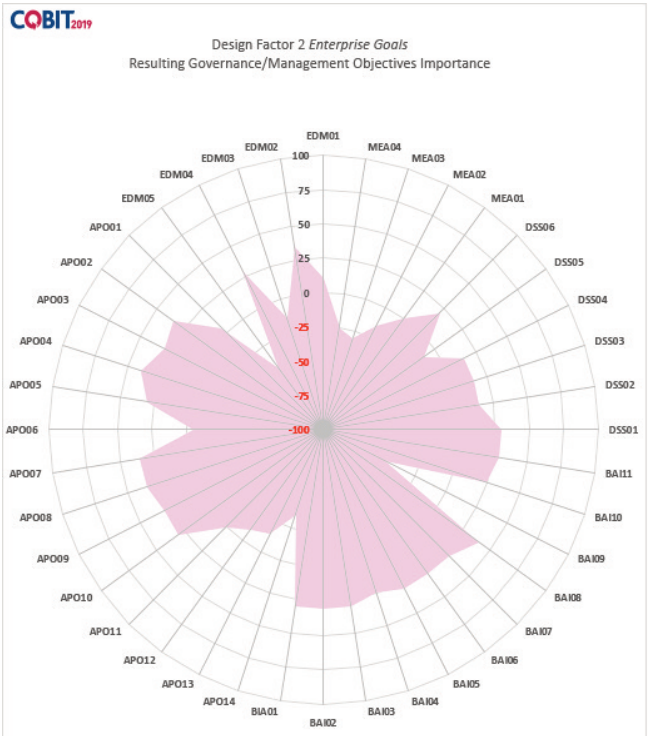
6.3.2 Enterprise Goals and Applying the COBIT Goals Cascade (Design Factor 2)

Input	• Each of the thirteen enterprise goals must be rated between 1 (not important) and 5 (most important). • Using the generic enterprise goals, determine the most important goals for the enterprise. It is advisable to select the top three to five most important enterprise goals; too many high-priority goals will lead to less meaningful goals cascade results. • It is recommended to maintain sufficient spread between values.
Calculation	• The tool performs a double matrix calculation between (1) the rated enterprise goals and the mapping table between enterprise goals and IT alignment goals, and (2) the result of the first matrix calculation and the mapping table between IT alignment goals and governance/management objectives. • The tool performs a second set of matrix calculations of a baseline set of values for Design Factor 2 *Enterprise goals*, resulting in a baseline score for each governance/management objective. • The tool then calculates the relative importance for each governance/management objective as the relative difference between both sets of values, expressed as a percentage and rounded to 5. This number can be positive or negative, indicating that a governance/management objective is more or less important when compared to the baseline score.
Output	• The output section of this sheet contains the calculated relative importance of each of the 40 COBIT® 2019 governance and management objectives. • The results are represented in table format, as a bar chart and as a spider diagram.

Sample Input Graph



Sample Output Graph



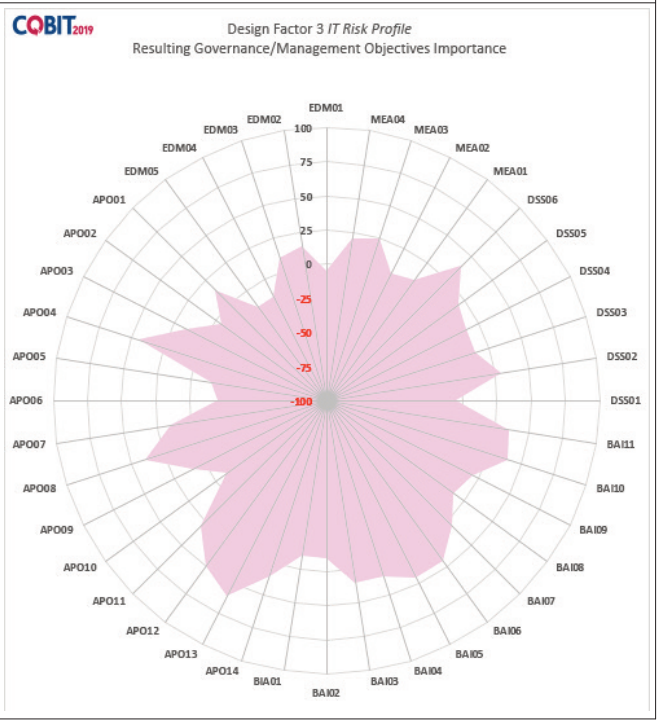
6.3.3 Risk Profile of the Enterprise (Design Factor 3)

Input	• Each of the 19 risk categories contained in the risk profile design factor must be rated as follows:
	  ▪ Impact of the risk should it occur, as a value between 1 (not important) and 5 (critical)
	  ▪ Likelihood of the risk to occur, as a value between 1 (very unlikely) and 5 (very likely)
	• The tool assigns a risk rating (very high, high, normal, low) to each risk category, based on the combination of the impact and likelihood ratings.
	• It is recommended to maintain sufficient spread between values.

Calculation	• The tool performs a matrix calculation of the risk ratings with the mapping table for Design Factor 3 *Risk profile*, resulting in a score for each governance/management objective. • The tool performs a second matrix calculation of a baseline set of risk ratings for design factor 3 with the mapping table for design factor 3, resulting in a baseline score for each governance/management objective. • The tool then calculates a relative importance for each governance/management objective as the relative difference between both sets of values, expressed as a percentage and rounded to 5. This number can be positive or negative, indicating that a governance/management objective is more or less important when compared to the baseline score.
Output	• The output section of this tool contains the calculated relative importance of each of the 40 COBIT® 2019 governance and management objectives. • The results are represented in table format, as a bar chart and as a spider diagram.

Risk Scenario Category	Impact (1-5)	Likelihood (1-5)	Risk Rating	Baseline
IT investment decision making, portfolio definition & maintenance	2	2		9
Program & projects life cycle management	4	3		9
IT cost & oversight	2	2		9
IT expertise, skills & behavior	4	4		9
Enterprise/IT architecture	2	2		9
IT operational infrastructure incidents	3	2		9
Unauthorized actions	3	4		9
Software adoption/usage problems	4	3		9
Hardware incidents	2	2		9
Software failures	3	3		9
Logical attacks (hacking, malware, etc.)	4	5		9
Third-party/supplier incidents	2	2		9
Noncompliance	3	3		9
Geopolitical Issues	2	2		9
Industrial action	1	3		9
Acts of nature	3	3		9
Technology-based innovation	5	3		9
Environmental	2	3		9
Data & information management	4	4		9

	Very High Risk
	High Risk
	Normal Risk
	Low Risk



6.3.4 Current I&T-Related Issues of the Enterprise (Design Factor 4)

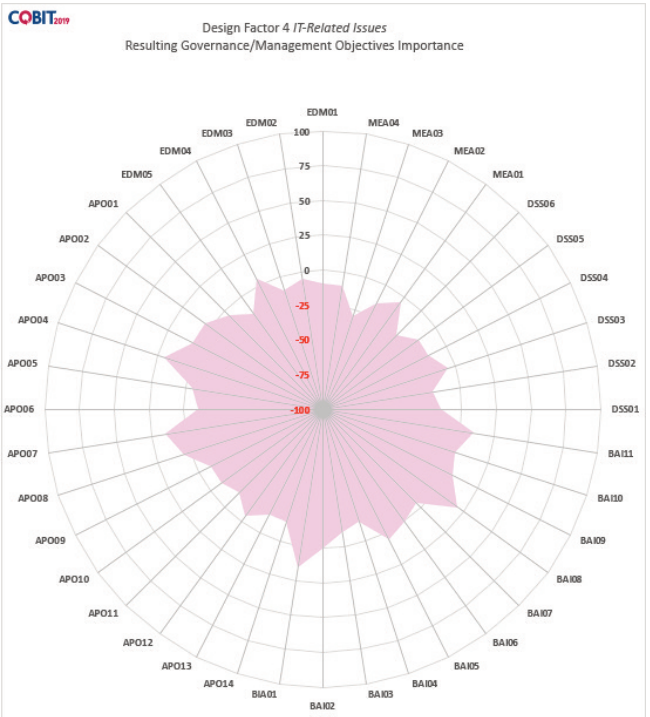
Input	• Each of the 20 I&T-related issues for the I&T-related issues design factor must be rated between 1 (no issue) and 3 (serious issue). Numbers 1, 2 or 3 should be keyed into the tool; the tool will then automatically translate values into a symbol, based on the tool's key for this rating. • It is recommended to maintain sufficient spread between values.
Calculation	• The tool performs a matrix calculation of the entered values for Design Factor 4 *I&T-Related Issues* with the mapping table for design factor 4, resulting in a score for each governance/management objective. • The tool performs a second matrix calculation of a baseline set of values for design factor 4 with the mapping table for design factor 4, resulting in a baseline score for each governance/management objective. • The tool then calculates a relative importance for each governance/management objective as the relative difference between both sets of values, expressed as a percentage and rounded to 5. This number can be positive or negative, indicating that a governance/management objective is more or less important when compared to the baseline score.
Output	• The output section of this tab contains the calculated relative importance of each of the 40 COBIT® 2019 governance and management objectives.

Sample Input Table

IT-Related Issue	Importance (1-3)	Baseline
Frustration between different IT entities across the organization because of a perception of low contribution to business value	✓	2
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	✓	2
Significant IT-related incidents, such as data loss, security breaches, project failure and application errors, linked to IT	!	2
Service delivery problems by the IT outsourcer(s)	!	2
Failures to meet IT-related regulatory or contractual requirements	✓	2
Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems	✓	2
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	!	2
Duplications or overlaps between various initiatives, or other forms of wasted resources	✗	2
Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction	✗	2
IT-enabled changes or projects frequently failing to meet business needs and delivered late or over budget	!	2
Reluctance by board members, executives or senior management to engage with IT, or a lack of committed business sponsorship for IT	!	2
Complex IT operating model and/or unclear decision mechanisms for IT-related decisions	!	2
Excessively high cost of IT	✓	2
Obstructed or failed implementation of new initiatives or innovations caused by the current IT architecture and systems	✗	2
Gap between business and technical knowledge, which leads to business users and information and/or technology specialists speaking different languages	✗	2
Regular issues with data quality and integration of data across various sources	✓	2
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	✓	2
Business departments implementing their own information solutions with little or no involvement of the enterprise IT department (related to end-user computing, which often stems from dissatisfaction with IT solutions and services)	!	2
Ignorance of and/or noncompliance with privacy regulations	✓	2
Inability to exploit new technologies or innovate using I&T	✗	2

✓	No Issue
!	Issue
✗	Serious Issue

Sample Output Graph

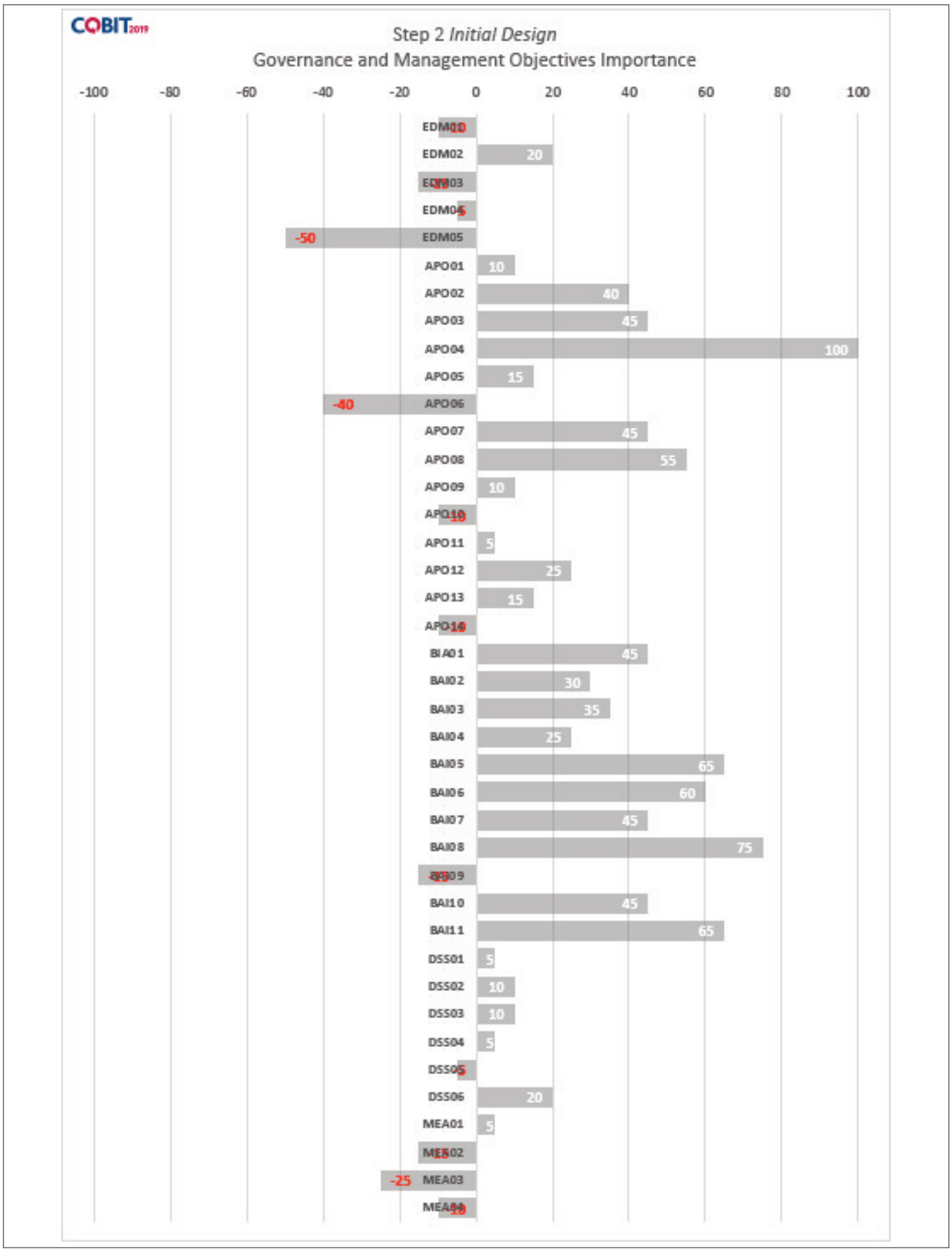


6.3.5 Conclusion

Input	• N/A

Calculation	• The tool performs a weighted summation of the calculated governance/management objectives importance scores related to the first four design factors.
	• Weights can be entered on the canvas tab and are set to 1 by default. The weighting can be changed, if, for example, the enterprise strategy is of greater importance than enterprise goals, risk or I&T-related issues.
	• The achieved results are then normalized on a scale of 100 (both positive and negative) and reflected on the Step 2 summary tab.
	  ▪ The highest value (positive or negative) obtains a score of 100.
	  ▪ All other values are then prorated against this value.
	• The resulting list of scores not only provides a reliable view of the relative importance of all governance/management objectives against each other, but also gives an indication of the absolute importance. This output allows an enterprise not only to prioritize governance/management objectives against each other, but also to define adequate target capability levels.

Output	• The Step 2 summary tab contains the calculated relative importance of each of the 40 COBIT® 2019 governance and management objectives. • The results are represented in table format (on the canvas tab), and as a bar chart (Step 2 summary tab)


COBIT 2019
Step 2 Initial Design
Governance and Management Objectives Importance
-100
-80
-60
-40
-20
0
20
40
60
80
100
EDM01
EDM02
20
EDM03
EDM04
5
-50
EDM05
APO01
10
APO02
40
APO03
45
APO04
100
APO05
15
-40
APO06
APO07
45
APO08
55
APO09
10
APO10
APO11
5
APO12
25
APO13
15
APO14
BAI01
45
BAI02
30
BAI03
35
BAI04
25
BAI05
65
BAI06
60
BAI07
45
BAI08
75
BAI09
BAI10
45
BAI11
65
DSS01
5
DSS02
10
DSS03
10
DSS04
5
DSS05
DSS06
20
MEA01
5
MEA02
-25
MEA03
MEA04

Note: The preceding sample graph is consistent with sample graphs for each design factor, in that it represents the actual result, should design factors 1 through 4 be entered as shown in the sample inputs provided in this Chapter 6.

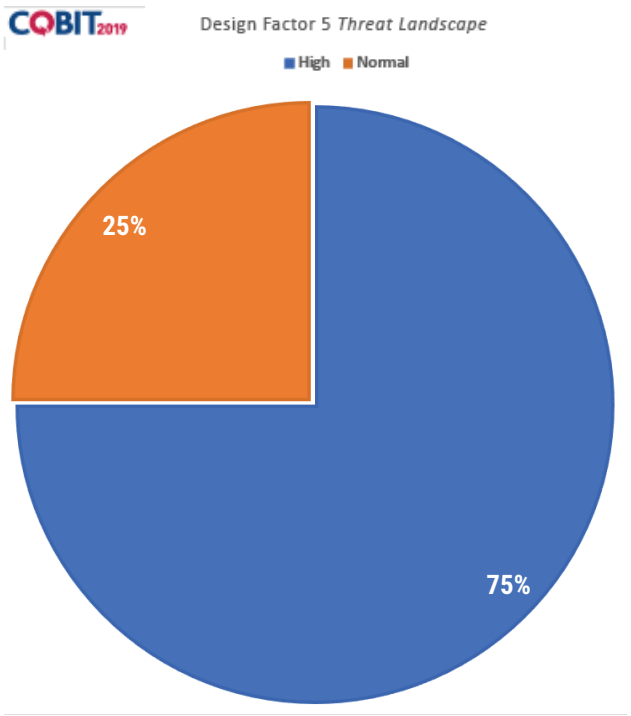
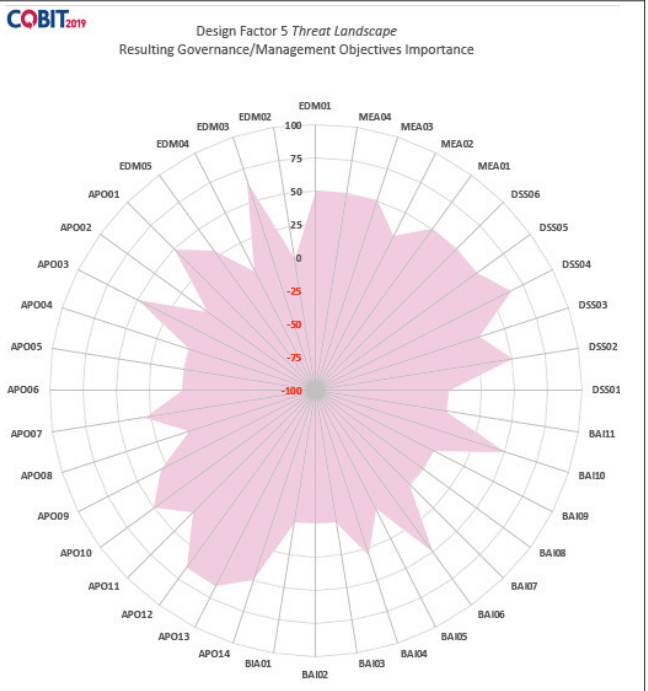
6.4 Step 3: Refine the Scope of the Governance System

In this step, the initial scope of the governance system is further refined based on the assessment of the remaining design factors:

1. Threat landscape
2. Compliance requirements
3. Role of IT
4. Sourcing model for IT
5. IT implementation methods
6. Technology adoption strategy
7. Enterprise size (note, this design factor is not included as part of the tool; see Section 6.4.7 for further detail)

6.4.1 Threat Landscape (Design Factor 5)

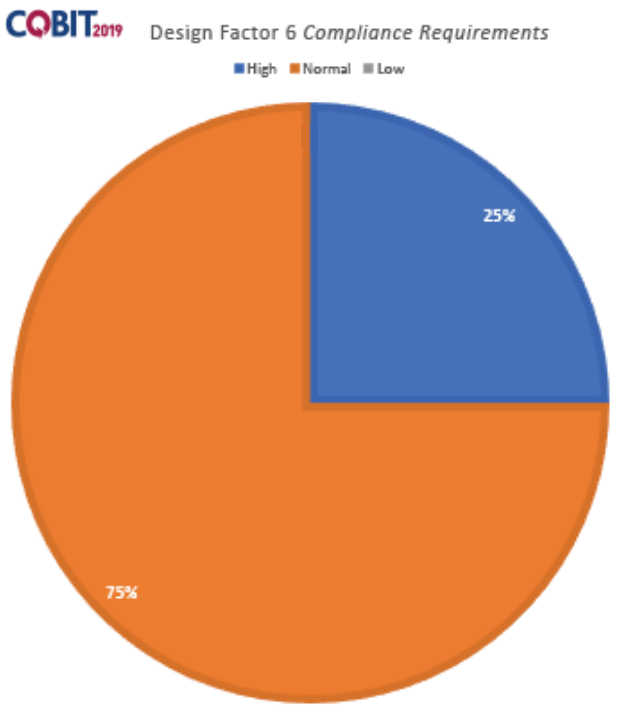
Input	• Each of the two possible values (high and normal) for the threat landscape design factor must be rated between 0% and 100%. The sum of both values must be 100%. • For many enterprises, 100% will be assigned to one of the categories. The option is available to assign percentages where a portion of enterprise operations is subject to a high threat landscape, while others are subject to a more normal threat landscape.
Calculation	• The tool performs a matrix calculation of the entered values for Design Factor 5 *Threat landscape* with the mapping table for design factor 5, resulting in a score for each governance/management objective. • The tool performs a second matrix calculation of a baseline set of values for design factor 5 with the mapping table for design factor 5, resulting in a baseline score for each governance/management objective. • The tool then calculates the relative importance for each governance/management objective as the relative difference between both sets of values, expressed as a percentage and rounded to 5. This number can be positive or negative, indicating that a governance/management objective is more or less important when compared to the baseline score.
Output	• The output of this tab contains the calculated relative importance of each of the 40 COBIT® 2019 governance and management objectives. • The results are represented in table format, as a bar chart and as a spider diagram.

Sample Input Graph	Sample Output Graph
	

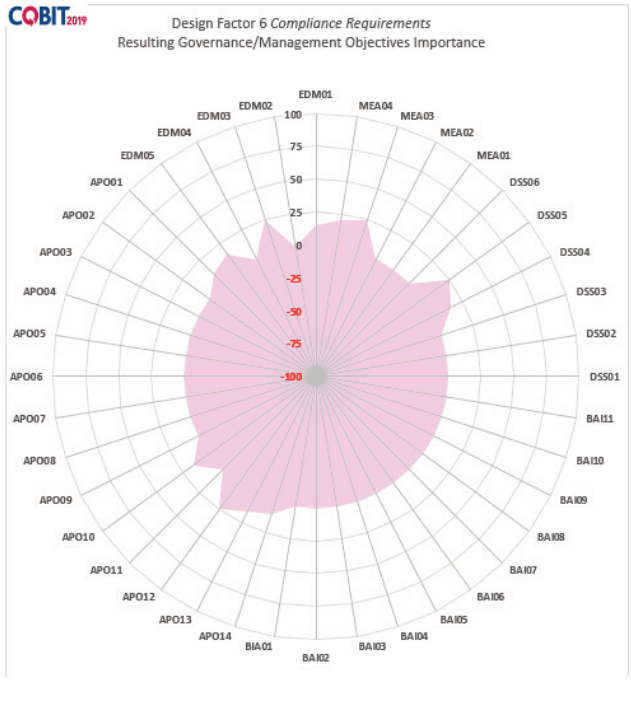
6.4.2 Compliance Requirements (Design Factor 6)

Input	• Each of the three possible values for the compliance requirements design factor must be rated between 0% and 100%. The sum of all three values must be 100%. • For many enterprises, 100% will be assigned to one of the categories. However, the option is available to assign different percentages, if the enterprise's IT landscape is quite vast, and certain parts are subject to strict compliance regulation, while other parts are subject to less strict regulation.
Calculation	• The tool performs a matrix calculation of the entered values for Design Factor 6 *Compliance Requirements* with the mapping table for design factor 6, resulting in a score for each governance/management objective. • The tool performs a second matrix calculation of a baseline set of values for design factor 6 with the mapping table for design factor 6, resulting in a baseline score for each governance/management objective. • The tool then calculates a relative importance for each governance/management objective as the relative difference between both sets of values, expressed as a percentage and rounded to 5. This number can be positive or negative, indicating that a governance/management objective is more or less important when compared to the baseline score.
Output	• The output of this tab contains the calculated relative importance of each of the 40 COBIT® 2019 governance and management objectives. • The results are represented in table format, as a bar chart and as a spider diagram.

Sample Input Graph

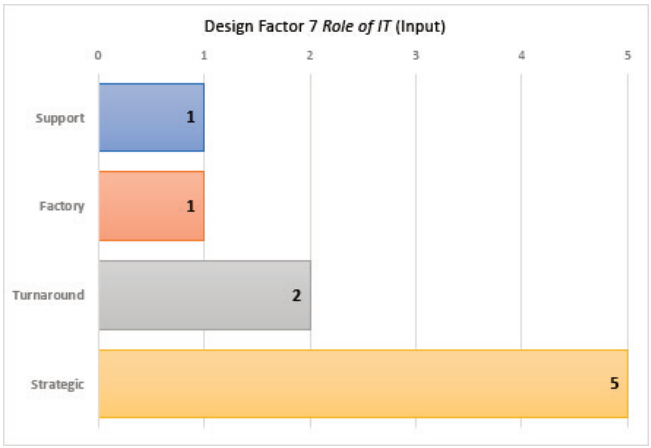
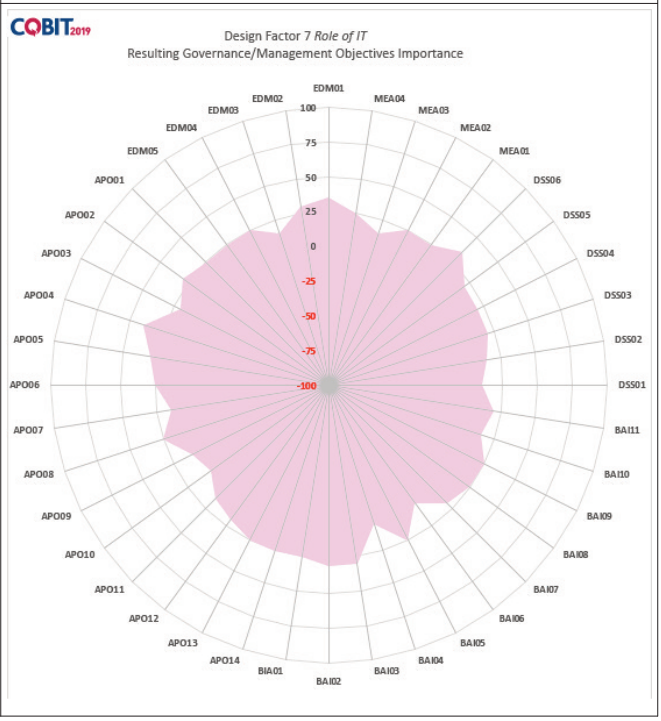


Sample Output Graph



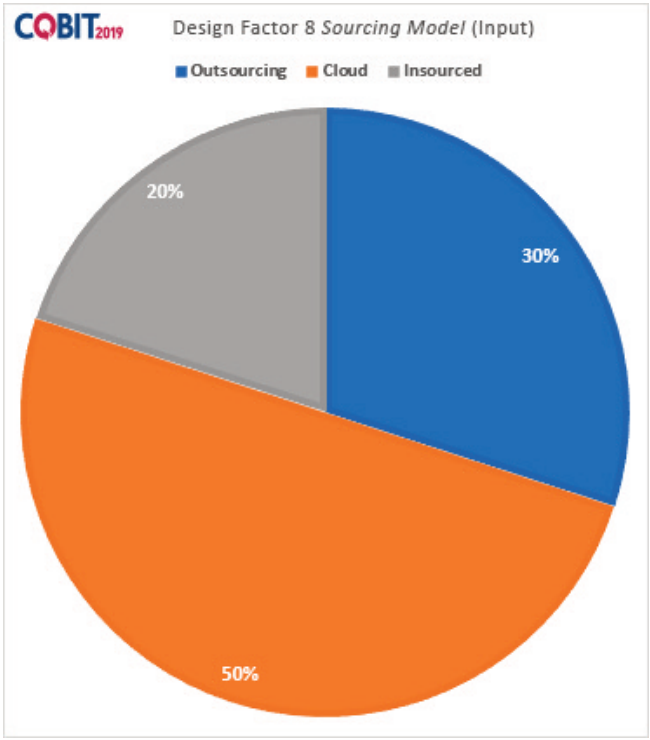
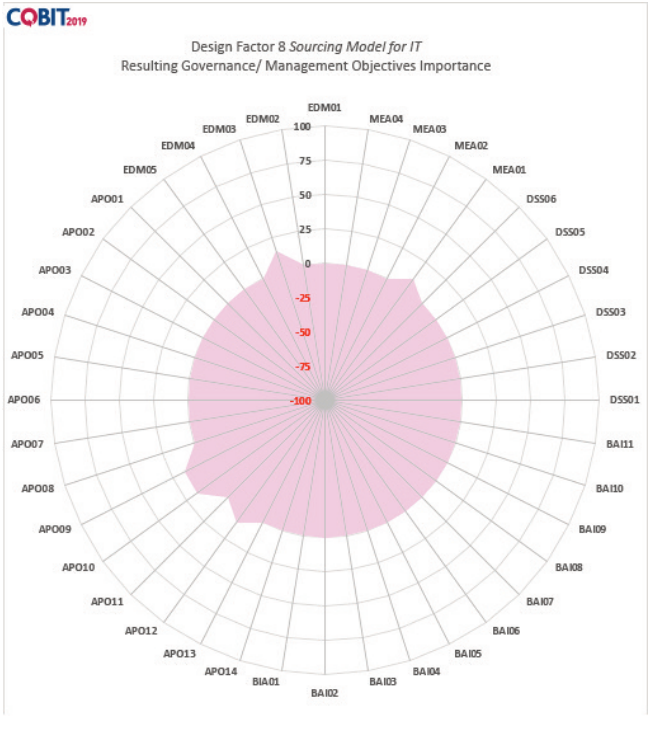
6.4.3 Role of IT (Design Factor 7)

Input	• Each of the four possible values for the role of IT design factor—support, factory, turnaround and strategic—must be rated between 1 (not important) and 5 (most important). • It is recommended to maintain sufficient spread between values.
Calculation	• The tool performs a matrix calculation of the entered values for Design Factor 7 *Role of IT* with the mapping table for design factor 7, resulting in a score for each governance/management objective. • The tool performs a second matrix calculation of a baseline set of values for design factor 7 with the mapping table for design factor 7, resulting in a baseline score for each governance/management objective. • The tool then calculates a relative importance for each governance/management objective as the relative difference between both sets of values, expressed as a percentage and rounded to 5. This number can be positive or negative, indicating that a governance/management objective is more or less important when compared to the baseline score.
Output	• The output of this tab contains the calculated relative importance of each of the 40 COBIT® 2019 governance and management objectives. • The results are represented in table format, as a bar chart and as a spider diagram.

Sample Input Graph	Sample Output Graph
	

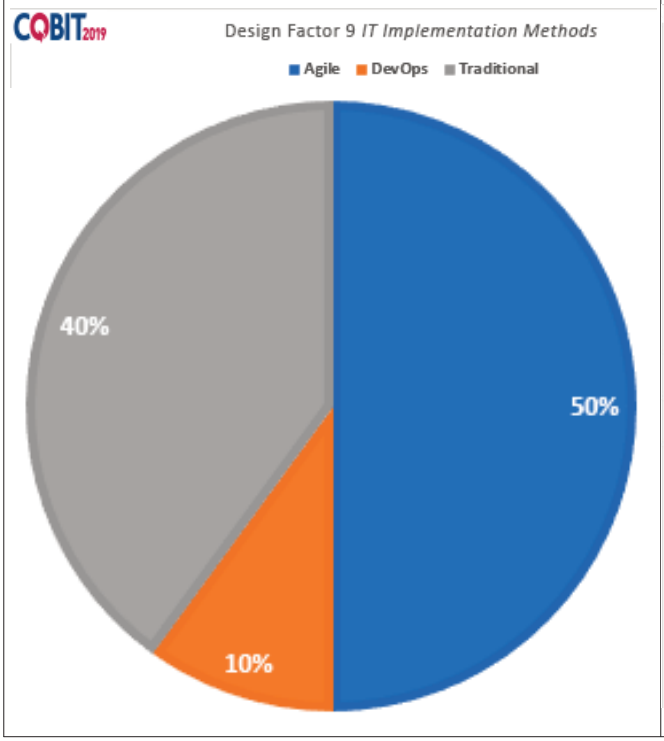
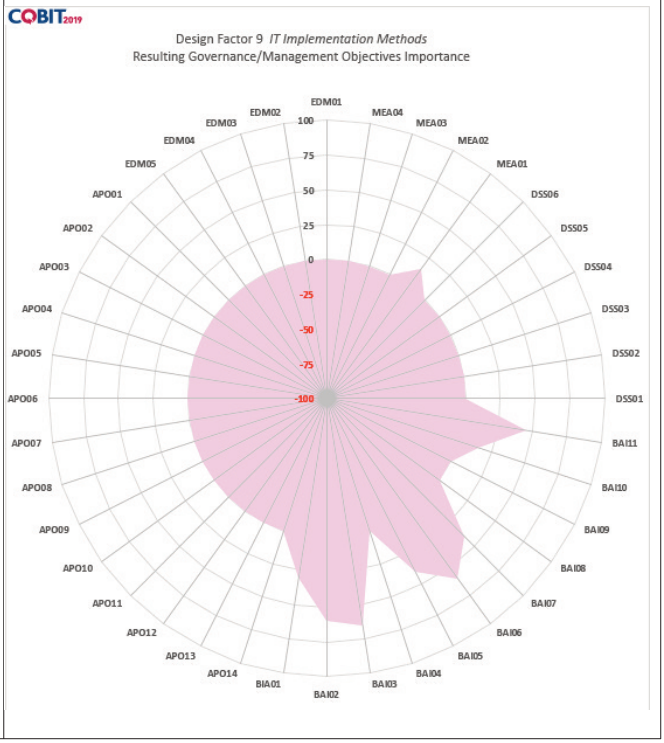
6.4.4 Sourcing Model for IT (Design Factor 8)

Input	• Each of the three possible values for the sourcing model for IT design factor—outsourcing, cloud and insourcing—must be rated between 0% and 100%. The sum of all three values must be 100%. • Note that there is a fourth category—the hybrid classification. This is not denoted in the tool, because, by definition, assigning percentages to more than one of the other three values creates a hybrid model.
Calculation	• The tool performs a matrix calculation of the entered values for Design Factor 8 *Sourcing Model for IT* with its corresponding mapping table, resulting in a score for each governance/management objective. • The tool performs a second matrix calculation of a baseline set of values for design factor 8 with the mapping table for design factor 8, resulting in a baseline score for each governance/management objective. • The tool then calculates a relative importance for each governance/management objective as the relative difference between both sets of values, expressed as a percentage and rounded to 5. This number can be positive or negative, indicating that a governance/management objective is more or less important when compared to the baseline score.
Output	• The output section of this tab contains the calculated relative importance of each of the 40 COBIT® 2019 governance and management objectives. • The results are represented in table format, as a bar chart and as a spider diagram.

Sample Input Graph	Sample Output Graph
	

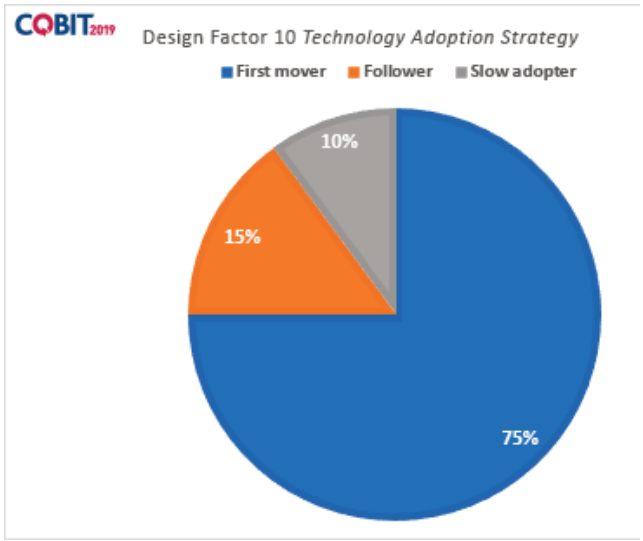
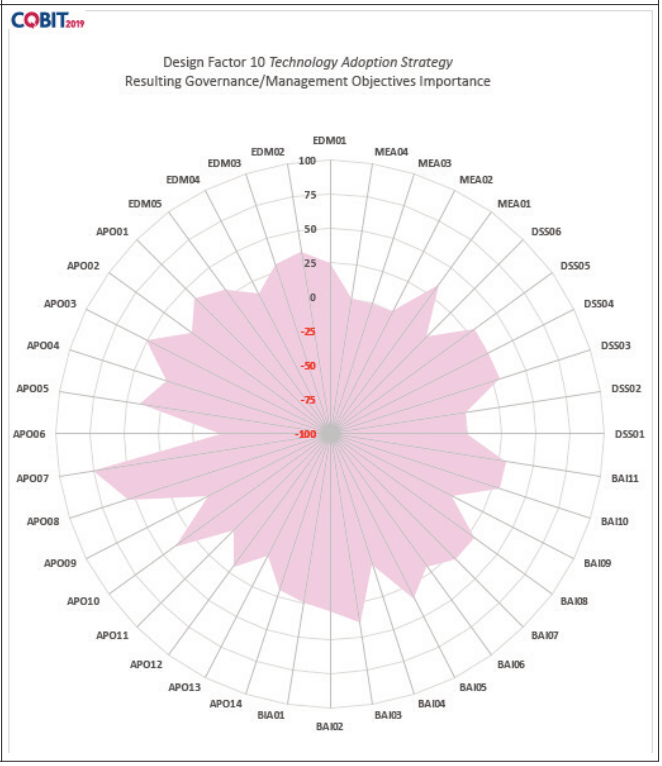
6.4.5 IT Implementation Methods (Design Factor 9)

Input	• Each of the three possible values for the IT implementation methods design factor—Agile, DevOps and traditional—must be rated between 0% and 100%. The sum of all three values must be 100%. • Note that there is a fourth category—the hybrid classification. This is not denoted in the tool, because, by definition, assigning percentages to more than one of the other three values creates a hybrid model.
Calculation	• The tool performs a matrix calculation of the entered values for Design Factor 9 *IT Implementation Methods* with the mapping table for design factor 9, resulting in a score for each governance/management objective. • The tool performs a second matrix calculation of a baseline set of values for design factor 9 with the mapping table for design factor 9, resulting in a baseline score for each governance/management objective. • The tool then calculates a relative importance for each governance/management objective as the relative difference between both sets of values, expressed as a percentage and rounded to 5. This number can be positive or negative, indicating that a governance/management objective is more or less important when compared to the baseline score.
Output	• The output section of this tab contains the calculated relative importance of each of the 40 COBIT® 2019 governance and management objectives. • The results are represented in table format, as a bar chart and as a spider diagram.

Sample Input Graph	Sample Output Graph
	

6.4.6 Technology Adoption Strategy (Design Factor 10)

Input	• Each of the three possible values for the technology adoption strategy design factor—first mover, follower, slow adopter—must be rated between 0% and 100%. The sum of all three values must be 100%. • For many enterprises, 100% may be assigned to one of the categories. However, the option is available to assign different percentages, if the enterprise's IT landscape is quite vast, and different areas adopt technology at difference paces.
Calculation	• The tool performs a matrix calculation of the entered values for Design Factor 10 *Technology Adoption Strategy* with the mapping table for design factor 10, resulting in a score for each governance/management objective. • The tool performs a second matrix calculation of a baseline set of values for design factor 10 with the mapping table for design factor 10, resulting in a baseline score for each governance/management objective. • The tool then calculates a relative importance for each governance/management objective as the relative difference between both sets of values, expressed as a percentage and rounded to 5. This number can be positive or negative, indicating that a governance/management objective is more or less important when compared to the baseline score.
Output	• The output of this tab contains the calculated relative importance of each of the 40 COBIT® 2019 governance and management objectives. • The results are represented in table format, as a bar chart and as a spider diagram.

Sample Input Graph	Sample Output Graph
	

6.4.7 Enterprise Size (Design Factor 11)

The enterprise size design factor only indicates whether the small and medium enterprise focus area guidance should be used, instead of the core COBIT guidance.[27] The size of an enterprise has no impact on the priority and target capability levels of governance and management objectives.

6.4.8 Conclusion

Input	• N/A

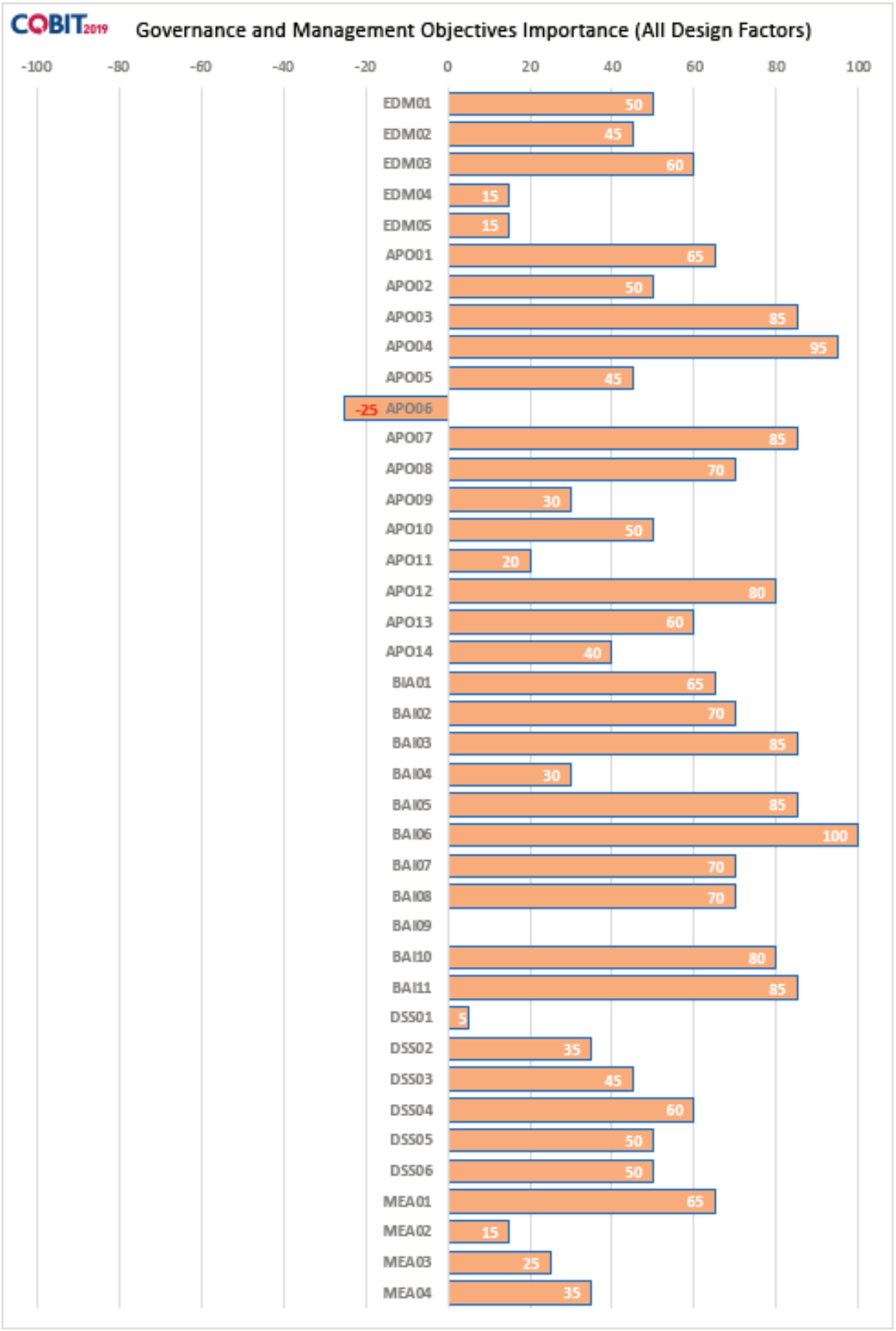
Calculation	• The tool performs a weighted summation of the calculated governance/management objectives importance scores related to the design factors 5 through 10, and combines it with the results of Step 2 *Initial design of the governance system*.
	• Weights can be entered on the canvas tab and are set to 1 by default. The weighting can be changed, if, for example, compliance requirements are of greater importance (because the enterprise operates in a highly regulated industry).
	• The achieved results are then normalized on a scale of 100.
	  ▪ The highest value (positive or negative) obtains a score of 100.
	  ▪ All other values are then prorated against this value.
	• The resulting list of scores not only provides a reliable view of the relative importance of all governance/management objectives against each other, but also gives an indication of the absolute importance. This output allows an enterprise not only to prioritize governance/management objectives against each other, but also to define adequate target capability levels.

Output	• The Step 3 summary tab contains the calculated relative importance of each of the 40 COBIT® 2019 governance and management objectives. • The results are represented in table format (on the canvas tab) and as a bar chart (on the Step 3 summary tab)

Note: The following sample graph is consistent with sample graphs for each design factor, in that it represents the actual result, should design factors 5 through 10 be entered as shown in the sample inputs provided in this Chapter 6.

[27] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, the small and medium enterprise focus area content was in development and not yet released.

Sample Output Graph



Chapter 7
Examples

7.1 Introduction

In this chapter, the workflow explained in Chapter 4 is applied to two fictitious examples and one case study, in order to illustrate the governance system design process. The examples include:

1. Manufacturing enterprise (Section 7.2)
2. Medium-sized innovative company (Section 7.3)
3. High-profile government agency (Section 7.4)

7.2 Example 1: Manufacturing Enterprise

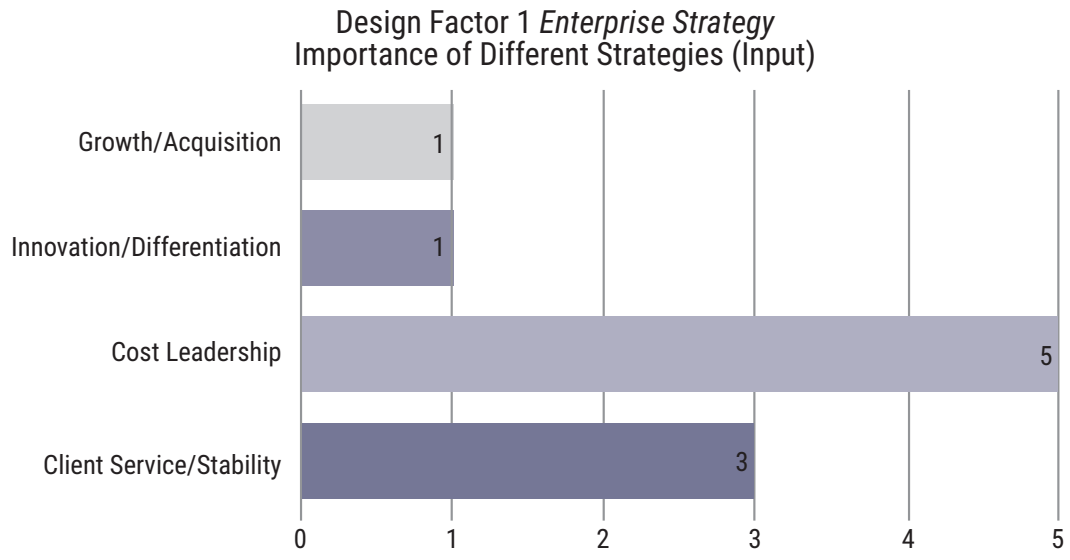
The corporation manufactures goods, is a large enterprise, is very cost conscious, and desires to be a cost leader in its market. The enterprise considers I&T purely a supporting function for efficient and effective operations. Although IT is a supporting function, the enterprise is critically dependent on it. The enterprise takes a traditional approach to new development and operations, and is quite hesitant to adopt new technologies. Recently, the enterprise was confronted with a malware attack and suffered from a number of operational IT problems. The enterprise houses and operates critical IT equipment in-house.

7.2.1 Step 1: Understand the Enterprise Context and Strategy

The first step of the governance design workflow is to summarize the external and internal context of the enterprise.

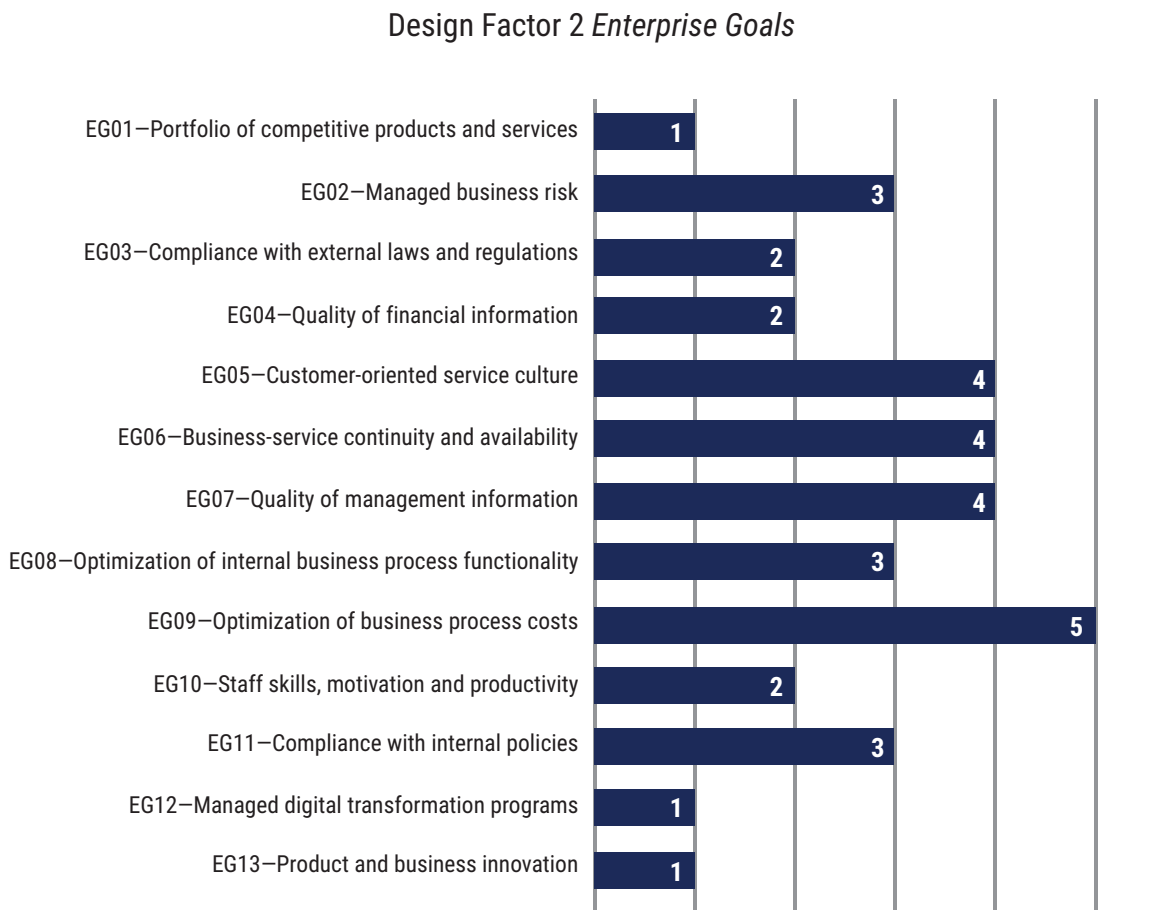
Step 1.1: Understand enterprise strategy—A primary focus on **cost leadership** and a secondary focus **on client service/stability** are depicted in **figure 7.1**.

Figure 7.1—Example 1, Step 1.1: Enterprise Strategy



Step 1.2: Understand enterprise goals—The enterprise has ranked the 13 generic enterprise goals on a scale from 1 to 5, as depicted in the following diagram. **Figure 7.2** shows that EG09 *Optimization of business process costs* is the highest-ranked enterprise goal.

Figure 7.2—Example 1, Step 1.2: Enterprise Goals



Step 1.3: Understand the risk profile—A high-level risk analysis has resulted in a risk profile, identifying the following highest risk categories (marked with red dots in the risk-rating column in **figure 7.3**): IT operational infrastructure incidents, unauthorized actions, software adoption/usage problems, hardware incidents, software failures and logical attacks. (These are broad categories. For detailed examples of risk scenarios within each category, please see Section 2.6.)

Figure 7.3—Example 1, Step 1.3: Risk Profile

Design Factor 3 *Risk Profile*

Risk Scenario Category	Impact (1-5)	Likelihood (1-5)	Risk Rating
IT investment decision making, portfolio definition and maintenance	4	3	●
Program and projects lifecycle management	3	1	●
IT cost and oversight	2	2	●
IT expertise, skills and behavior	3	3	●
Enterprise/it architecture	2	1	●
IT operational infrastructure incidents	4	4	●
Unauthorized actions	5	4	●
Software adoption/usage problems	4	4	●
Hardware incidents	4	4	●
Software failures	4	4	●
Logical attacks (hacking, malware, etc.)	5	3	●
Third-party/supplier incidents	2	4	●
Noncompliance	1	3	●
Geopolitical issues	2	1	●
Industrial action	4	2	●
Acts of nature	4	2	●
Technology-based innovation	4	1	●
Environmental	2	2	●
Data and information management	4	3	●

●	Very High Risk
●	High Risk
●	Normal Risk
●	Low Risk

Step 1.4: Understand current I&T-related issues—An analysis of the current situation (on a scale from 1 to 3) resulted in an assessment of current I&T-related issues, as depicted in **figure 7.4**. These are perceived to be important issues to the enterprise: significant incidents, service delivery problems by outsourcers, hidden IT cost and IT cost overall.

Figure 7.4—Example 1, Step 1.4: I&T-Related Issues

Value	Importance (1-3)	*Baseline*
Frustration between different IT entities across the organization because of a perception of low contribution to business value	✔	2
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	!	2
Significant IT-related incidents, such as data loss, security breaches, project failure and application errors, linked to IT	X	2
Service delivery problems by the IT outsourcer(s)	X	2
Failures to meet IT-related regulatory or contractual requirements	✔	2
Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems	✔	2
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	X	2
Duplications or overlaps between various initiatives, or other forms of wasted resources	✔	2
Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction	!	2
IT-enabled changes or projects frequently failing to meet business needs and delivered late or over budget	✔	2
Reluctance by board members, executives or senior management to engage with IT, or a lack of committed business sponsorship for IT	✔	2
Complex IT operating model and/or unclear decision mechanisms for IT-related decisions	✔	2
Excessively high cost of IT	X	2
Obstructed or failed implementation of new initiatives or innovations caused by the current IT architecture and systems	✔	2
Gap between business and technical knowledge, which leads to business users and information and/or technology specialists speaking different languages	✔	2
Regular issues with data quality and integration of data across various sources	!	2
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	✔	2
Business departments implementing their own information solutions with little or no involvement of the enterprise IT department	!	2
Ignorance of and/or noncompliance with privacy regulations	✔	2
Inability to exploit new technologies or innovate using I&T	✔	2

✔	No Issue
!	Issue
X	Serious Issue

7.2.2 Step 2: Determine the Initial Scope of the Governance System

The initial scope of the governance system is determined by using the information (partial or in full) collected during Step 1. Step 2 translates this information on enterprise goals, enterprise strategy and risk profile to relevant governance components.

Step 2.1: Consider enterprise strategy—**Figure 7.5** represents the enterprise strategy, as identified in step 1.1. **Figure 7.6** shows the relative influence these strategies have on governance and management objectives**.**

Figure 7.5—Example 1, Step 2.1: Enterprise Strategy

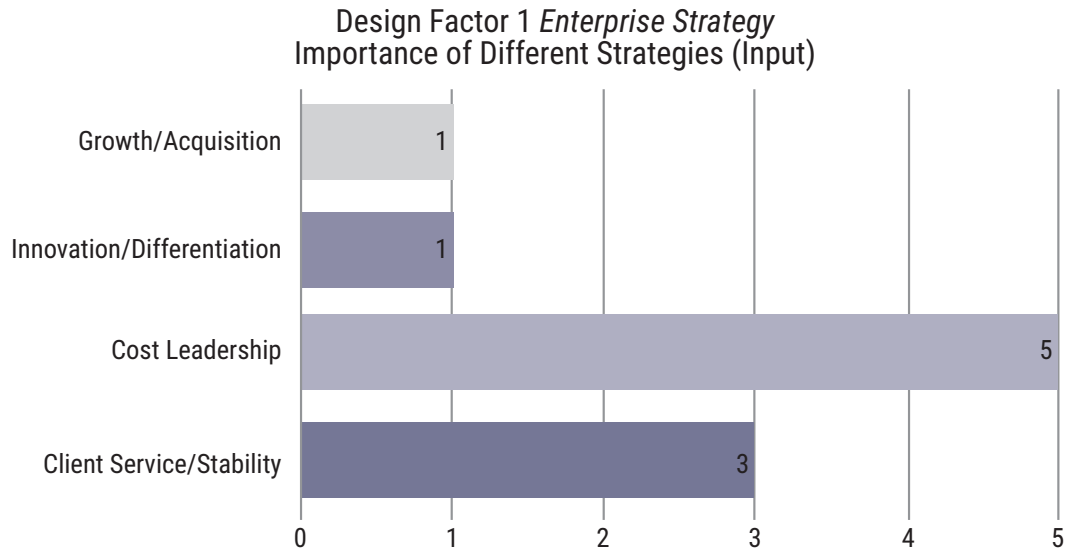
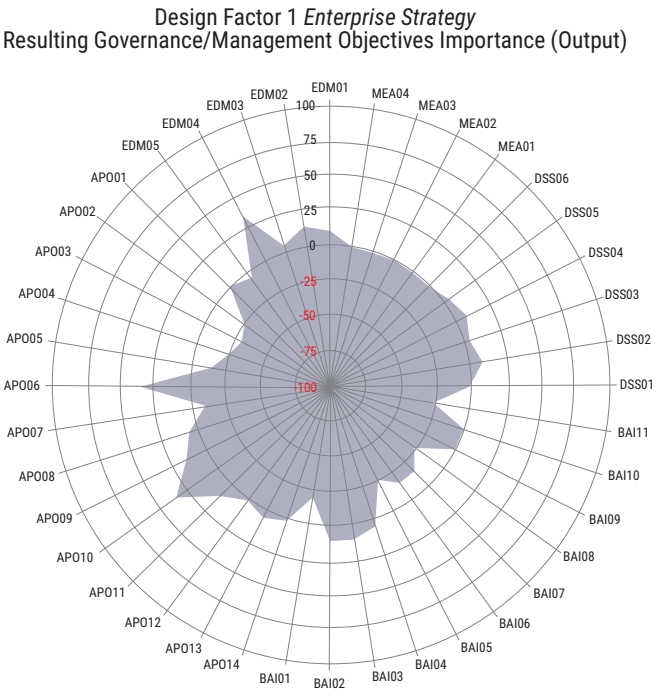


Figure 7.6—Example 1, Step 2.1: Resulting Governance/Management Objectives Importance for Design Factor 1 *Enterprise Strategy*



In addition to the governance and management processes highlighted by **figure 7.6**, the following other components also require attention require attention:

- Focus on IT costing and budgeting skills
- Influence of the culture and behavior component
- Contribution of the services, infrastructure and applications component (e.g., for automation of controls, improving efficiency)

Step 2.2: Consider enterprise goals and apply the COBIT goals cascade—At this point, the COBIT goals cascade is applied to determine which governance and management objectives are relevant to achieve the priority enterprise goals, based on their ranking, assigned in step 1.2 (**figure 7.7**). **Figure 7.8** shows the relative influence these ranked enterprise goals have on governance and management objectives.

Figure 7.7—Example 1, Step 2.2: Enterprise Goals

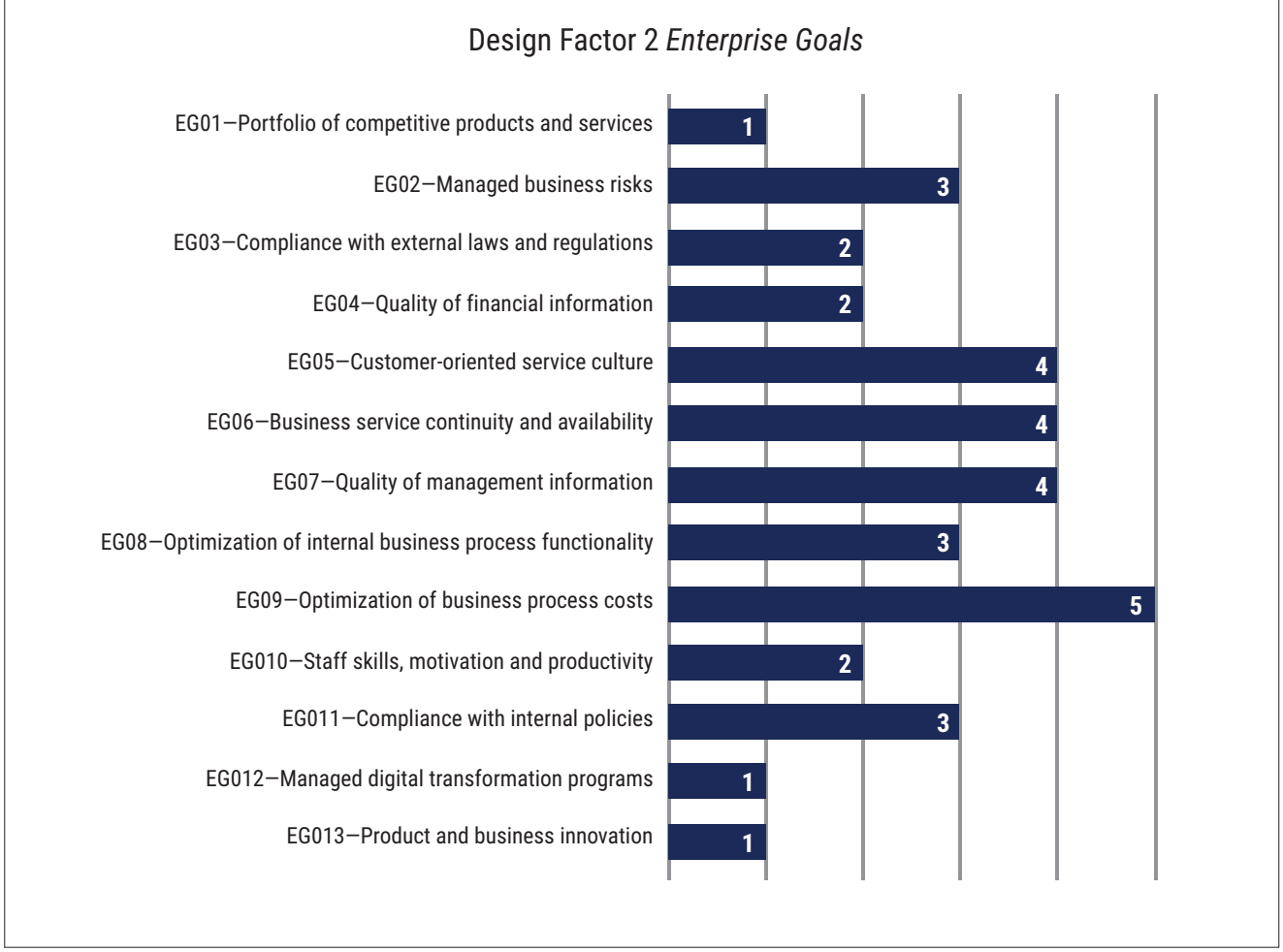
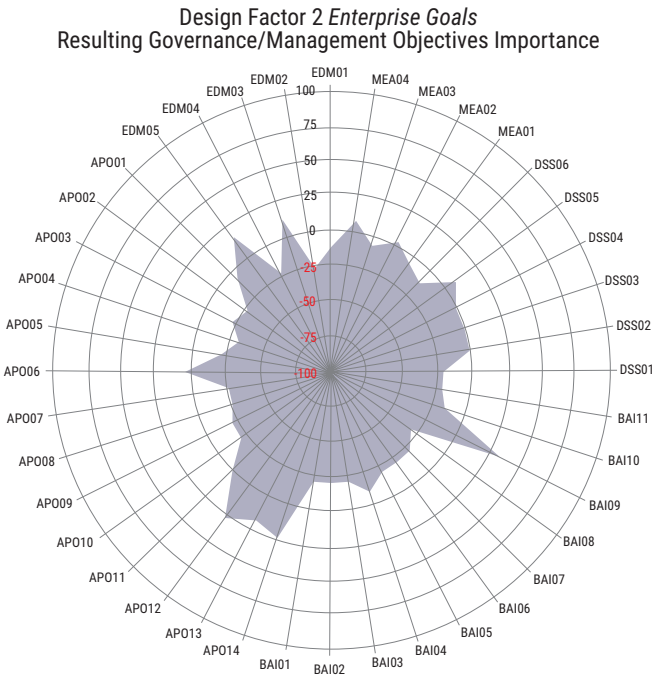


Figure 7.8—Example 1, Step 2.2: Resulting Governance/Management Objectives Importance for Design Factor 2 *Enterprise Goals*



Step 2.3: Consider the risk profile of the enterprise—In step 1.3, the IT risk categories were identified and analyzed at a high level (**figure 7.9**). Based on the mapping between the risk profile and the COBIT governance and management objectives (as explained in Section 4.2.3, and per the mapping table included in Appendix D), **figure 7.10** shows the relative ranking of the governance and management objectives, based on the results of the risk analysis.

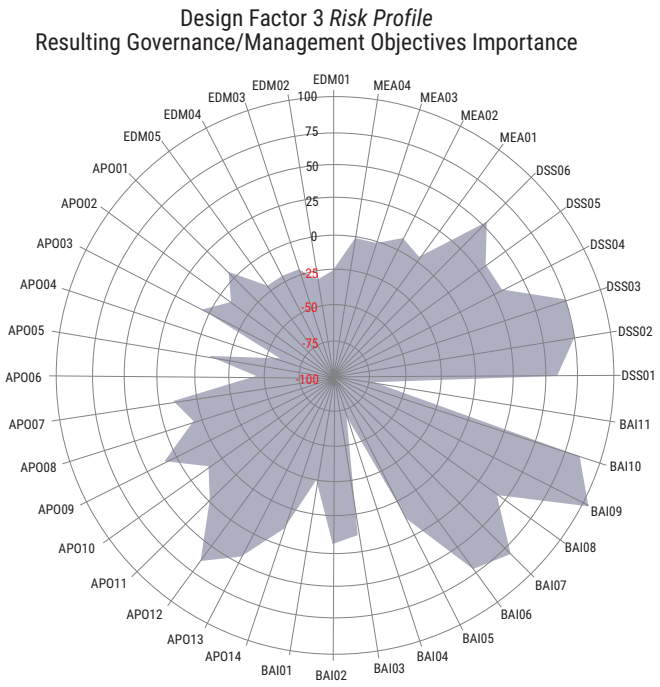
Figure 7.9—Example 1, Step 2.3: Risk Profile

Design Factor 3 *Risk Profile*

Risk Scenario Category	Impact (1-5)	Likelihood (1-5)	Risk Rating
IT investment decision making, portfolio definition and maintenance	4	3	
Program and projects lifecycle management	3	1	
IT cost and oversight	2	2	
IT expertise, skills and behavior	3	3	
Enterprise/it architecture	2	1	
IT operational infrastructure incidents	4	4	
Unauthorized actions	5	4	
Software adoption/usage problems	4	4	
Hardware incidents	4	4	
Software failures	4	4	
Logical attacks (hacking, malware, etc.)	5	3	
Third-party/supplier incidents	2	4	
Noncompliance	1	3	
Geopolitical issues	2	1	
Industrial action	4	2	
Acts of nature	4	2	
Technology-based innovation	4	1	
Environmental	2	2	
Data and information management	4	3	

	Very High Risk
	High Risk
	Normal Risk
	Low Risk

Figure 7.10—Example 1, Step 2.3: Resulting Governance/Management Objectives Importance for Design Factor 3 *Risk Profile*



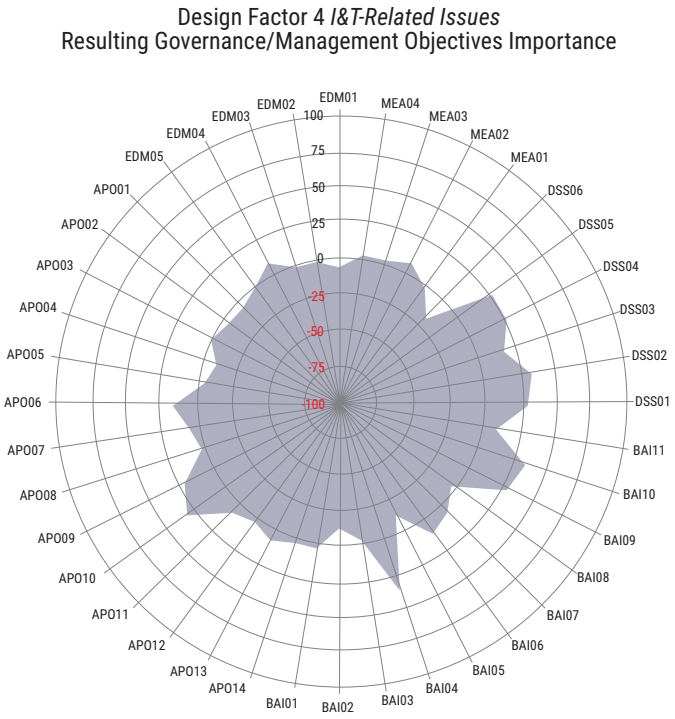
Step 2.4: Consider current I&T-related issues—In this step, the issues identified in step 1.4 are related to the COBIT governance and management objectives through a mapping table (**Appendix E**) that associates each issue to one or more governance or management objectives that can influence that issue. Based on that mapping (as explained in Section 4.2.4), **figure 7.12** shows the relative ranking of the governance and management objectives, based on the enterprise's analysis of current I&T-related issues **(figure 7.11)**.

Figure 7.11—Example 1, Step 2.4: I&T-Related Issues

Value	Importance (1-3)	*Baseline*
Frustration between different IT entities across the organization because of a perception of low contribution to business value	✔	2
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	!	2
Significant IT-related incidents, such as data loss, security breaches, project failure and application errors, linked to IT	X	2
Service delivery problems by the IT outsourcer(s)	X	2
Failures to meet IT-related regulatory or contractual requirements	✔	2
Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems	✔	2
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	X	2
Duplications or overlaps between various initiatives, or other forms of wasted resources	✔	2
Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction	!	2
IT-enabled changes or projects frequently failing to meet business needs and delivered late or over budget	✔	2
Reluctance by board members, executives or senior management to engage with IT, or a lack of committed business sponsorship for IT	✔	2
Complex IT operating model and/or unclear decision mechanisms for IT-related decisions	✔	2
Excessively high cost of IT	X	2
Obstructed or failed implementation of new initiatives or innovations caused by the current IT architecture and systems	✔	2
Gap between business and technical knowledge, which leads to business users and information and/or technology specialists speaking different languages	✔	2
Regular issues with data quality and integration of data across various sources	!	2
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	✔	2
Business departments implementing their own information solutions with little or no involvement of the enterprise IT department	!	2
Ignorance of and/or noncompliance with privacy regulations	✔	2
Inability to exploit new technologies or innovate using I&T	✔	2

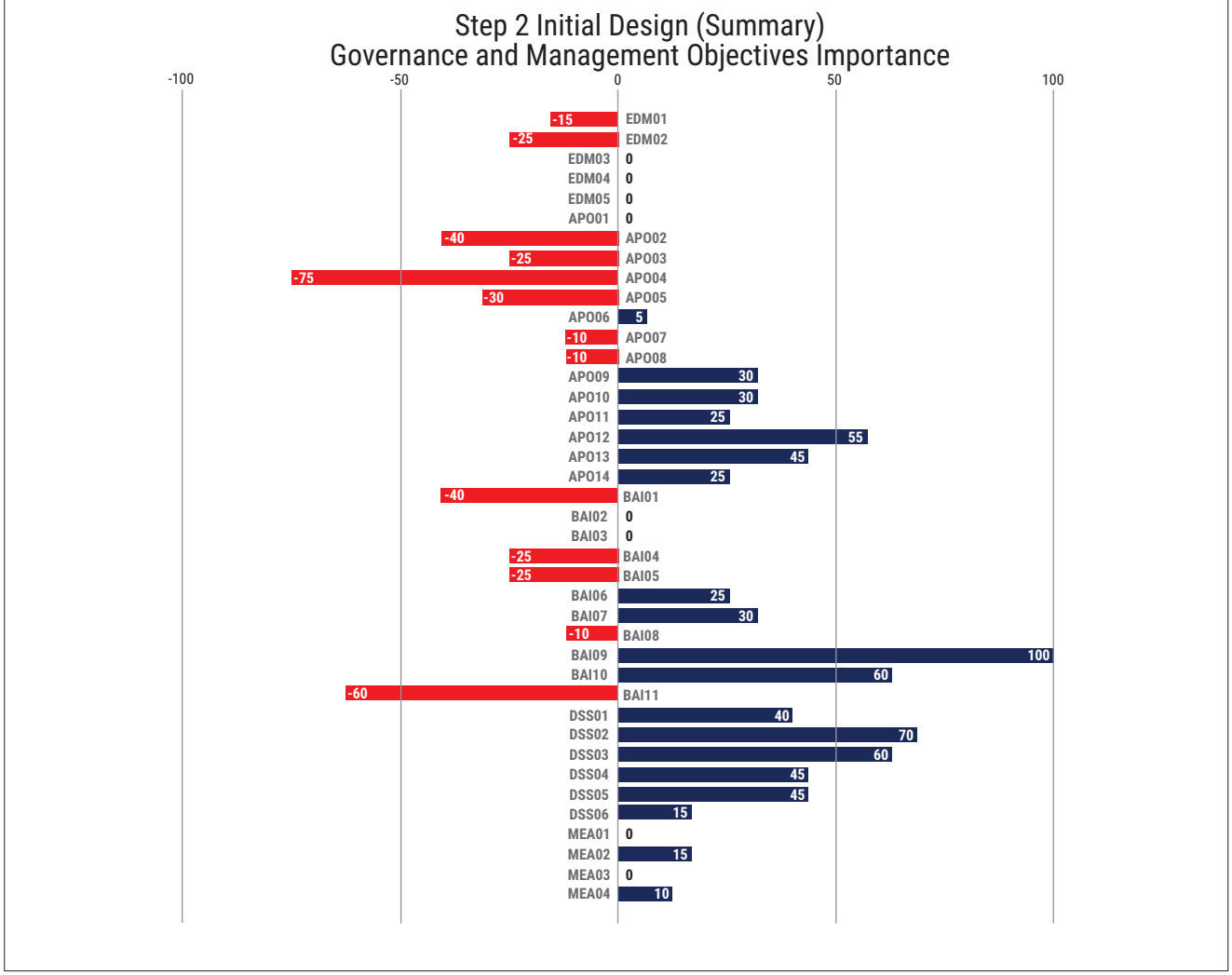
✔	No Issue
!	Issue
X	Serious Issue

Figure 7.12—Example 1, Step 2.4: Resulting Governance/Management Objectives Importance for Design Factor 4 *I&T-Related Issues*



Step 2.5: Initial scope of the governance system—At this point, it is possible to combine the resulting governance and management priorities from the previous four steps to produce the following initial priorities for governance and management objectives in the governance system (**figure 7.13**).

Figure 7.13—Example 1, Step 2.5: Initial Design Summary of Governance and Management Objectives Importance



The top five following management objectives are likely to be important for the governance system of this enterprise:

- BAI09 *Managed Assets*
- DSS02 *Managed Service Requests and Incidents*
- DSS03 *Managed Problems*
- BAI10 *Managed Configuration*
- APO12 *Managed Risk*

The following management objectives seem (for now) the least important:

- APO04 *Managed Innovation*

- BAI11 *Managed Projects*
- APO02 *Managed Strategy*
- BAI01 *Managed Programs*
- APO05 *Managed Portfolio*

The next step will determine which refinements are still required to this initial scope of the governance system.

7.2.3 Step 3: Refine the Scope of the Governance System

In step 3, refinements to the initial scope are identified, based on the remaining set of design factors to be analyzed. Not all design factors might be applicable for each enterprise, in which case they can be ignored. **Figure 7.14** shows a summary of the design factors 5 through 11 that are applicable to the manufacturing enterprise in this example. When more than one value was applicable for a certain design factor, it is so indicated in the value column of the figure.

Figure 7.14—Example 1 Tailored Version of Governance System

Ref	Design Factor	Value	Governance and Management Objectives Priority	Components	Focus Area Guidance
DF5			**Threat Landscape**		
	High	90%[28]	Important governance and management objectives include: • EDM01, EDM03 • APO01, APO03, APO10, APO12, APO13, APO14 • BAI06, BAI10 • DSS02, DSS04, DSS05, DSS06 • MEA01, MEA03, MEA04	Important organizational structures include: • Security strategy committee • CISO Important culture and behavior aspects include: • Security awareness Information flows: • Security policy • Security strategy	Information security focus area[29]
	Normal	10%	• *As per the initial scope definition*	• *N/A*	COBIT core model
DF6			**Compliance Requirements**		
	Normal	75%	Most important, but yet moderate, management objectives include: • EDM01, EDM03 • APO12 • MEA03	• *N/A*	COBIT core model
	Low	25%	• *As per the initial scope definition*	• *N/A*	COBIT core model
DF7			**Role of IT**		
	Factory	5 on scale of 5	Important governance and management objectives include: • EDM03 • DSS01, DSS02, DSS03, DSS04	• *N/A*	Information security focus area[30]
	Turnaround	2 on scale of 5	Important governance and management objectives include: • APO02, APO04 • BAI02, BAI03	• *N/A*	DevOps focus area[31]

[28] This figure means that 90% of the enterprise's operations and I&T activities are done in a high threat landscape.
[29] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, the information security focus area content was in development and not yet released.
[30] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, the information security focus area content was in development and not yet released.
[31] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, the DevOps focus area content was in development and not yet released.

Figure 7.14—Example 1 Tailored Version of Governance System *(cont.)*					
Ref	**Design Factor**	**Value**	**Governance and Management Objectives Priority**	**Components**	**Focus Area Guidance**
DF8	**Sourcing Model for IT**				
	Outsourcing	20%	Important management objectives include: • APO09, APO10 • MEA01	• *N/A*	Vendor management focus area [32]
	Insourced	80%	• *As per the initial scope definition*	• *N/A*	COBIT core model
DF9	**IT Implementation Methods**				
	Traditional		• *As per the initial scope definition*	• *N/A*	COBIT core model
DF10	**Technology Adoption Strategy**				
	Follower	90%[33]	Important governance and management objectives include: • APO02, APO04 • BAI01	Processes that can run at a slower pace	COBIT core model
	Slow Adopter	10%[34]	• *As per the initial scope definition*	• *N/A*	COBIT core model
DF11	**Enterprise Size**				
	Large		• *As per the initial scope definition*	• *N/A*	COBIT core model

For each design factor in **figure 7.14**, the current assessed situation can be combined with the mapped governance and management objectives and other guidance in **figure 7.14**. The following examples were produced using matrix calculations between the input values and a mapping between these values and governance and management objectives. Mapping tables are included in Appendices F through K of this publication. The resulting spider charts, with the prioritized governance and management objectives, represent relative importance levels compared to a baseline level. Relative importance levels are expressed on a scale from -100 to +100, with zero (0) indicating that there is no impact on the importance of a governance or management objective, and +100 indicating that the objective has become twice as important due to the design factor at hand.

[32] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, the vendor management focus area content was being contemplated as a potential future focus area.
[33] This figure means that the organization is 90% considered to be a follower in terms of technology adoption.
[34] This figure means that 10% of the enterprise's I&T activities are considered to be at a slow adopter pace.

Step 3.1—Consider the threat landscape —**Figure 7.15** depicts the threat landscape under which the enterprise believes it operates. **Figure 7.16** shows the impact on governance and management objectives of the assessed threat landscape.

Figure 7.15—Example 1, Step 3.1: Threat Landscape

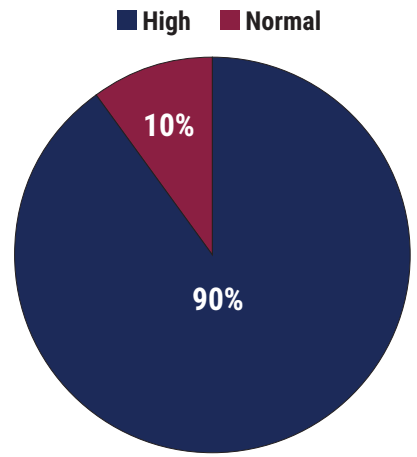
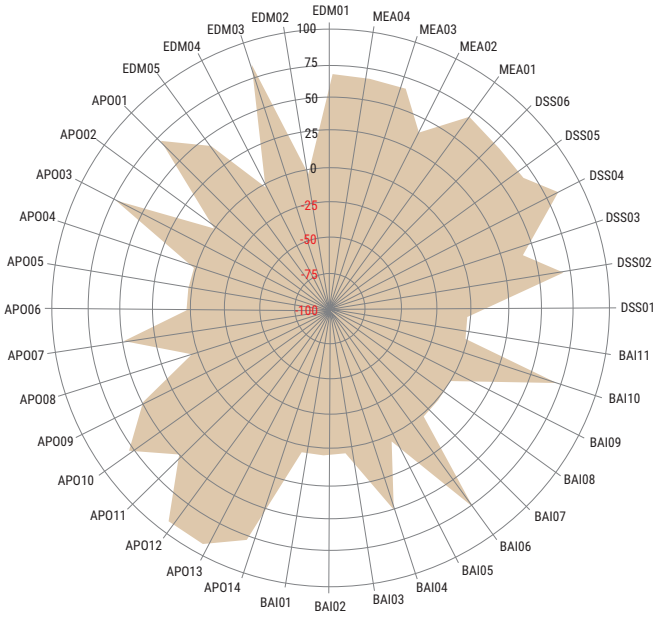


Figure 7.16—Example 1, Step 3.1: Resulting Governance/Management Objectives Importance for Design Factor 5 *Threat Landscape*



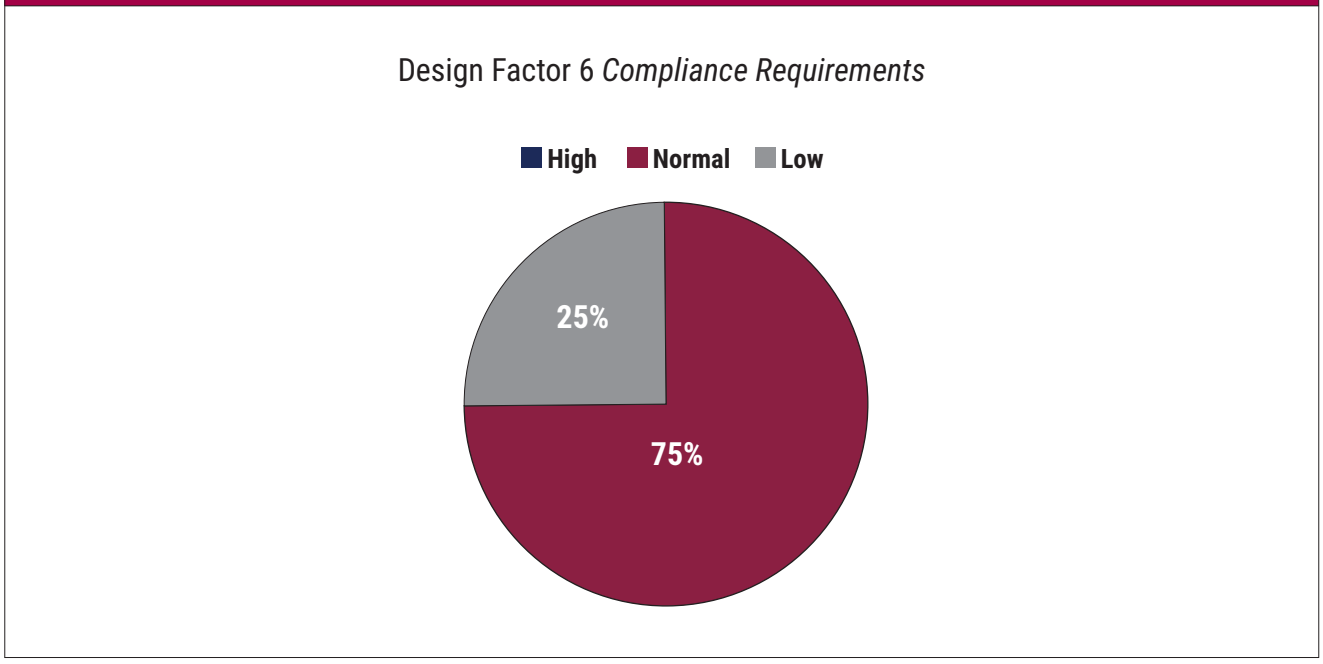
This classification of the threat landscape renders a substantial number of governance and management objectives more important, per the **figure 7.14** entry related to high-threat landscape. Guidance on these governance and management objectives should be drawn from the information security focus area guidance,[35] which contains more detailed and specific guidance on information security than the COBIT core model.

In addition, the enterprise must consider (for inclusion in its governance system design) the presence and performance of the following:

- Important organizational structures, including:
  - Security strategy committee
  - CISO
- Important culture and behavior aspects, including:
  - Security awareness
- Information flows:
  - Security policy
  - Security strategy

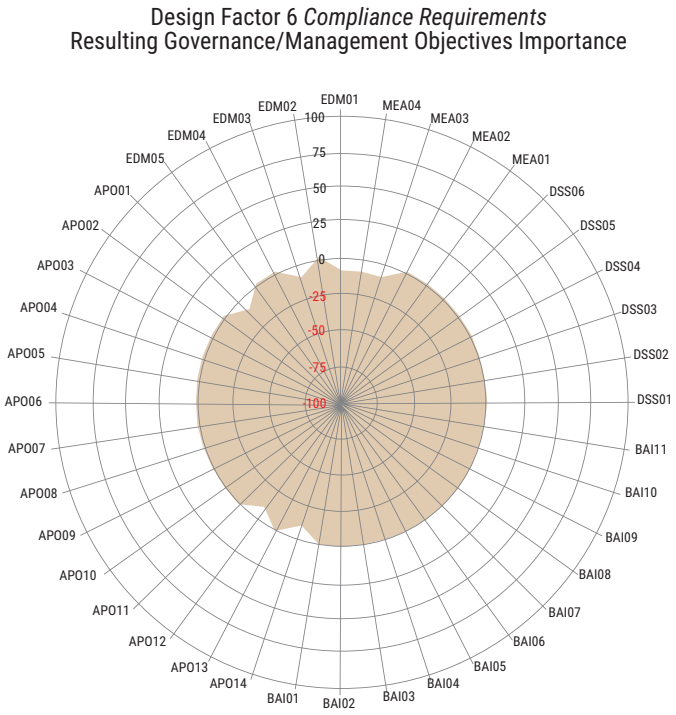
Step 3.2—Consider compliance requirements—**Figure 7.17** depicts the compliance requirements for the enterprise, which are estimated to be normal, leaning to low. **Figure 7.18** shows the impact of the assessed compliance requirements on the governance and management objectives. There is very little impact, which is the expected result.

Figure 7.17—Example 1, Step 3.2: Compliance Requirements



[35] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, the information security focus area content was in development and not yet released.

Figure 7.18—Example 1, Step 3.2: Resulting Governance/Management Objectives Importance for Design Factor 6 *Compliance Requirements*



Step 3.3—Consider the role of IT—**Figure 7.19** shows the role of IT, which is expressed as factory, with a secondary choice of turnaround, indicating that the enterprise is highly operationally dependent on its IT services. **Figure 7.20** shows the impact of the assessed role of IT on the governance and management objectives.

Figure 7.19—Example 1, Step 3.3: Role of IT

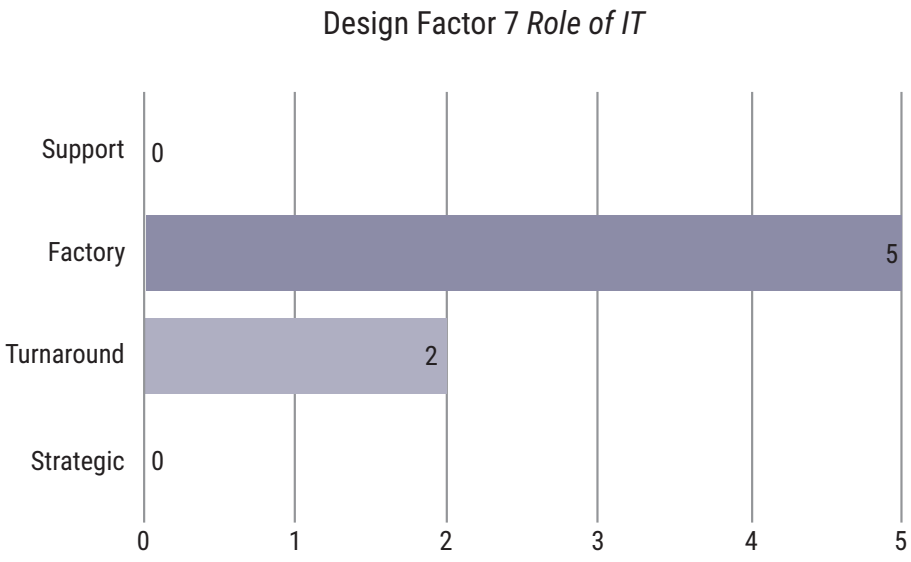
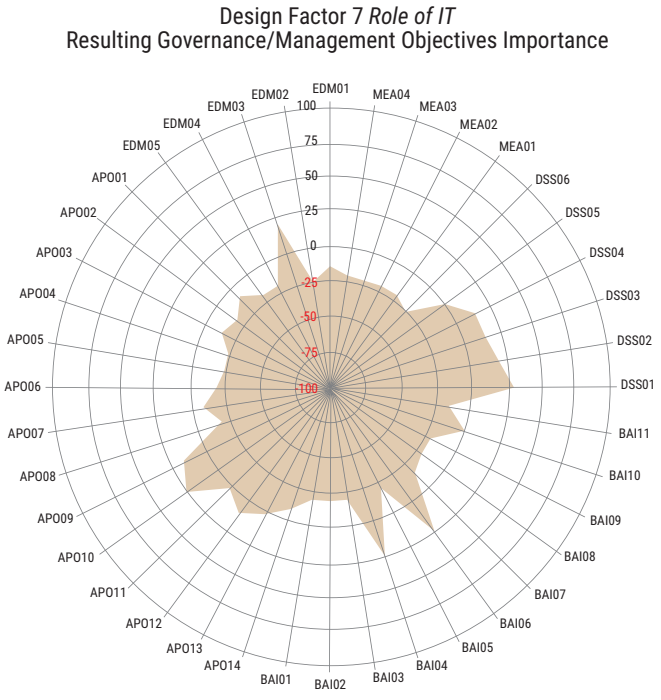


Figure 7.20—Example 1, Step 3.3: Resulting Governance/Management Objectives Importance for Design Factor 7 *Role of IT*



In addition to the prioritized governance and management objectives, guidance should be drawn from the information security and DevOps focus areas (when available and necessary).

Step 3.4—Consider the sourcing model—**Figure 7.21** depicts the selected sourcing model of the enterprise, which is predominantly insourcing. **Figure 7.22** shows the impact of the assessed sourcing model on the governance and management objectives. The impact is quite limited for this design factor.

Figure 7.21—Example 1, Step 3.4: Sourcing Model for IT

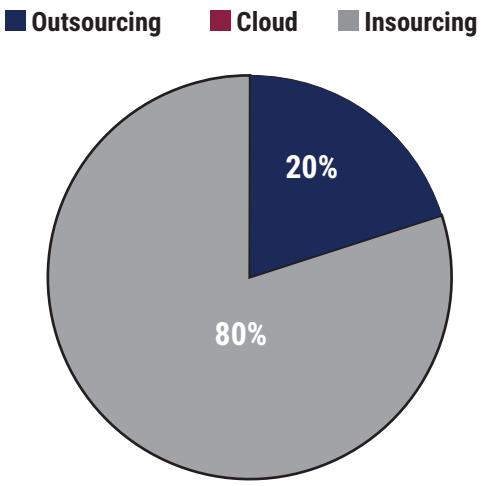
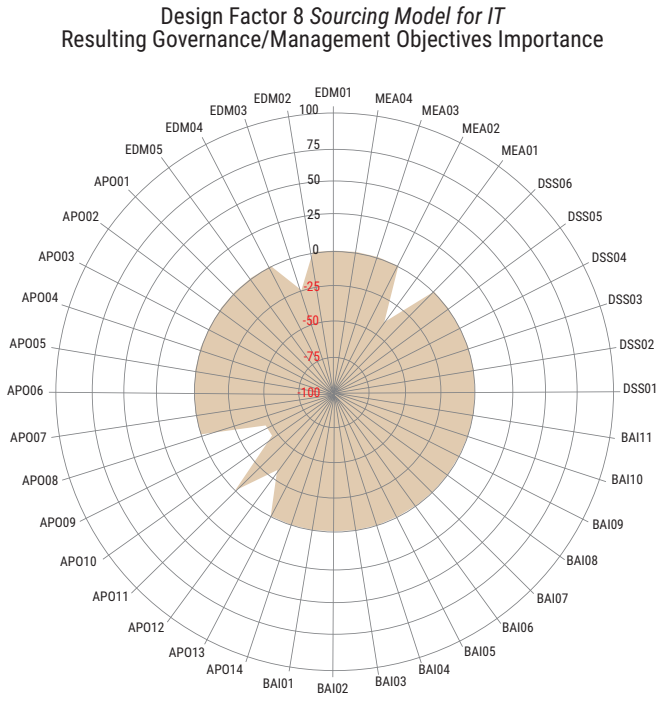


Figure 7.22—Example 1, Step 3.4: Resulting Governance/Management Objectives Importance for Design Factor 8 *Sourcing Model for IT*



Step 3.5—Consider IT implementation methods—The enterprise uses traditional IT development and operations methods (**figure 7.23**), leading to no impact on the governance and management objectives (**figure 7.24**).

Figure 7.23—Example 1, Step 3.5: IT Implementation Methods

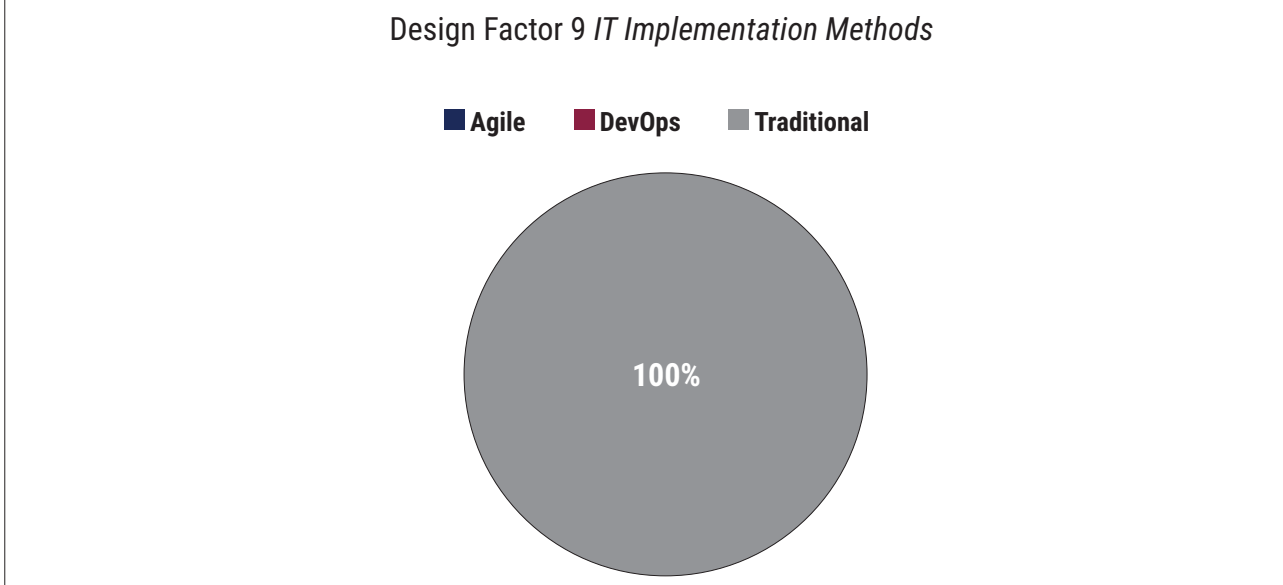
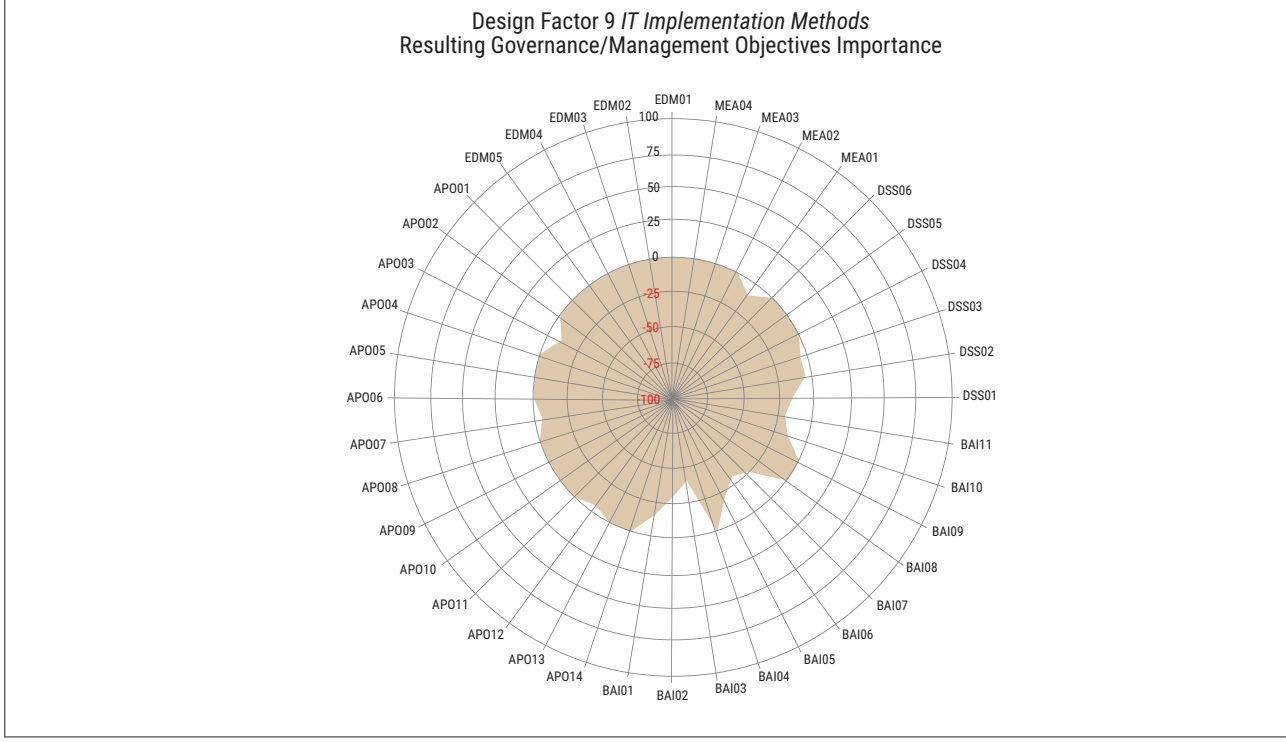


Figure 7.24—Example 1, Step 3.5: Resulting Governance/Management Objectives Importance for Design Factor 9 *IT Implementation Methods*



Step 3.6—Consider the technology adoption strategy—**Figure 7.25** indicates that the enterprise is, at best, a follower when it comes to new technology adoption. **Figure 7.26** shows the very limited impact this has on governance and management objectives priorities.

Figure 7.25—Example 1, Step 3.6: Technology Adoption Strategy

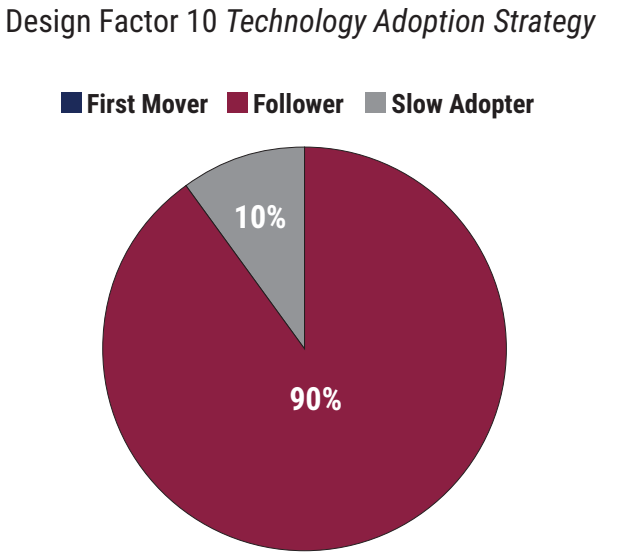
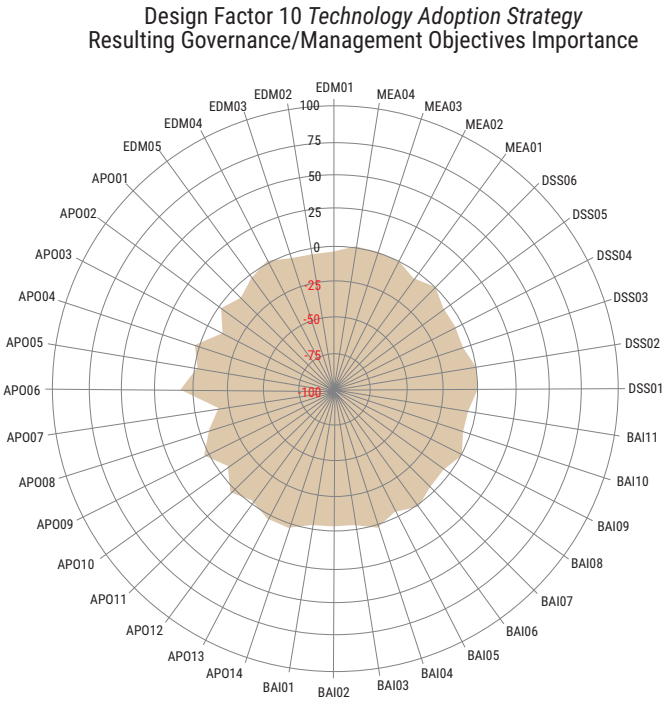


Figure 7.26—Example 1, Step 3.6: Resulting Governance/Management Objectives Importance for Design Factor 10 *Technology Adoption Strategy*



Step 3.7—Consider Enterprise Size—The enterprise is classified as large. Per **figure 7.14**, this means that the COBIT core model should be used as the basis for the definition of the governance system.

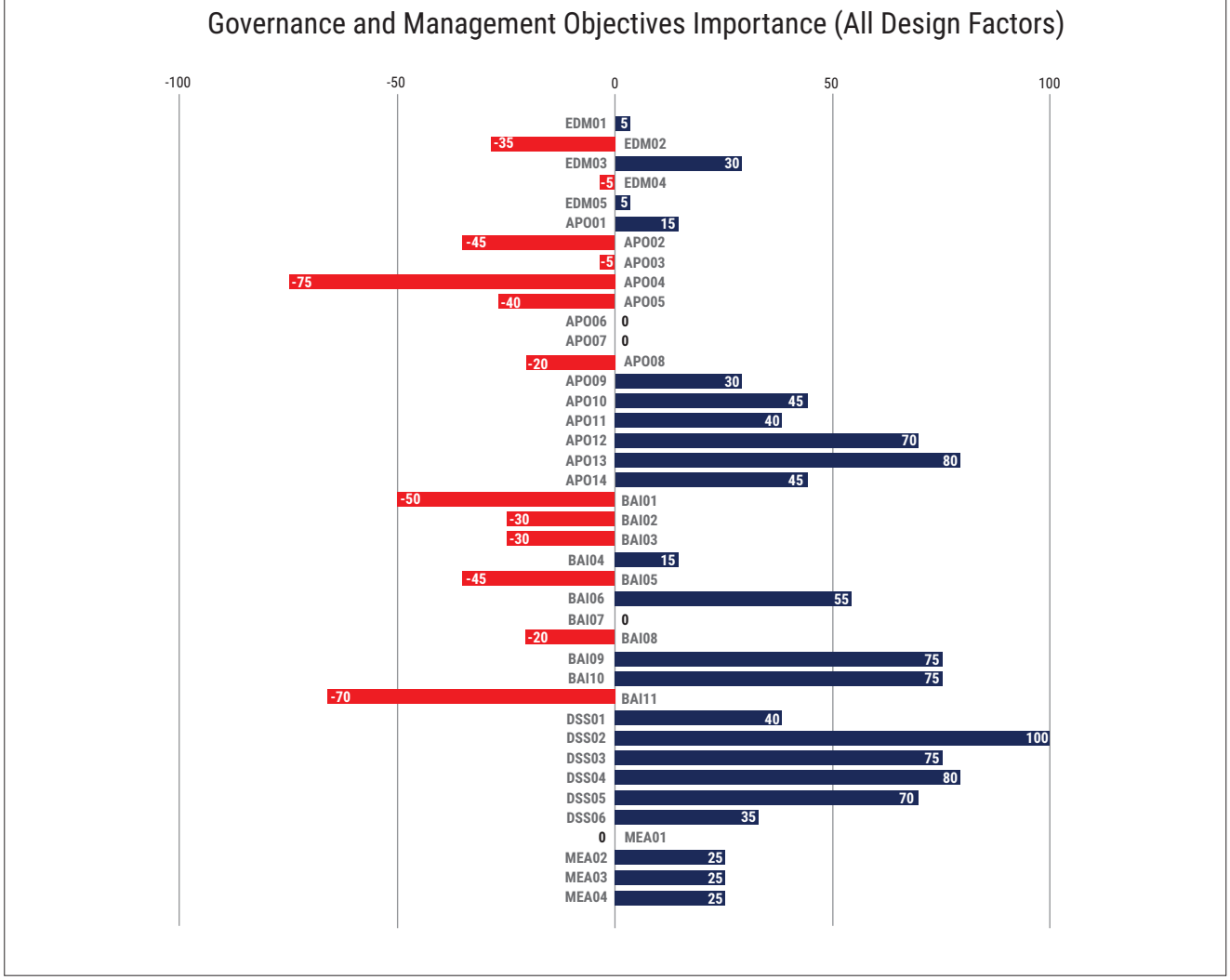
7.2.4 Step 4: Conclude the Governance Solution Design

The last step in the design process requires all inputs from previous steps to be discussed, conflicts resolved and a conclusion reached. The resulting governance system reflects careful consideration of all inputs, taking into account that these inputs were sometimes conflicting, and choices had to be made.

7.2.4.1 Governance and Management Objectives

At this point, it is possible to add the governance and management priorities resulting from steps 3.1 through 3.7 to the results obtained from the initial governance system design in steps 2.1 through 2.4. This synthesis results in the following adjusted priorities for governance and management objectives in the governance system **(figure 7.27)**.

Figure 7.27—Example 1, Step 4: Governance and Management Objectives Importance (All Design Factors)



The following management objectives are likely to be important for the governance system of this enterprise:

- DSS02 *Managed service requests and incidents* (100)
- APO13 *Managed security* (80)
- DSS04 *Managed continuity* (80)
- DSS03 *Managed problems* (75)
- BAI09 *Managed assets* (75)
- BAI10 *Managed configuration* (75)

The most important objectives have changed slightly compared to the list identified in the initial scope definition in step 2.5. Some governance/management objectives have changed places, one dropped (APO12), and two were added (DSS04 and APO13).

The following management objectives seem the least important:

- APO04 *Managed innovation*
- BAI11 *Managed projects*
- BAI01 *Managed programs*
- APO02 *Managed strategy*
- BAI05 *Managed organizational change*

Compared to the most important objectives, this list of the least important objectives changed even less from the list identified in the initial scope definition in step 2.5. This proves both that the initial scoping, based on the fundamental design factors, was already quite accurate, and also that accounting for other design factors resulted in additional adjustments.

In its discussions, the enterprise decides that the automatically generated importance values for some governance/management objectives are not what they should be, and makes the following adjustments:

- APO06 *Managed budget and cost*: +75
- EDM04 *Ensured resource optimization*: +75
- DSS02 *Managed service requests and incidents*: -25

In conclusion, the enterprise decides that the first stage of its governance system design will consist of the governance and management objectives (with the underlying processes) shown in **figure 7.28**.

Figure 7.28—Example 1, Governance and Management Objectives and Target Process Capability Levels

Reference	Governance/Management Objective	Target Process Capability Level
EDM03	Ensured risk optimization	2
EDM04	Ensured resource optimization	3
APO06	Managed budget and costs	4
APO09	Managed service level agreements	2
APO10	Managed vendors	2
APO11	Managed quality	2
APO12	Managed risk	3
APO13	Managed security	4
APO14	Managed data	2

Figure 7.28—Example 1, Governance and Management Objectives and Target Process Capability Levels *(cont.)*		
Reference	**Governance/Management Objective**	**Target Process Capability Level**
BAI06	Managed IT changes	3
BAI09	Managed assets	4
BAI10	Managed configuration	4
DSS01	Managed operations	2
DSS02	Managed service requests and incidents	4
DSS03	Managed problems	4
DSS04	Managed continuity	4
DSS05	Managed security services	3
DSS06	Managed business process controls	2
MEA02	Managed system of internal control	2
MEA03	Managed compliance with external requirements	2
MEA04	Managed assurance	2

Figure 7.28 shows the reference, governance or management objective title, and the target capability level at which the related processes should be implemented. Given the high importance of a number of processes, the target capability level has been set at a higher value (3 or 4). The logic applied by the enterprise was that:

- Any governance/management objective that scored 75 or higher—meaning that its importance was at least 75% higher compared to a benchmark situation—would require a capability level 4.
- Any governance/management objective that scored 50 or higher would require a capability level 3.
- Any governance/management objective that scored 25 or higher would require a capability level 2.

It is reasonable to consider that the remaining processes should reach capability level 1.

7.2.4.2 Other Components

The enterprise will need to pay specific attention to a strong implementation of the following roles and structures:

- Security strategy committee
- CISO

The enterprise will also ensure adequate security awareness throughout the enterprise, and implement important information items and flows (security policy and security strategy).

7.2.4.3 Specific Focus Area Guidance

The enterprise will use the following guidance to complement the COBIT core model:

- Information security focus area[36] guidance, given the high threat landscape and the results of the risk analysis and the current I&T-related issues
- DevOps and vendor management focus area[37] guidance, when and where applicable

[36] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, the information security focus area content was in development and not yet released.
[37] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, the DevOps focus area content was in development and not yet released, and the vendor management focus area is being contemplated as a potential future focus area.

7.3 Example 2: Medium-Sized Innovative Company

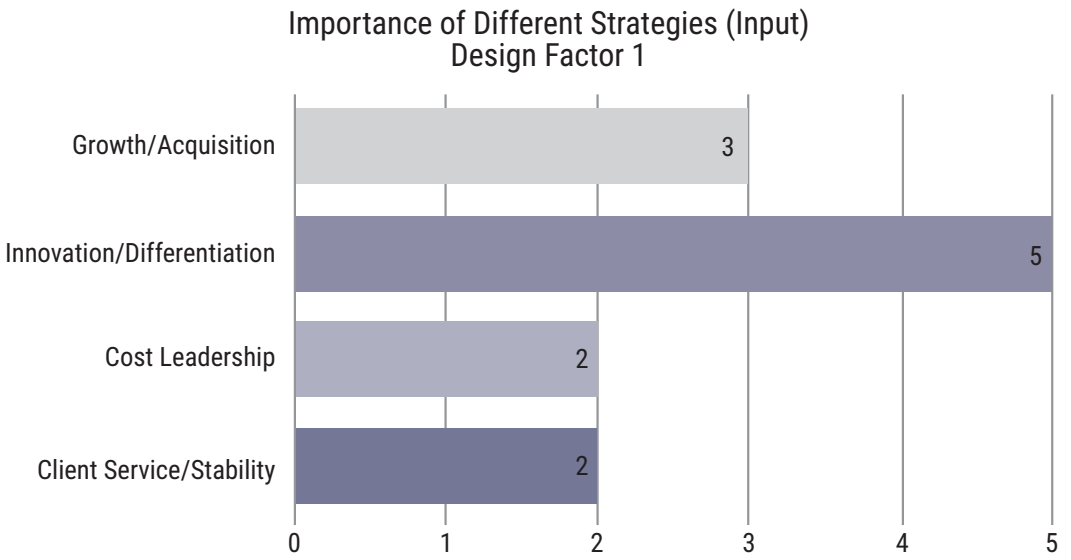
This example concerns a medium-sized innovative company, developing appliances for the automotive sector. The enterprise is relatively small, and its claim to fame is its fast innovation. It is critically dependent on IT for both product development and manufacturing of appliances. The enterprise is both a user and a developer of software. It is very eager to benefit from every newly available technology, and it is investing in a DevOps approach wherever possible. It has made a strategic choice to outsource all infrastructure-related IT services and go to the cloud.

7.3.1 Step 1: Understand the Enterprise Context and Strategy

The first step of the governance design workflow is to summarize the external and internal context of the enterprise.

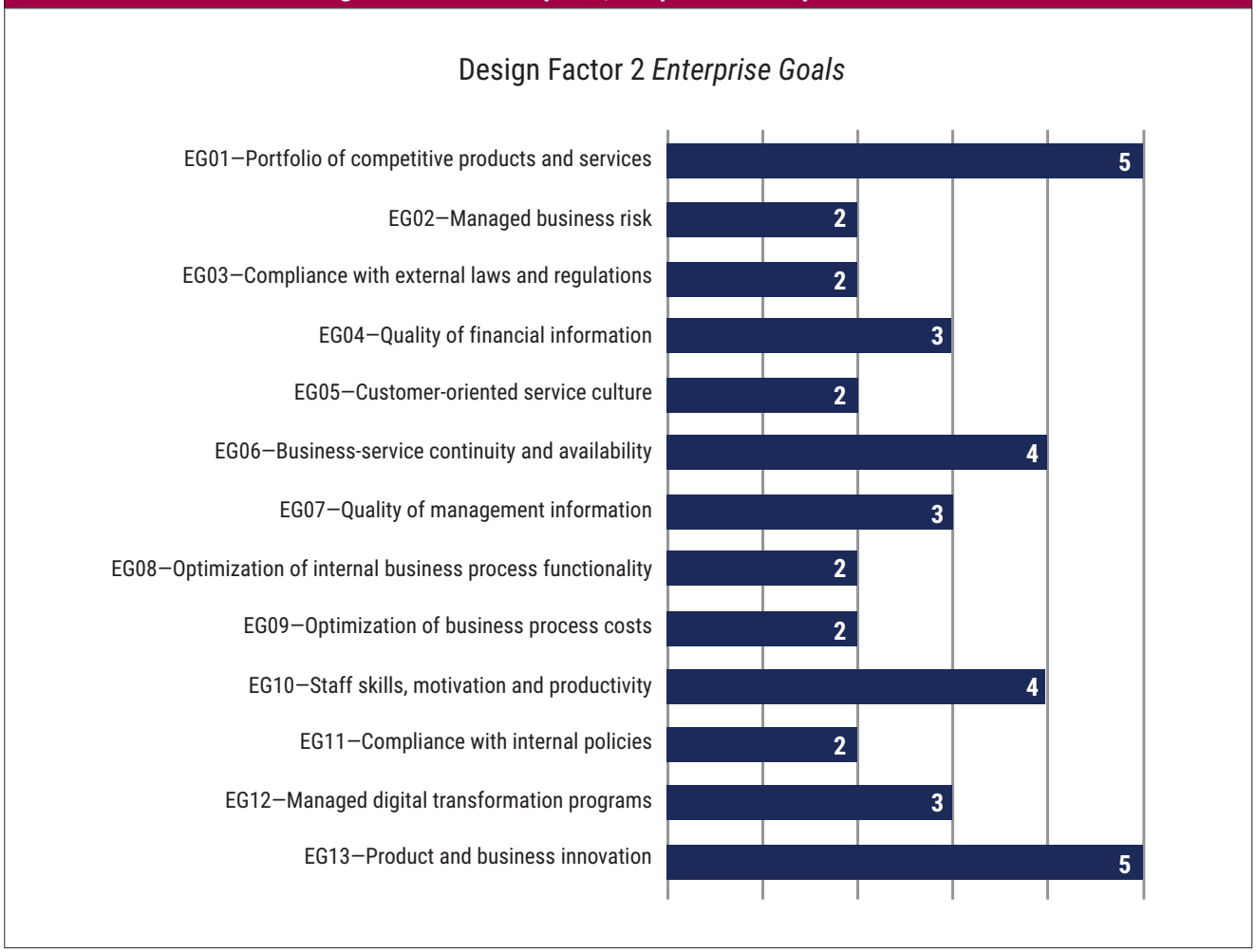
Step 1.1: Understand enterprise strategy—A primary focus on **innovation and differentiation** and a secondary focuson **growth/acquisition** are depicted in **figure 7.29**.

Figure 7.29—Example 2, Step 1.1: Enterprise Strategy



Step 1.2: Understand enterprise goals—The enterprise has ranked the 13 generic enterprise goals on a scale from 1 to 5, as depicted in **figure 7.30**. The diagram shows that EG01 *Portfolio of competitive products and services* and EG13 *Product and business innovation* are the highest-ranked enterprise goals.

Figure 7.30—Example 2, Step 1.2: Enterprise Goals



Step 1.3: Understand the risk profile—A high-level risk analysis resulted in a risk profile, identifying the highest risk categories (marked with red dots in the risk-rating column in **figure 7.31**: IT investment decision making, portfolio definition and maintenance; IT expertise, skills and behavior; and technology-based innovation. (These are broad categories. For detailed examples of risk scenarios within each category, please see Section 2.6.)

Figure 7.31—Example 2, Step 1.3: Risk Profile

Design Factor 3 *Risk Profile*

Risk Scenario Category	Impact (1-5)	Likelihood (1-5)	Risk Rating
IT investment decision making, portfolio definition and maintenance	5	3	●
Program and projects lifecycle management	4	2	●
IT cost and oversight	5	1	●
IT expertise, skills and behavior	4	4	●
Enterprise/it architecture	4	2	●
IT operational infrastructure incidents	4	2	●
Unauthorized actions	4	3	●
Software adoption/usage problems	3	2	●
Hardware incidents	4	2	●
Software failures	3	2	●
Logical attacks (hacking, malware, etc.)	3	4	●
Third-party/supplier incidents	4	2	●
Noncompliance	2	3	●
Geopolitical issues	2	2	●
Industrial action	2	1	●
Acts of nature	2	1	●
Technology-based innovation	5	3	●
Environmental	3	1	●
Data and information management	4	3	●

●	Very High Risk
●	High Risk
●	Normal Risk
●	Low Risk

Step 1.4: Understand current I&T-related issues—An analysis of the current situation (on a scale of importance from 1 to 3) resulted in an assessment of current I&T-related issues, as depicted in **figure 7.32**. The following are perceived to be important issues to the enterprise: insufficient IT resources, IT architecture and data quality issues.

Figure 7.32—Example 2, Step 1.4: I&T-Related Issues

Value	Importance (1-3)	*Baseline*
Frustration between different IT entities across the organization because of a perception of low contribution to business value	✔	*2*
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	✔	*2*
Significant IT-related incidents, such as data loss, security breaches, project failure and application errors, linked to IT	!	*2*
Service delivery problems by the IT outsourcer(s)	!	*2*
Failures to meet IT-related regulatory or contractual requirements	✔	*2*
Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems	✔	*2*
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	!	*2*
Duplications or overlaps between various initiatives, or other forms of wasted resources	✔	*2*
Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction	X	*2*
IT-enabled changes or projects frequently failing to meet business needs and delivered late or over budget	!	*2*
Reluctance by board members, executives or senior management to engage with IT, or a lack of committed business sponsorship for IT	!	*2*
Complex IT operating model and/or unclear decision mechanisms for IT-related decisions	✔	*2*
Excessively high cost of IT	!	*2*
Obstructed or failed implementation of new initiatives or innovations caused by the current IT architecture and systems	X	*2*
Gap between business and technical knowledge, which leads to business users and information and/or technology specialists speaking different languages	!	*2*
Regular issues with data quality and integration of data across various sources	X	*2*
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	✔	*2*
Business departments implementing their own information solutions with little or no involvement of the enterprise IT department	✔	*2*
Ignorance of and/or noncompliance with privacy regulations	✔	*2*
Inability to exploit new technologies or innovate using I&T	!	*2*

✔	No Issue
!	Issue
X	Serious Issue

7.3.2 Step 2: Determine the Initial Scope of the Governance System

The initial scope of the governance system is determined by using the information (partial or in full) collected during Step 1. Step 2 translates this information on enterprise strategy, enterprise goals, risk profile and I&T-related issues into relevant governance components.

Step 2.1: Consider enterprise strategy—**Figure 7.33** represents the enterprise strategy, as identified in step 1.1. **Figure 7.34** shows the relative influence these strategies have on governance and management objectives**.**

Figure 7.33—Example 2, Step 2.1: Enterprise Strategy

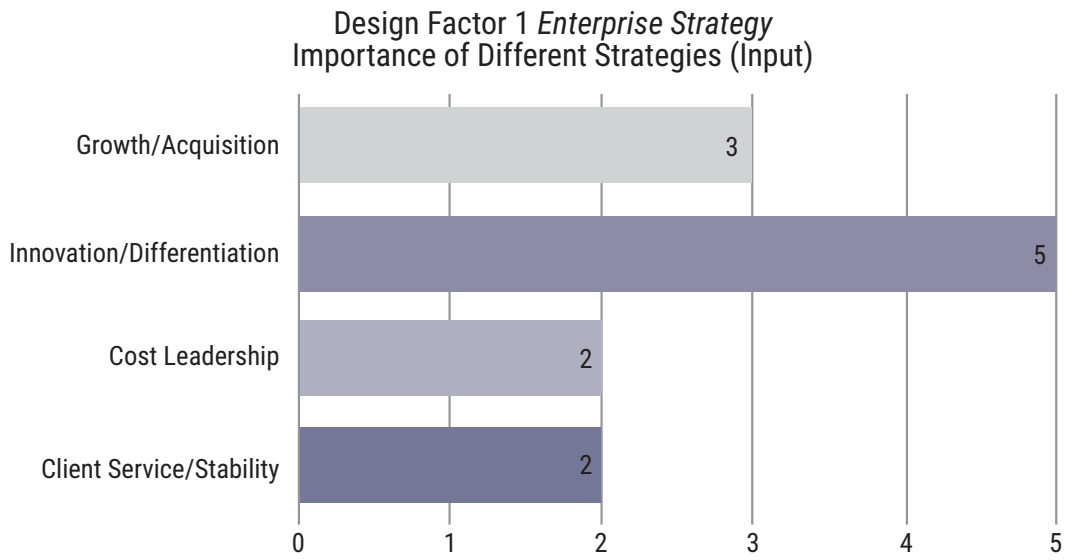
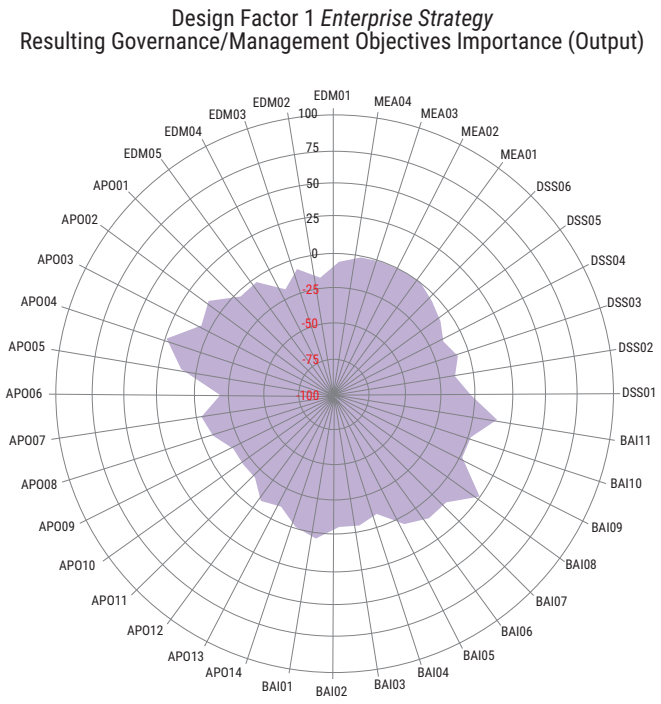


Figure 7.34—Example 2, Step 2.1: Resulting Governance/Management Objectives Importance for Design Factor 1 *Enterprise Strategy*



In addition to the governance and management processes highlighted by **figure 7.34**, the following other components also require attention:

- Support for the portfolio management role with the function responsible for overseeing all investments
- The roles of enterprise architect and chief digital officer
- A services, infrastructure and applications component to facilitate automation and growth, and to realize economies of scale
- Influence of culture and behavior component on innovation

Step 2.2: Consider enterprise goals and apply the COBIT goals cascade—At this point, the COBIT goals cascade can be applied to determine which governance and management objectives are relevant to achieve the priority enterprise goals, based on the ranking assigned in step 1.2 (**figure 7.35**). **Figure 7.36** shows the relative influence these ranked enterprise goals have on governance and management objectives.

Figure 7.35—Example 2, Step 2.2: Enterprise Goals

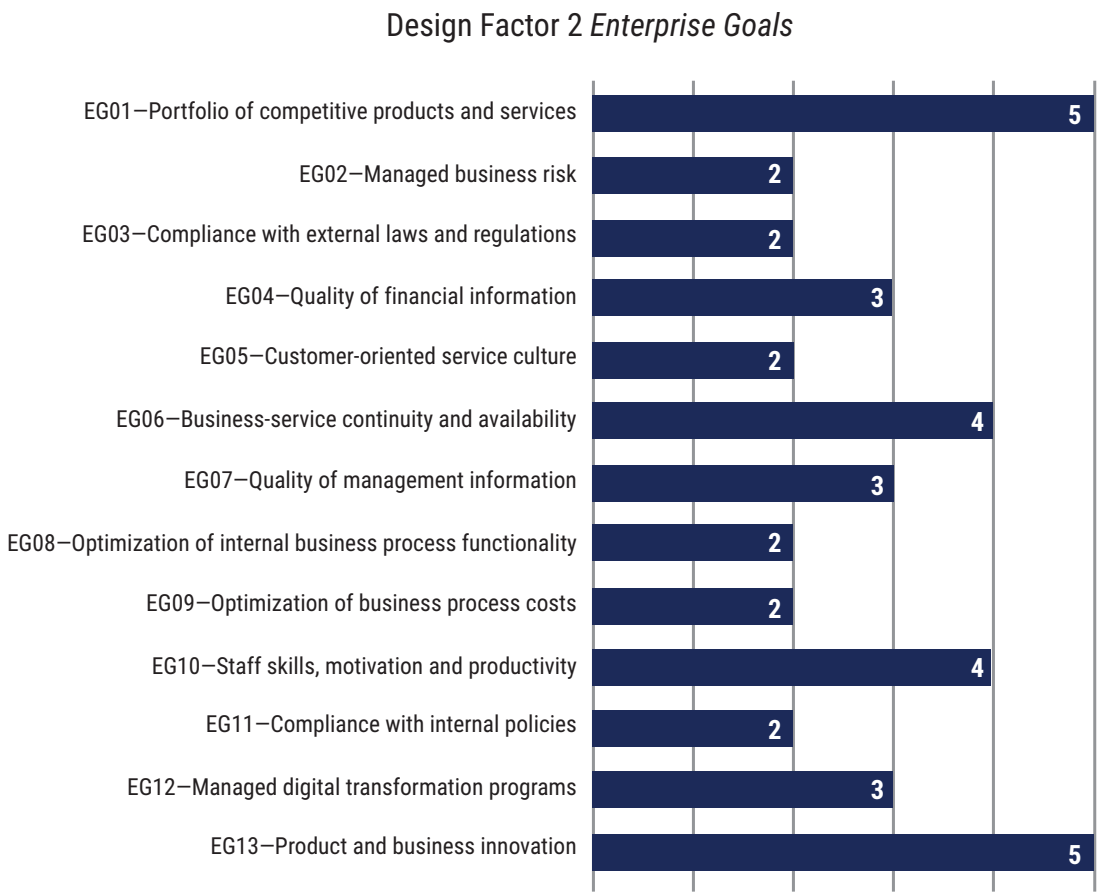
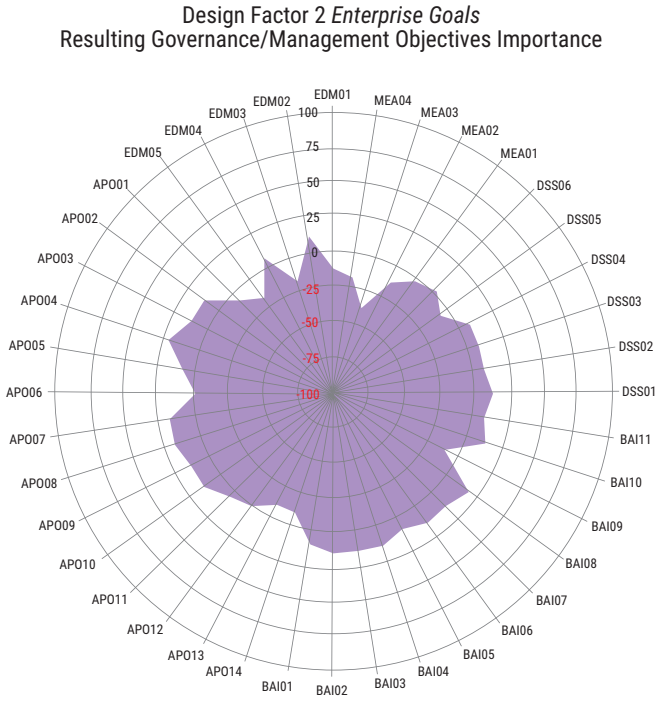


Figure 7.36—Example 2, Step 2.2: Resulting Governance/Management Objectives Importance for Design Factor 2 *Enterprise Goals*



Step 2.3: Consider the risk profile of the enterprise—In step 1.3, the IT risk categories were identified and analyzed at a high level (**figure 7.37**). Based on the mapping between the risk profile and the COBIT governance and management objectives (as explained in Section 4.2.3, and per the mapping table included in Appendix D), **figure 7.38** shows the relative ranking of the governance and management objectives, based on the results of the risk analysis.

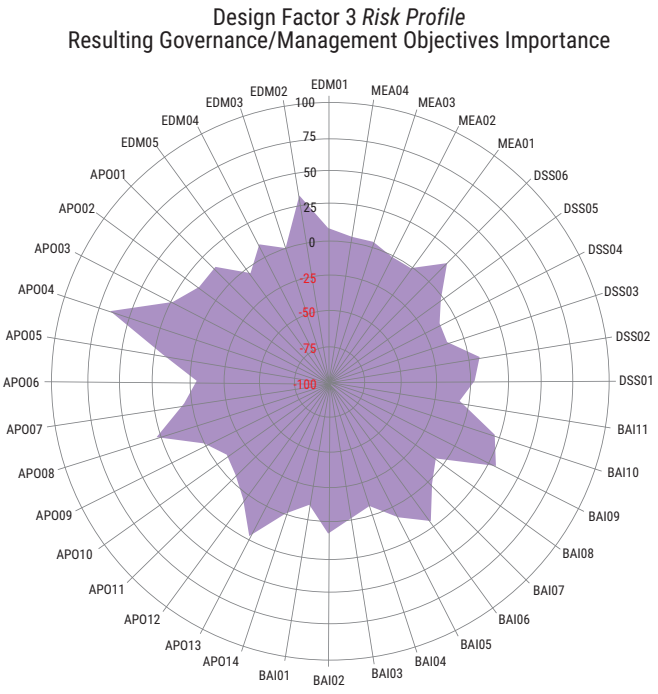
Figure 7.37—Example 2, Step 2.3: Risk Profile

Design Factor 3 *Risk Profile*

Risk Scenario Category	Impact (1-5)	Likelihood (1-5)	Risk Rating
IT investment decision making, portfolio definition and maintenance	5	3	●
Program and projects lifecycle management	4	2	●
IT cost and oversight	5	1	●
IT expertise, skills and behavior	4	4	●
Enterprise/it architecture	4	2	●
IT operational infrastructure incidents	4	2	●
Unauthorized actions	4	3	●
Software adoption/usage problems	3	2	●
Hardware incidents	4	2	●
Software failures	3	2	●
Logical attacks (hacking, malware, etc.)	3	4	●
Third-party/supplier incidents	4	2	●
Noncompliance	2	3	●
Geopolitical issues	2	2	●
Industrial action	2	1	●
Acts of nature	2	1	●
Technology-based innovation	5	3	●
Environmental	3	1	●
Data and information management	4	3	●

●	Very High Risk
●	High Risk
●	Normal Risk
●	Low Risk

Figure 7.38—Example 2, Step 2.3: Resulting Governance/Management Objectives Importance for Design Factor 3 *Risk Profile*



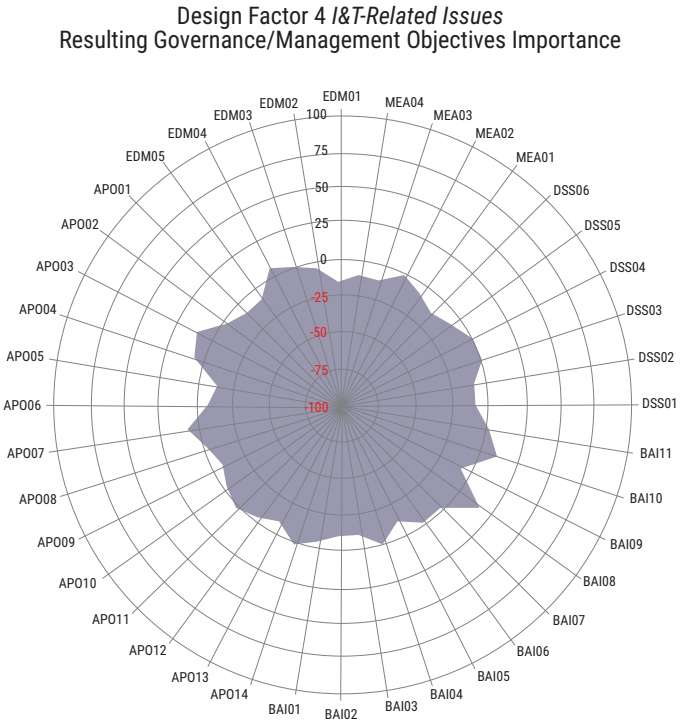
Step 2.4: Consider current I&T-related issues—In this step, the issues identified in step 1.4 are related to the COBIT governance and management objectives through a mapping table (**Appendix E**) that associates each issue to one or more governance or management objectives that can influence that issue. Based on the mapping (as explained in Section 4.2.4), **figure 7.40** shows the relative ranking of the governance and management objectives, based on the analysis of current I&T-related issues (**figure 7.39**).

Figure 7.39—Example 2, Step 2.4: I&T-Related Issues

Value	Importance (1-3)	*Baseline*
Frustration between different IT entities across the organization because of a perception of low contribution to business value	✔	*2*
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	✔	*2*
Significant IT-related incidents, such as data loss, security breaches, project failure and application errors, linked to IT	!	*2*
Service delivery problems by the IT outsourcer(s)	!	*2*
Failures to meet IT-related regulatory or contractual requirements	✔	*2*
Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems	✔	*2*
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	!	*2*
Duplications or overlaps between various initiatives, or other forms of wasted resources	✔	*2*
Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction	X	*2*
IT-enabled changes or projects frequently failing to meet business needs and delivered late or over budget	!	*2*
Reluctance by board members, executives or senior management to engage with IT, or a lack of committed business sponsorship for IT	!	*2*
Complex IT operating model and/or unclear decision mechanisms for IT-related decisions	✔	*2*
Excessively high cost of IT	!	*2*
Obstructed or failed implementation of new initiatives or innovations caused by the current IT architecture and systems	X	*2*
Gap between business and technical knowledge, which leads to business users and information and/or technology specialists speaking different languages	!	*2*
Regular issues with data quality and integration of data across various sources	X	*2*
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	✔	*2*
Business departments implementing their own information solutions with little or no involvement of the enterprise IT department	✔	*2*
Ignorance of and/or noncompliance with privacy regulations	✔	*2*
Inability to exploit new technologies or innovate using I&T	!	*2*

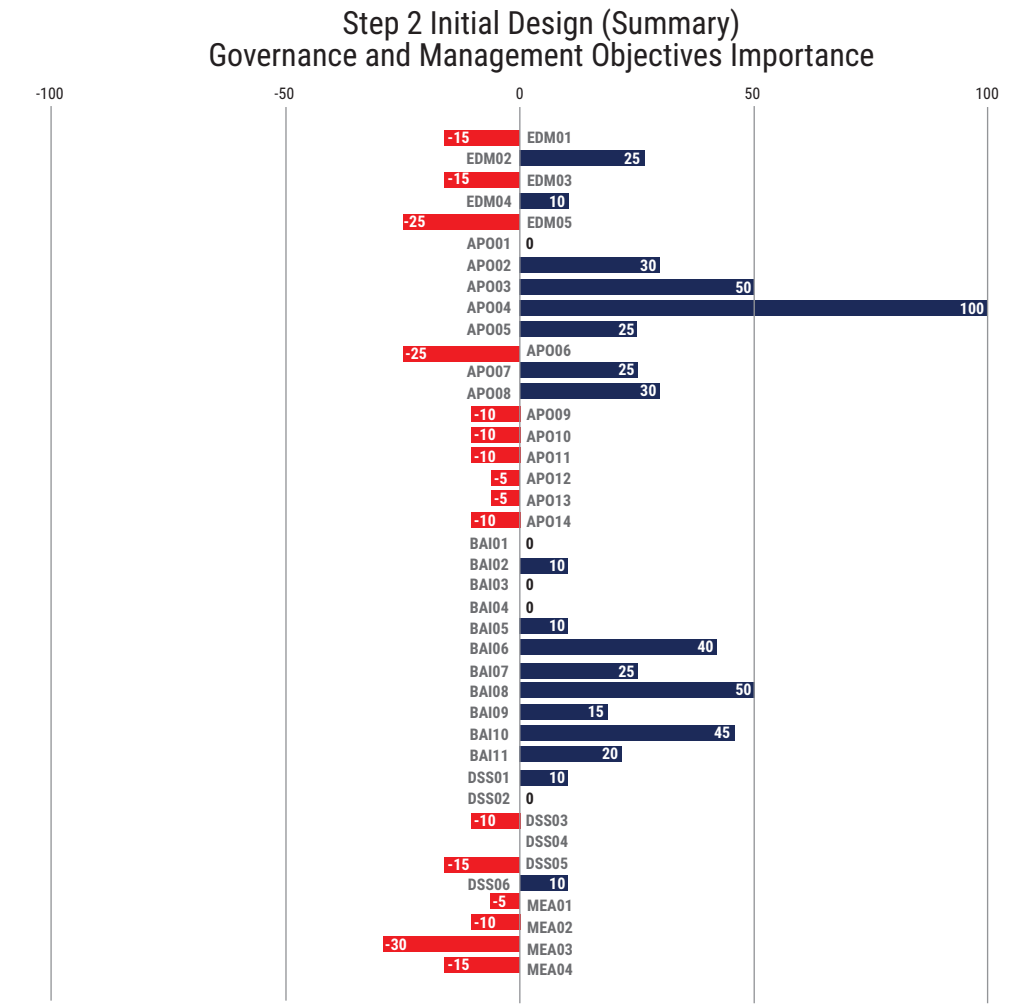
✔	No Issue
!	Issue
X	Serious Issue

Figure 7.40—Example 2, Step 2.4: Resulting Governance/Management Objectives Importance for Design Factor 4 *I&T-Related Issues*



Step 2.5: Initial scope of the governance system—At this point, it is possible to combine the resulting governance and management priorities from the previous steps to produce initial priorities for governance and management objectives in the governance system **(figure 7.41)**.

Figure 7.41—Example 2, Step 2.5: Initial Design Summary of Governance and Management Objectives Importance



The following management objectives are likely to be important for the governance system of this enterprise (top five):

- APO04 *Managed innovation*
- BAI08 *Managed knowledge*
- APO03 *Managed enterprise architecture*
- BAI10 *Managed configuration*
- BAI06 *Managed IT changes*

The following management objectives seem (for now) the least important:

- MEA03 *Managed compliance with external requirements*
- EDM05 *Ensured stakeholder engagement*
- APO06 *Managed budget and cost*
- EDM01 *Ensured governance framework setting and maintenance*
- EDM03 *Ensured risk optimization*
- DSS05 *Managed security services*

The next step will determine which refinements are required to this initial scope of the governance system.

7.3.3 Step 3: Refine the Scope of the Governance System

In step 3, refinements to the initial scope are identified, based on the remaining set of design factors to be analyzed. (Not all design factors are necessarily applicable to each enterprise, and therefore, some may be ignored.) **Figure 7.42** summarizes the design factors 5 through 11 that are applicable to the medium-sized innovation company in this example. When more than one value was applicable for a certain design factor, it is so indicated in the value column of the figure.

Figure 7.42—Governance System Scope Refinement Table Applied to Example 2

Ref	Design Factor	Value	Governance and Management Objectives Priority	Components	Focus Area Guidance
DF5	**Threat Landscape**				
	High	50%	Important governance and management objectives include: • EDM01, EDM03 • APO01, APO03, APO10, APO12, APO13, APO14 • BAI06, BAI10 • DSS02, DSS04, DSS05, DSS06 • MEA01, MEA03, MEA04	Important organizational structures include: • Security strategy committee • CISO Important culture and behavior aspects include: • Security awareness Information flows: • Security policy • Security strategy	Information security focus area[38]
	Normal	50%	• *As per the initial scope definition*	• *N/A*	COBIT core model
DF6	**Compliance Requirements**				
	Normal	100%	Important management objectives include: • EDM01, EDM03 • APO12 • MEA03, MEA04	• *N/A*	COBIT core model

[38] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, the information security focus area content was in development and not yet released.

Figure 7.42—Governance System Scope Refinement Table Applied to Example 2 *(cont.)*					
Ref	**Design Factor**	**Value**	**Governance and Management Objectives Priority**	**Components**	**Focus Area Guidance**
DF7	**Role of IT**				

	Strategic	5 on a scale of 5	Combination of strategic and factory mode (bimodal approach); see **figure 4.5** for governance and management objectives linked to factory and turnaround IT	Typical bimodal components, including:
				• Organizational structures
				  ▪ Chief digital officer
				• Skills and competencies
				  ▪ Staff who can work in an ambidextrous environment that combines both exploration and exploitation
				• Processes
				  ▪ A portfolio and innovation process that integrates exploration and exploitation of digital transformation opportunities
					Digital transformation focus area[39]

DF8	**Sourcing Model for IT**				
	Cloud	100%	Important management objectives include: • APO09, APO10 • MEA01	• *N/A*	Cloud focus area[40]
DF9	**IT Implementation Methods**				
	DevOps Agile Traditional	70% 15% 15%	Important governance and management objectives include: • BAI02, BAI03, BAI06	Important and specific roles as identified in the DevOps focus area guidance	DevOps focus area[41]
DF10	**Technology Adoption Strategy**				
	First Mover	100%	Important governance and management objectives include: • EDM01, EDM02 • APO02, APO04, APO05, APO08 • BAI01, BAI02, BAI03, BAI05, BAI07, BAI11 • MEA01	Processes that can run at a higher pace	DevOps focus area[41] Digital transformation focus area
DF11	**Enterprise Size**				
	Medium		• *As per the initial scope definition*	• *N/A*	SME Focus area

For each design factor in **figure 7.42**, the current assessed situation can be combined with the mapped governance and management objectives and other guidance in **figure 7.42**. The following examples were produced using matrix calculations between the input values and a mapping between these values and governance and management objectives. Mapping tables are included in Appendices F through K of this publication. The resulting spider charts, with the prioritized governance and management objectives, represent relative importance levels compared to a baseline level. Relative importance levels are expressed on a scale from -100 to +100, with zero (0) indicating that there is no impact on the importance of a governance or management objective, and +100 indicating that the objective has become twice as important due to the design factor at hand.

[39] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, the digital transformation focus area content was being contemplated as a potential future focus area.

[40] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, the cloud focus area content was being contemplated as a potential future focus area.

[41] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, the DevOps focus area content was in development and not yet released.

Step 3.1: Consider the current IT threat landscape—**Figure 7.43** depicts the threat landscape under which the enterprise believes it operates. **Figure 7.44** shows the impact on governance and management objectives of the assessed threat landscape.

Figure 7.43—Example 2, Step 3.1: Threat Landscape

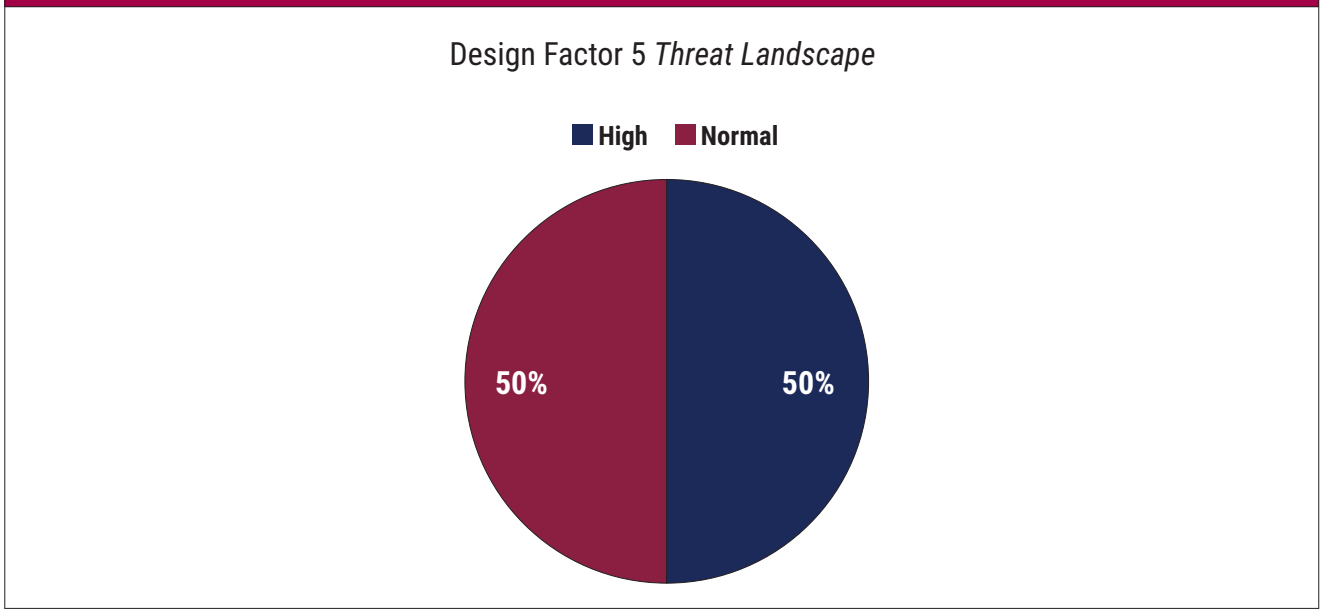
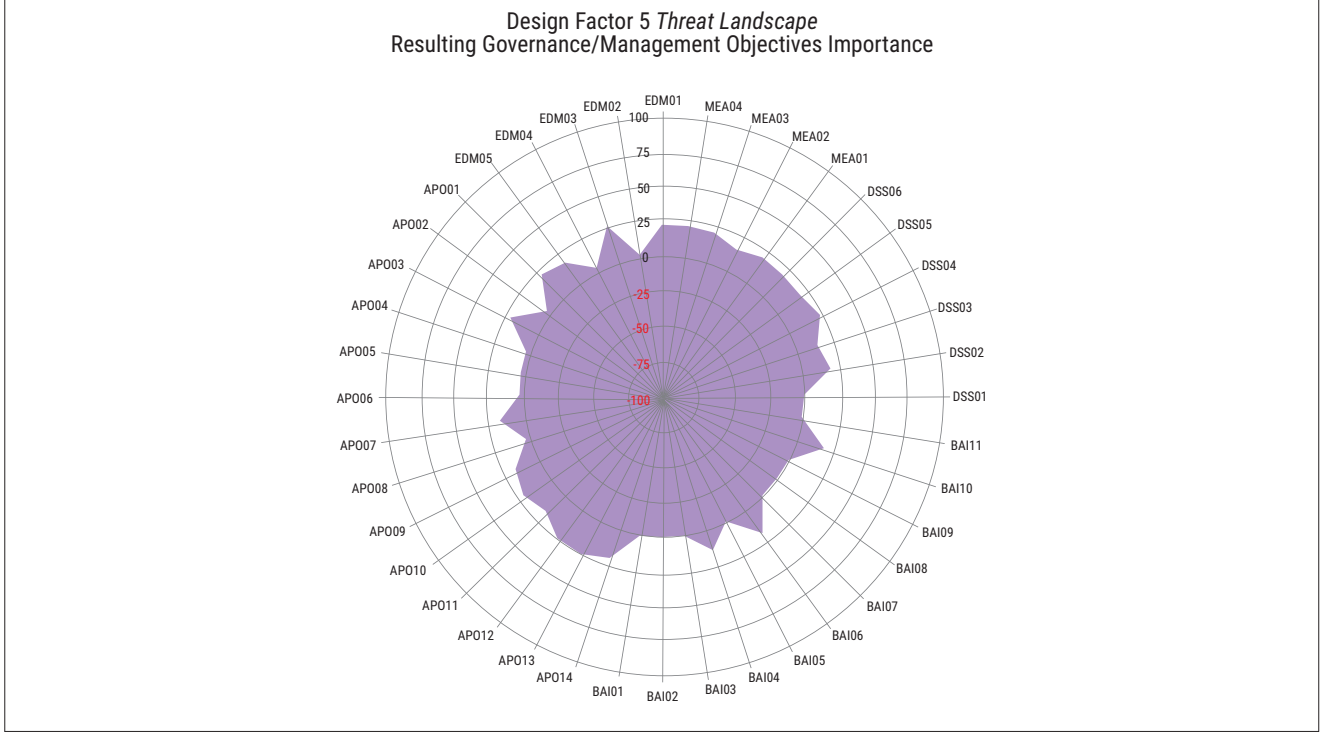


Figure 7.44—Example 2, Step 3.1: Resulting Governance/Management Objectives Importance for Design Factor 5 *Threat Landscape*



This classification of the threat landscape elevates the importance of a substantial number of governance and management objectives, per the entry in **figure 7.42** related to high threat landscape. Guidance on these governance and management objectives must be drawn from the information security focus area guidance, which contains more detailed and specific guidance on cybersecurity than does the COBIT core model.[42]

In addition, the enterprise must consider the following for inclusion in its governance system design:

- Important organizational structures, including:
  - Security strategy committee
  - CISO
- Important culture and behavior aspects, including:
  - Security awareness
- Information flows:
  - Security policy
  - Security strategy

[42] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, the information security focus area content was in development and not yet released.

Step 3.2: Consider compliance requirements—**Figure 7.45** depicts the compliance requirements for the enterprise, which are estimated to be normal. **Figure 7.46** shows the impact of the assessed compliance requirements on the governance and management objectives. There is no impact, which is the expected result, since normal is the baseline situation.

Figure 7.45—Example 2, Step 3.2: Compliance Requirements

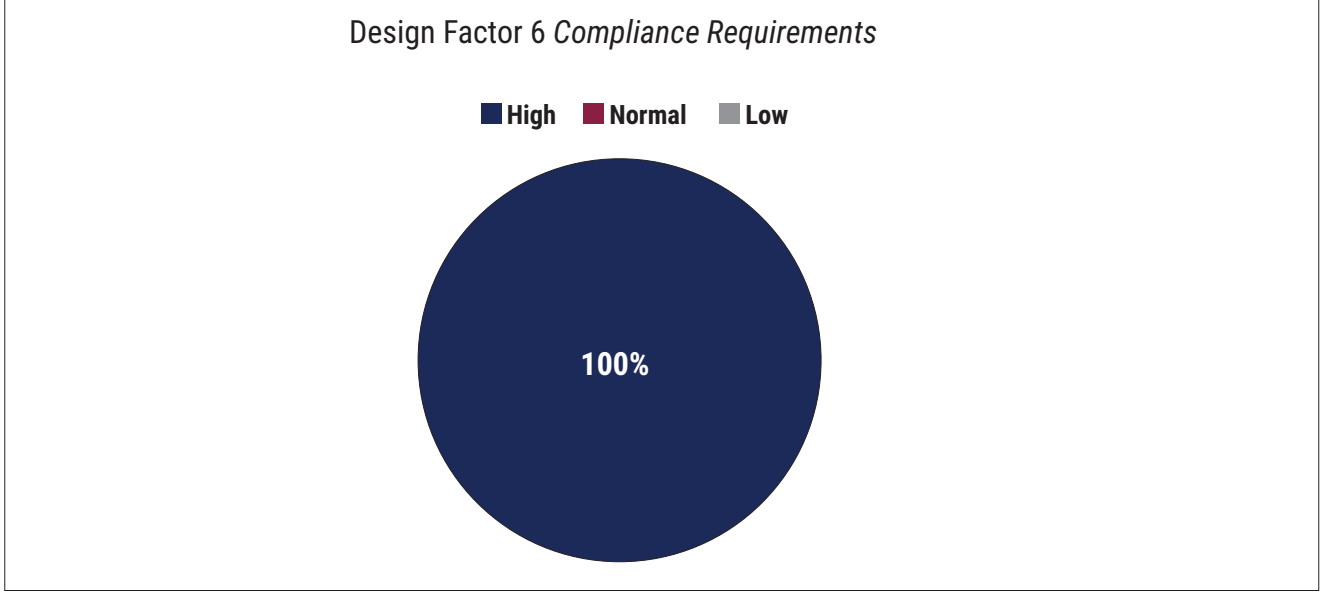
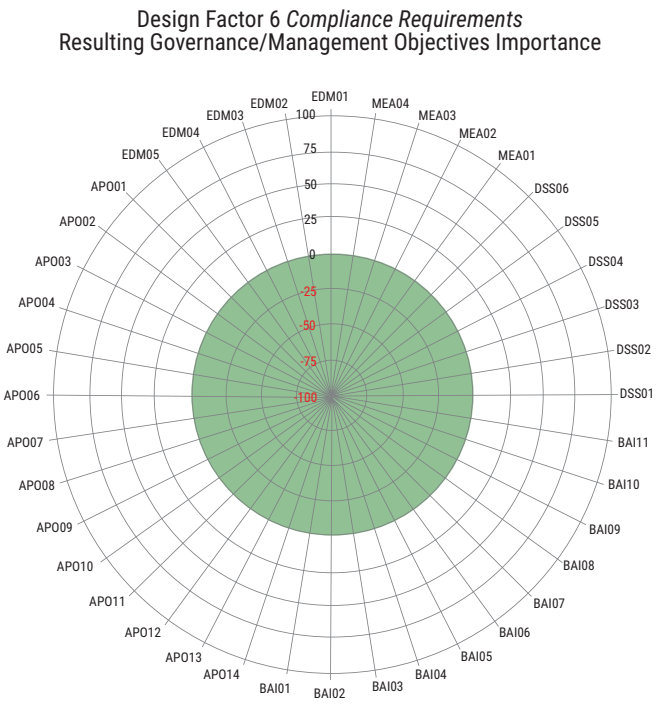


Figure 7.46—Example 2, Step 3.2: Resulting Governance/Management Objectives Importance for Design Factor 6 *Compliance Requirements*



Step 3.3: Consider the role of IT—**Figure 7.47** shows the role of IT, which is expressed as strategic. **Figure 7.48** shows the impact of the assessed role of IT on the governance and management objectives.

Figure 7.47—Example 2, Step 3.3: Role of IT

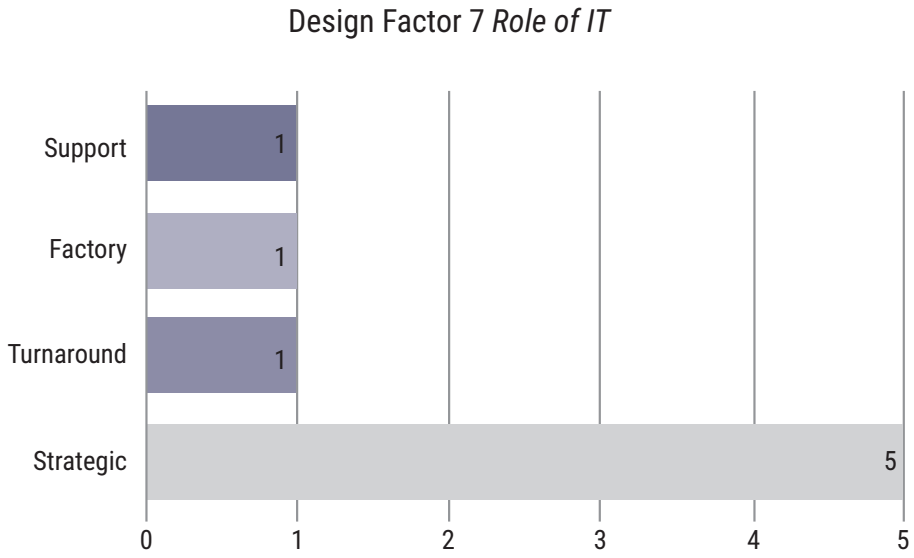
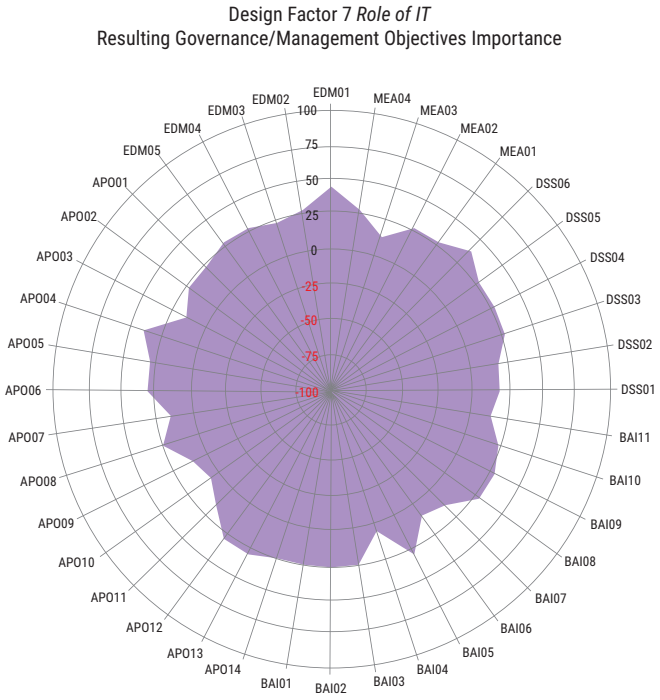


Figure 7.48—Example 2, Step 3.3: Resulting Governance/Management Objectives Importance for Design Factor 7 *Role of IT*



The enterprise must also consider the following typical bimodal components for inclusion in its governance system design:

- Organizational structures: chief digital officer
- Skills and competencies: staff who can work in an ambidextrous environment that combines both exploration and exploitation
- Processes: a portfolio and innovation process that integrates exploration and exploitation of digital transformation opportunities

In addition to the prioritized governance and management objectives, guidance should be drawn from the digital transformation focus area (when available).

Step 3.4: Consider the sourcing model for IT—**Figure 7.49** depicts the selected sourcing model of the enterprise, which is going fully cloud. **Figure 7.50** shows the impact of the assessed sourcing model on the governance and management objectives. The diagram shows that this impact is focused on three management objectives only. In addition, the enterprise will have to draw upon the cloud focus area guidance (when available).

Figure 7.49—Example 2, Step 3.4: Sourcing Model for IT

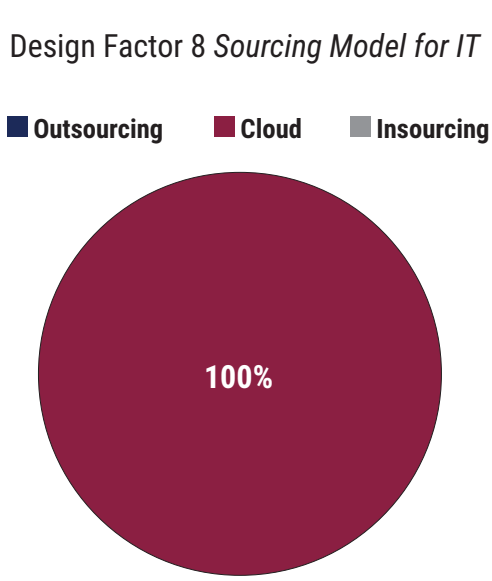
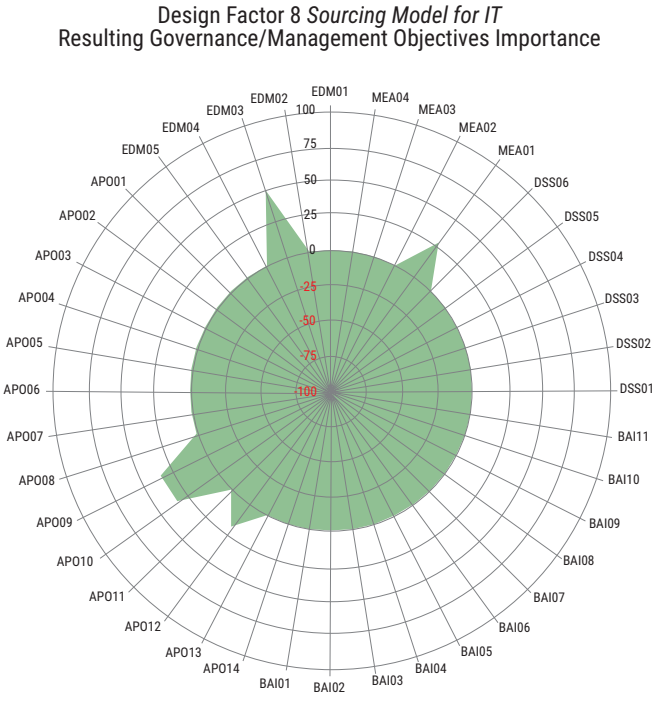


Figure 7.50—Example 2, Step 3.4: Resulting Governance/Management Objectives Importance for Design Factor 8 *Sourcing Model for IT*



Step 3.5: Consider IT implementation methods—The enterprise is using a mostly DevOps IT implementation method (see **figure 7.51**). **Figure 7.52** shows the impact this has on governance and management objectives. Guidance should be drawn from the DevOps management focus area, as indicated in **figure 7.42**.

Figure 7.51—Example 2, Step 3.5: IT Implementation Methods

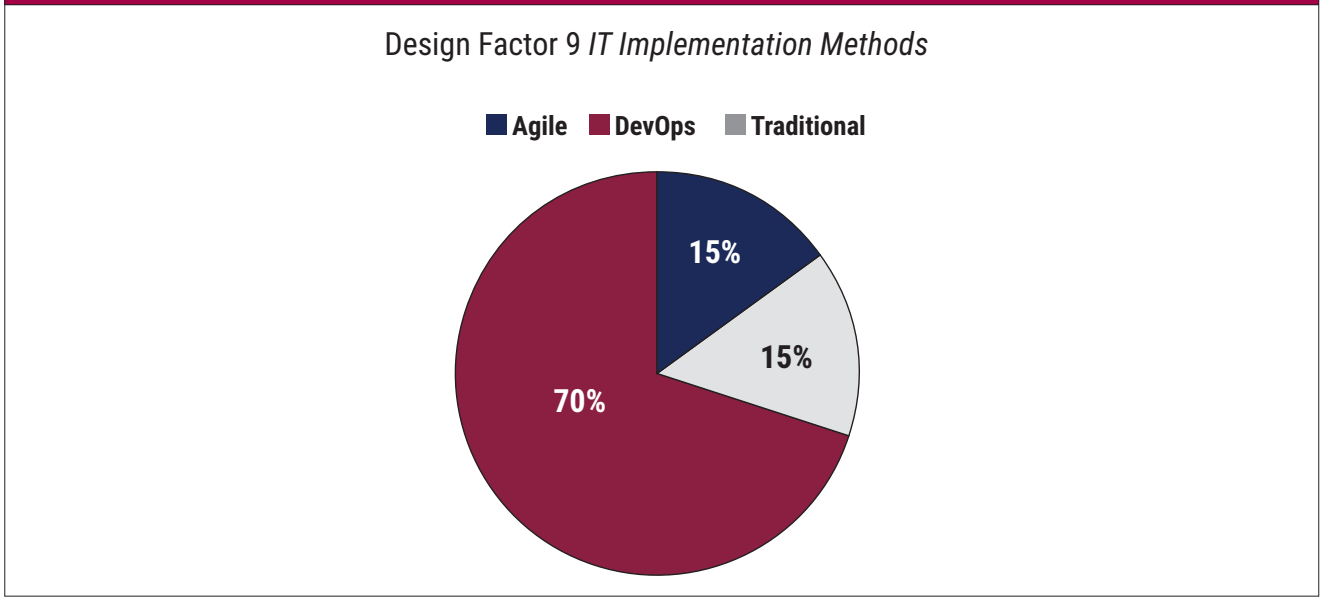
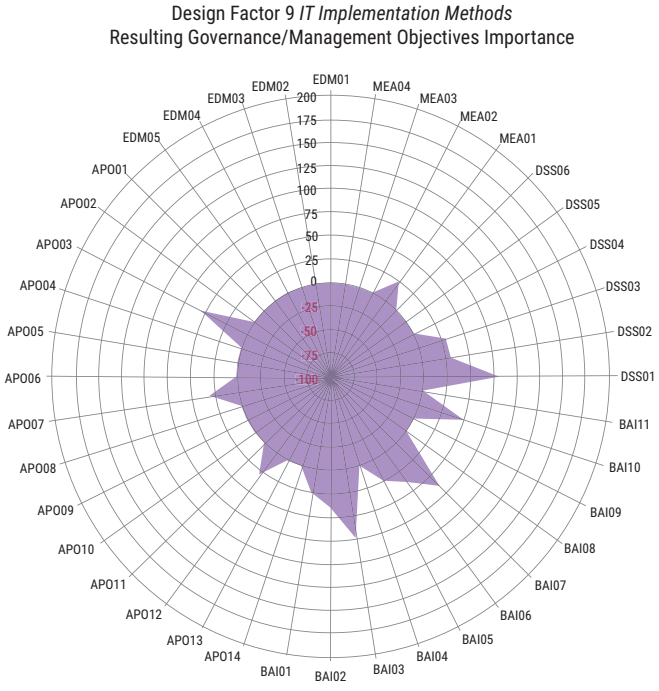


Figure 7.52—Example 2, Step 3.5: Resulting Governance/Management Objectives Importance for Design Factor 9 *IT Implementation Methods*



Step 3.6: Consider the technology adoption strategy—**Figure 7.53** indicates that the enterprise is a first mover when it comes to adopting new technology. **Figure 7.54** shows the impact this has on the governance and management objectives priorities.

Figure 7.53—Example 2, Step 3.6: Technology Adoption Strategy

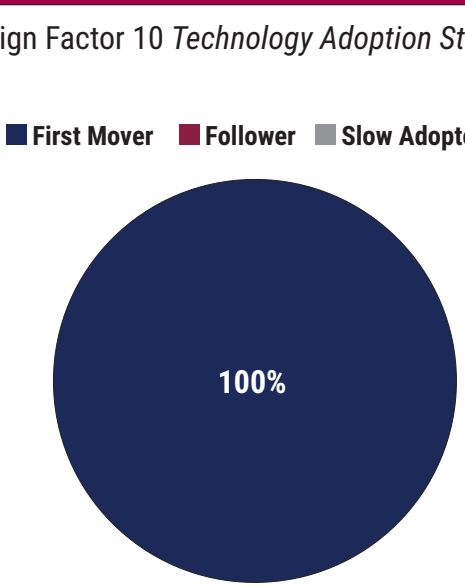


Figure 7.54—Example 2, Step 3.6: Resulting Governance/Management Objectives Importance for Design Factor 10 *Technology Adoption Strategy*

In addition to the prioritized governance and management objectives, guidance should be drawn from the digital transformation and DevOps focus areas (when available).

Step 3.7: Consider enterprise size—The enterprise is medium-sized. Per **figure 7.42**, this means that the small and medium enterprise focus area[43] should be used as the basis for the definition of the governance system.

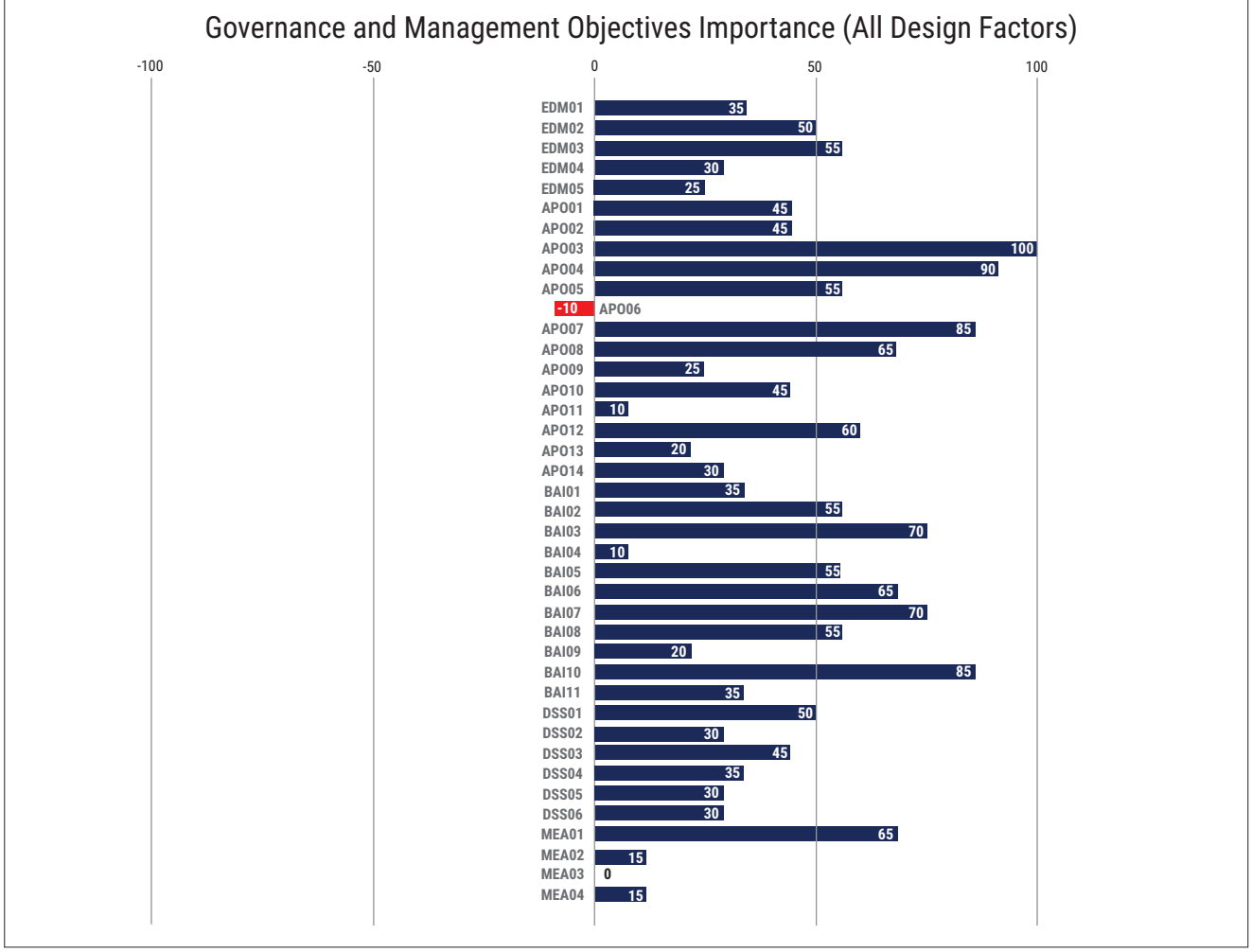
7.3.4 Step 4: Conclude the Governance Solution Design

The last step in the design process requires all inputs from previous steps to be discussed, conflicts resolved and a conclusion reached. The resulting governance system reflects careful consideration of all inputs, taking into account that these inputs were sometimes conflicting, and choices had to be made.

7.3.4.1 Governance and Management Objectives

At this point, it is possible to add the governance and management priorities resulting from steps 3.1 through 3.7 to the results obtained from the initial governance system design in steps 2.1 through 2.4. This synthesis results in the following adjusted priorities for governance and management objectives in the governance system (**figure 7.55)**.

Figure 7.55—Example 2, Step 4.1: Governance and Management Objectives Importance (All Design Factors)



[43] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, the small and medium enterprise focus area content was in development and not yet released.

The following management objectives are likely to be important for the governance system of this enterprise:

- APO03 *Managed enterprise architecture* (100)
- APO04 *Managed innovation* (90)
- APO07 *Managed human resources* (85)
- BAI10 *Managed configuration* (85)
- BAI03 *Managed solutions identification and build* (70)
- BAI07 *Managed IT change acceptance and transitioning* (70)

The most important objectives have changed slightly compared to the list identified in the initial scope definition in step 2.5.

The following management objectives seem the least important:

- APO06 *Managed budget and cost*
- MEA03 *Managed compliance with external requirements*
- APO11 *Managed projects*
- BAI04 *Managed availability and capacity*

When comparing this result to the initial scope, the following observations can be made:

- Overall, most governance/management objectives have gained significant importance after taking into account the additional design factors; this can be explained by the high threat landscape and strategic role of I&T.
- The governance/management objectives that ranked highest after the initial scope definition generally still rank high after scope refinement.

The enterprise decides that it is satisfied with the rating of governance and management objectives importance.

After discussion, the enterprise decides that the first stage of its governance system design will consist of the governance and management objectives (with the underlying processes) shown in **figure 7.56**.

Figure 7.56—Example 2 Governance and Management Objectives with Target Process Capability Levels

Reference	Governance/Management Objective	Target Process Capability Level
EDM01	Ensured governance framework setting and maintenance	2
EDM02	Ensured benefits delivery	3
EDM03	Ensured risk optimization	3
EDM04	Ensured resource optimization	2
EDM05	Ensured stakeholder engagement	2
APO01	Managed I&T management framework	2
APO02	Managed strategy	2
APO03	Managed enterprise architecture	4
APO04	Managed innovation	4
APO05	Managed portfolio	3
APO07	Managed human resources	4
APO08	Managed relationships	3
APO09	Managed service agreements	2
APO10	Managed vendors	2
APO12	Managed risks	3
APO14	Managed data	2

Figure 7.56—Example 2 Governance and Management Objectives with Target Process Capability Levels *(cont.)*		
Reference	**Governance/Management Objective**	**Target Process Capability Level**
BAI01	Managed programs	2
BAI02	Managed requirements definition	3
BAI03	Managed solutions identification and build	3
BAI05	Managed organizational change	3
BAI06	Managed IT changes	3
BAI07	Managed IT change acceptance and transitioning	3
BAI08	Managed knowledge	3
BAI10	Managed configuration	4
BAI11	Managed projects	2
DSS01	Managed operations	3
DSS02	Managed service requests and incidents	2
DSS03	Managed problems	2
DSS04	Managed continuity	2
DSS05	Managed security services	2
DSS06	Managed business process controls	2
MEA01	Managed performance and conformance monitoring	3

Figure 7.56 shows the reference, governance or management objective title, and the target capability level at which the related processes should be implemented. Given the high importance of a number of processes, the target capability level has been set at a higher value (3 or 4). The logic applied by the enterprise is the same used in Example 1:

- Any governance/management objective that scored 75 or higher—meaning that its importance was at least 75% higher than compared to a benchmark situation—would require a capability level 4.
- Any governance/management objective that scored 50 or higher would require a capability level 3.
- Any governance/management objective that scored 25 or higher would require a capability level 2.

7.3.4.2 Other Components

The enterprise will pay specific attention to a strong implementation of the following roles and structures (along with other components) of the governance system:

- Support for the portfolio management role with an investment office
- Roles of enterprise architect and chief digital officer
- A services, infrastructure and applications component to facilitate automation and growth, and realize economies of scale
- Influence of culture and behavior component for innovation
- Important organizational structures, including:
  - Security strategy committee
  - CISO
- Important culture and behavior aspects, including:
  - Security awareness

- Information flows:
  - Security policy
  - Security strategy
- Skills and competencies: staff who can work in an ambidextrous environment that combines both exploration and exploitation
- Processes: a portfolio and innovation process that integrates exploration and exploitation of digital transformation opportunities

7.3.4.3 Specific Focus Area Guidance

The enterprise will use the following guidance to complement the core COBIT guidance:

- The small and medium enterprise focus area guidance, because it is tailored for use by smaller organizations
- Information security focus area guidance, given the high threat landscape, and the results of the risk analysis and the current I&T-related issues
- DevOps, cloud and digital transformation focus area guidance, when and where applicable and available

7.4 Example 3: High-Profile Government Agency

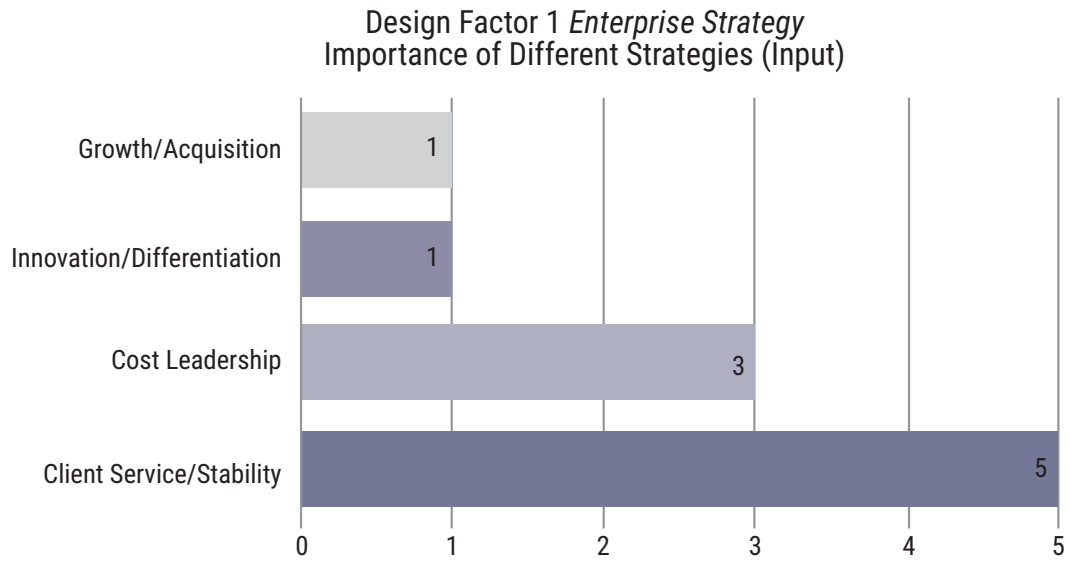
This case study shows the application of the workflow to design a tailored governance system for a high-profile, large government agency that provides healthcare, financial payments, education and other services to constituents needing assistance. Its operations are decentralized, with hospitals, clinics and offices in regions nationwide. Its I&T budget and planning and operations budget are spread among hospitals, financial benefits and other business units, with the IT shop providing infrastructure support, network operations and a security operations center. The agency considers I&T as critical to the success of the organization, and it must comply with laws and regulations, especially healthcare regulations that continue to emerge. It applies a traditional approach to new development and operations, and is hesitant to adopt new technologies. There is a very active audit function and dozens of significant findings exist related to how the agency protects its I&T, especially with respect to security and privacy. As a government agency, it is a major target of hackers and has just experienced a major hack of its entire beneficiary file.

7.4.1 Step 1: Understand the Enterprise Context and Strategy

The first step is to summarize the external and internal context of the agency.

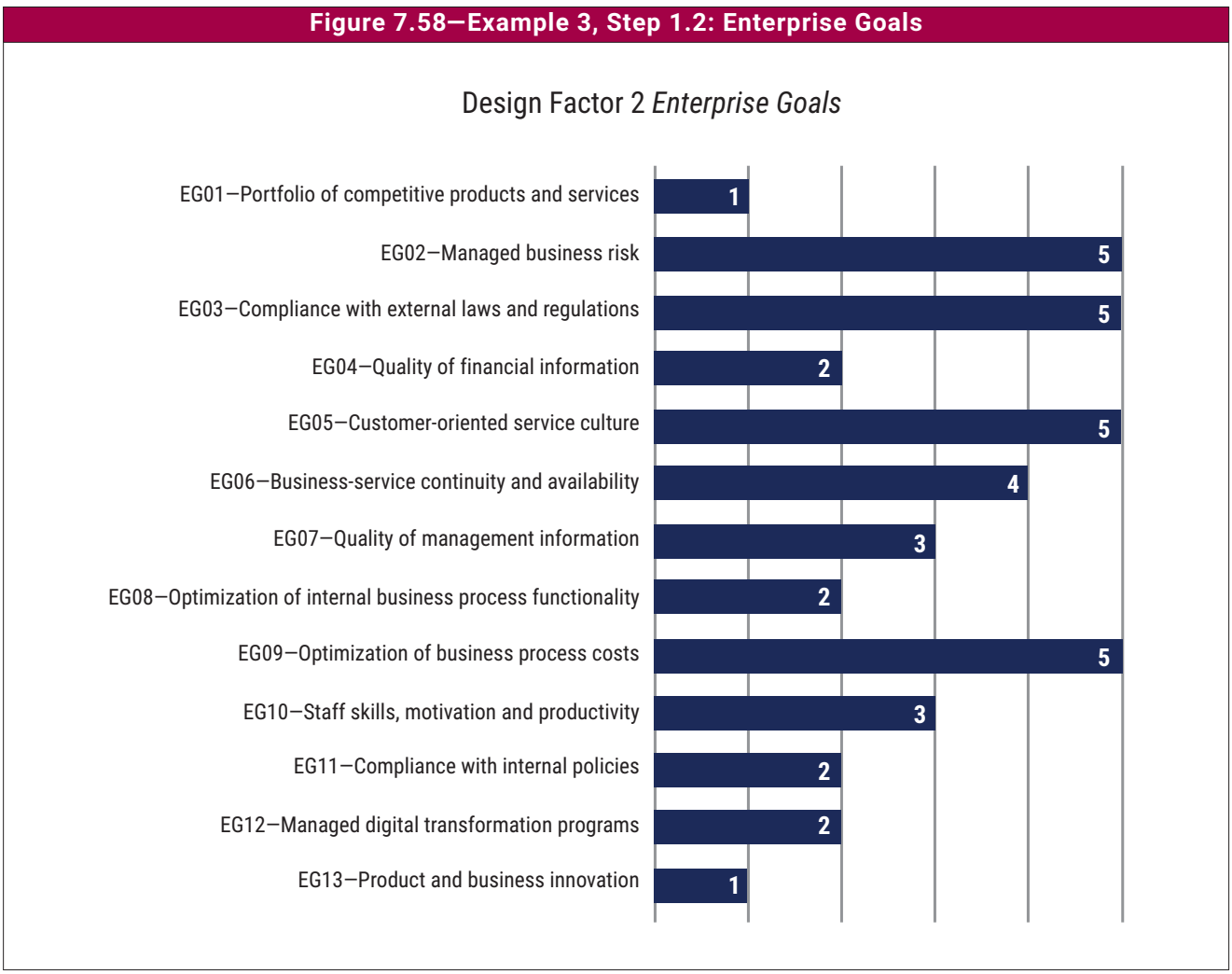
Step 1.1: Understand enterprise strategy—The agency's focus on providing outstanding services to constituents is reflected in **figure 7.57**.

Figure 7.57—Example 3, Step 1.1: Enterprise Strategy



Step 1.2: Understand enterprise goals—The agency has ranked the 13 generic enterprise goals on a scale from 1 to 5, as depicted in **figure 7.58**. The diagram shows that EG02 *Managed business risk,* EG03 *Compliance with external laws and regulations,* EG05 *Customer-oriented service culture* and EG09 *Optimization of business process costs* are the highest-ranked enterprise goals.

Figure 7.58—Example 3, Step 1.2: Enterprise Goals



Step 1.3: Understand the risk profile—A high-level risk analysis resulted in the risk profile shown in **figure 7.59**.

Figure 7.59—Example 3, Step 1.3: Risk Profile

Design Factor 3 *Risk Profile*

Risk Scenario Category	Impact (1-5)	Likelihood (1-5)	Risk Rating
IT investment decision making, portfolio definition and maintenance	4	4	●
Program and projects lifecycle management	4	4	●
IT cost and oversight	2	2	●
IT expertise, skills and behavior	4	4	●
Enterprise/it architecture	2	2	●
IT operational infrastructure incidents	4	4	●
Unauthorized actions	4	4	●
Software adoption/usage problems	3	3	●
Hardware incidents	2	2	●
Software failures	3	3	●
Logical attacks (hacking, malware, etc.)	4	5	●
Third-party/supplier incidents	2	2	●
Noncompliance	3	3	●
Geopolitical issues	2	2	●
Industrial action	1	3	●
Acts of nature	3	3	●
Technology-based innovation	4	3	●
Environmental	2	3	●
Data and information management	1	4	●

●	Very High Risk
●	High Risk
●	Normal Risk
●	Low Risk

Step 1.4: Understand current I&T-related issues—An analysis of the current situation resulted in the assessment of current I&T-related issues shown in **figure 7.60**.

Figure 7.60—Example 3, Step 1.4: I&T-Related Issues

Value	Importance (1-3)	*Baseline*
Frustration between different IT entities across the organization because of a perception of low contribution to business value	✗	2
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	✗	2
Significant IT-related incidents, such as data loss, security breaches, project failure and application errors, linked to IT	✗	2
Service delivery problems by the IT outsourcer(s)	!	2
Failures to meet IT-related regulatory or contractual requirements	!	2
Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems	✗	2
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	✗	2
Duplications or overlaps between various initiatives, or other forms of wasted resources	✗	2
Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction	✓	2
IT-enabled changes or projects frequently failing to meet business needs and delivered late or over budget	✗	2
Reluctance by board members, executives or senior management to engage with IT, or a lack of committed business sponsorship for IT	!	2
Complex IT operating model and/or unclear decision mechanisms for IT-related decisions	✗	2
Excessively high cost of IT	✓	2
Obstructed or failed implementation of new initiatives or innovations caused by the current IT architecture and systems	✓	2
Gap between business and technical knowledge, which leads to business users and information and/or technology specialists speaking different languages	✓	2
Regular issues with data quality and integration of data across various sources	✓	2
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	✗	2
Business departments implementing their own information solutions with little or no involvement of the enterprise IT department	✗	2
Ignorance of and/or noncompliance with privacy regulations	✓	2
Inability to exploit new technologies or innovate using I&T	!	2

✓	No Issue
!	Issue
✗	Serious Issue

7.4.2 Step 2: Determine the Initial Scope of the Governance System

The initial scope of the governance system is determined by using the information (partial or in full) collected during step 1. Step 2 translates this information on enterprise strategy, enterprise goals, risk profile and I&T-related issues into relevant governance components.

Step 2.1: Consider enterprise strategy—The following diagram represents the enterprise strategy, as identified in step 1.1 (**figure 7.61**). **Figure 7.62** shows the relative influence these strategies have on governance and management objectives**.**

Figure 7.61—Example 3, Step 2.1: Enterprise Strategy

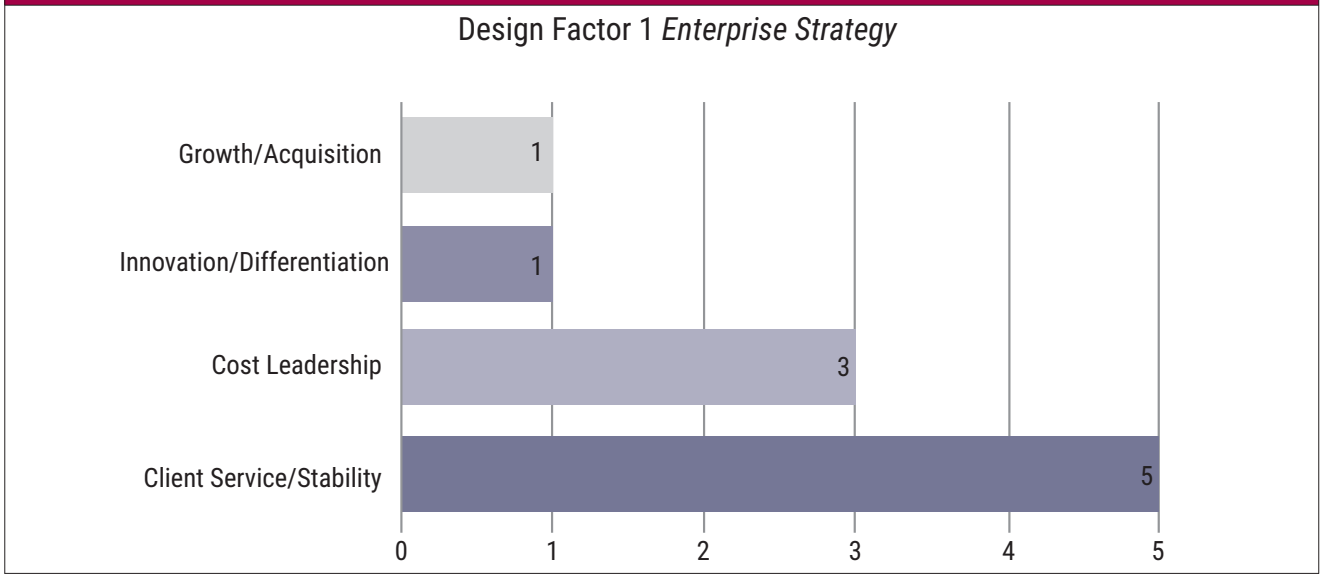
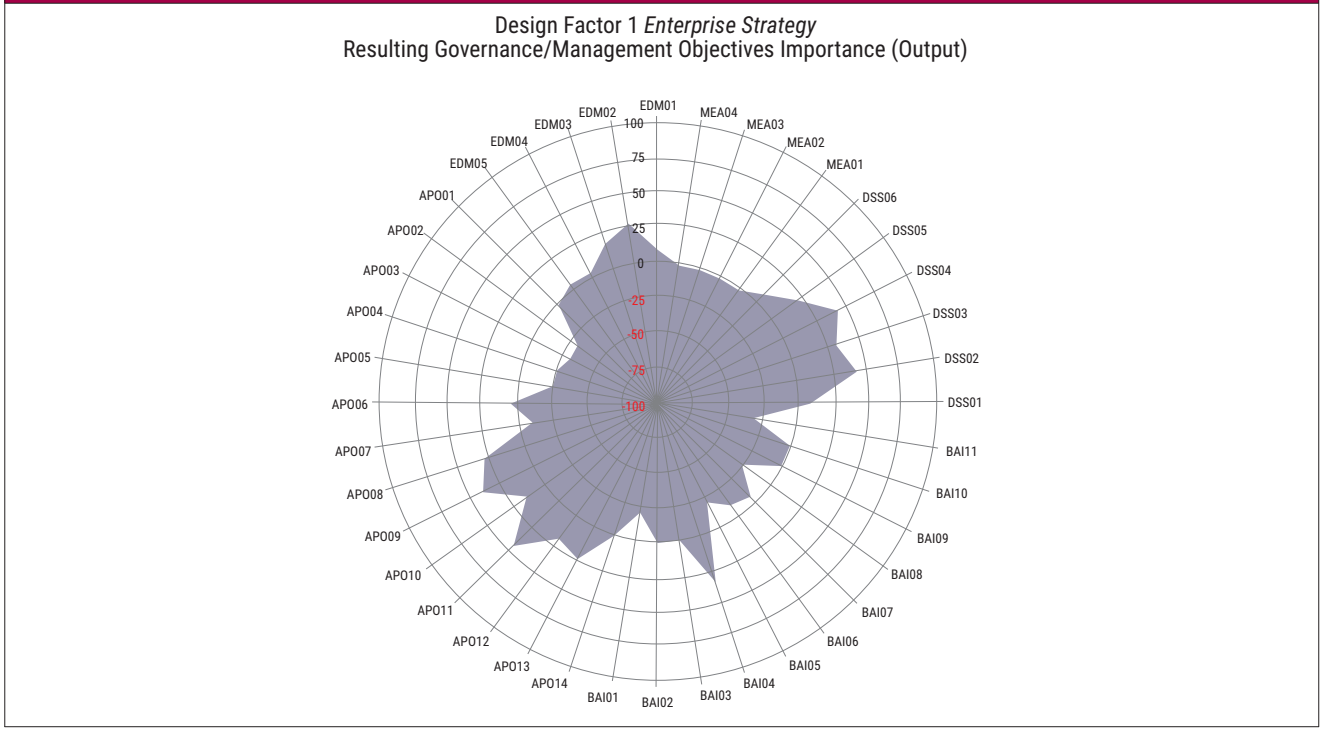


Figure 7.62—Example 3, Step 2.1: Resulting Governance/Management Objectives Importance for Design Factor 1 *Enterprise Strategy*



Step 2.2: Consider enterprise goals and apply the COBIT goals cascade—At this point, the COBIT goals cascade is applied to determine which governance and management objectives are relevant to achieve the priority enterprise goals, based on their ranking assigned in step 1.2 (**figure 7.63**). **Figure 7.64** shows the relative influence these ranked enterprise goals have on governance and management objectives.

Figure 7.63—Example 3, Step 2.2: Enterprise Goals

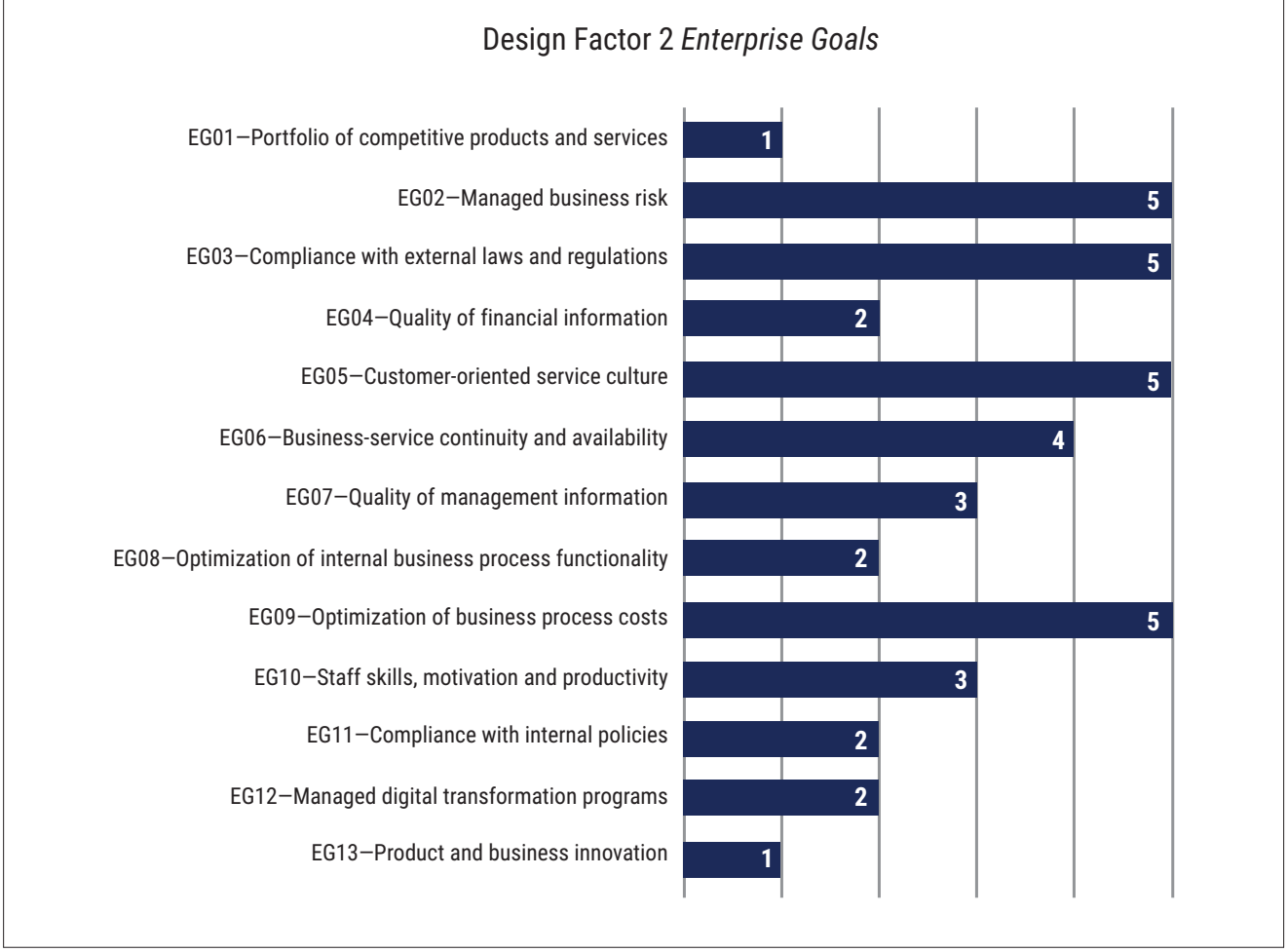


Figure 7.64—Example 3, Step 2.2: Resulting Governance/Management Objectives Importance for Design Factor 2 *Enterprise Goals*

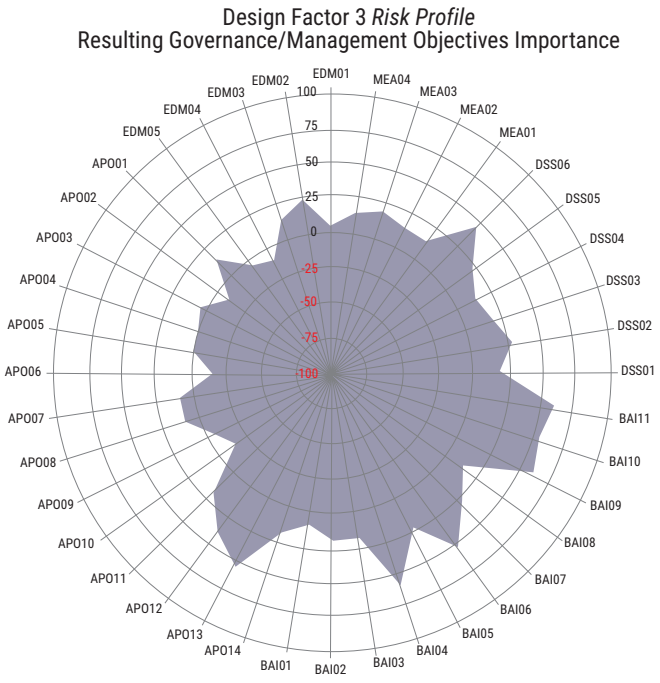
Step 2.3: Consider the risk profile of the enterprise—In step 1.3, IT risk categories were identified and analyzed at a high level (**figure 7.65**). Based on the mapping between the risk profile and the COBIT governance and management objectives (as explained in Section 4.2.3, and per the mapping table included in **Appendix D**), **figure 7.66** shows the relative ranking of the governance and management objectives based on the results of the risk analysis.

Figure 7.65—Example 3, Step 2.3: Risk Profile

Risk Scenario Category	Impact (1-5)	Likelihood (1-5)	Risk Rating
IT investment decision making, portfolio definition and maintenance	4	4	
Program and projects lifecycle management	4	4	
IT cost and oversight	2	2	
IT expertise, skills and behavior	4	4	
Enterprise/it architecture	2	2	
IT operational infrastructure incidents	4	4	
Unauthorized actions	4	4	
Software adoption/usage problems	3	3	
Hardware incidents	2	2	
Software failures	3	3	
Logical attacks (hacking, malware, etc.)	4	5	
Third-party/supplier incidents	2	2	
Noncompliance	3	3	
Geopolitical issues	2	2	
Industrial action	1	3	
Acts of nature	3	3	
Technology-based innovation	4	3	
Environmental	2	3	
Data and information management	4	4	

	Very High Risk
	High Risk
	Normal Risk
	Low Risk

Figure 7.66—Example 3, Step 2.3: Resulting Governance/Management Objectives Importance for Design Factor 3 *Risk Profile*



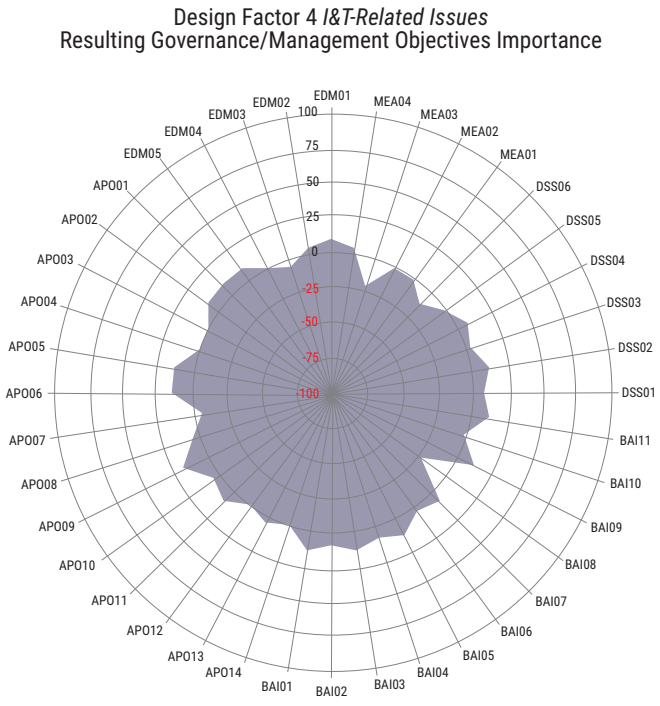
Step 2.4: Consider current I&T-related issues—In this step, the issues identified in step 1.4 are related to the COBIT governance and management objectives through a mapping table (**Appendix E**) that associates each issue to one or more governance or management objectives that can influence that issue (**figure 7.67**). Based on the mapping (as explained in Section 4.2.4), **Figure 7.68** shows the relative ranking of the governance and management objectives, based on the analysis of current I&T-related issues.

Figure 7.67—Example 3, Step 2.4: I&T-Related Issues

Value	Importance (1-3)	*Baseline*
Frustration between different IT entities across the organization because of a perception of low contribution to business value	✗	*2*
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	✗	*2*
Significant IT-related incidents, such as data loss, security breaches, project failure and application errors, linked to IT	✗	*2*
Service delivery problems by the IT outsourcer(s)	!	*2*
Failures to meet IT-related regulatory or contractual requirements	!	*2*
Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems	✗	*2*
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	✗	*2*
Duplications or overlaps between various initiatives, or other forms of wasted resources	✗	*2*
Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction	✓	*2*
IT-enabled changes or projects frequently failing to meet business needs and delivered late or over budget	✗	*2*
Reluctance by board members, executives or senior management to engage with IT, or a lack of committed business sponsorship for IT	!	*2*
Complex IT operating model and/or unclear decision mechanisms for IT-related decisions	✗	*2*
Excessively high cost of IT	✓	*2*
Obstructed or failed implementation of new initiatives or innovations caused by the current IT architecture and systems	✓	*2*
Gap between business and technical knowledge, which leads to business users and information and/or technology specialists speaking different languages	✓	*2*
Regular issues with data quality and integration of data across various sources	✓	*2*
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	✗	*2*
Business departments implementing their own information solutions with little or no involvement of the enterprise IT department	✗	*2*
Ignorance of and/or noncompliance with privacy regulations	✓	*2*
Inability to exploit new technologies or innovate using I&T	!	*2*

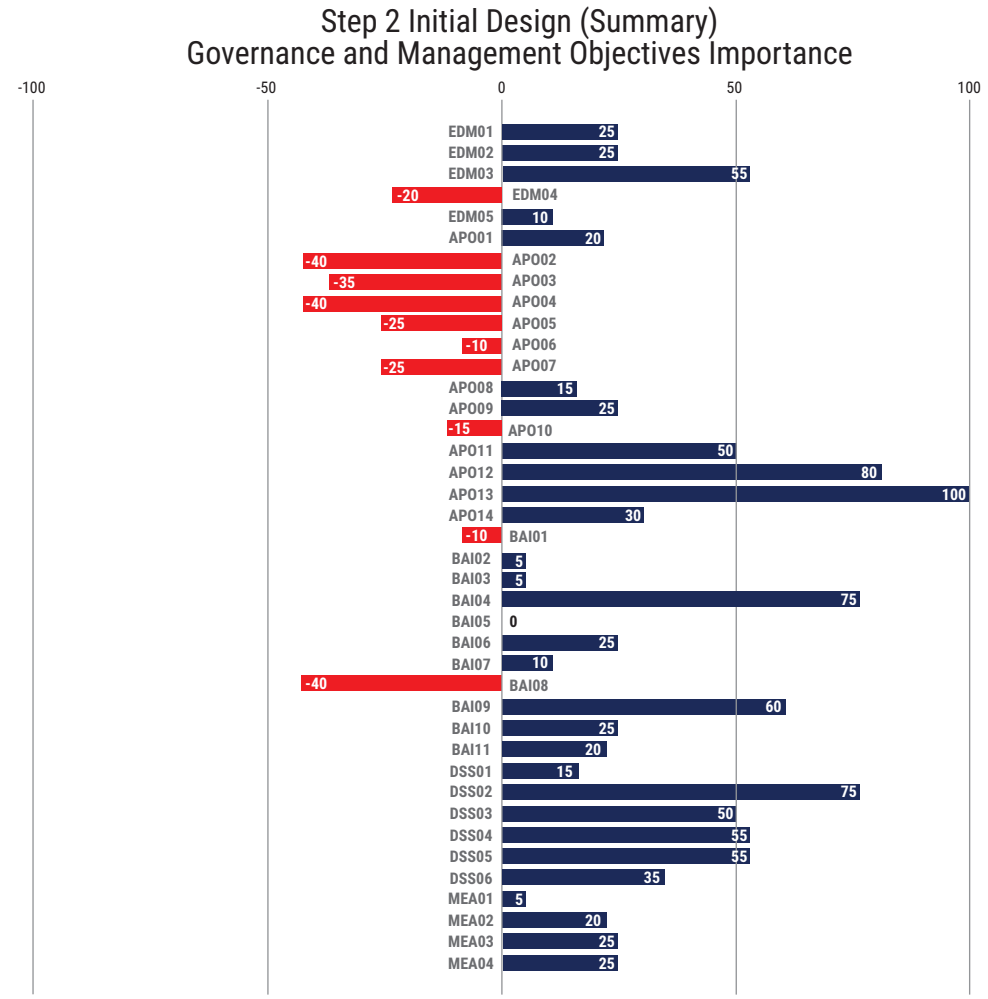
✓	No Issue
!	Issue
✗	Serious Issue

Figure 7.68—Example 3, Step 2.4: Resulting Governance/Management Objectives Importance for Design Factor 4 *I&T-Related Issues*



Step 2.5: Initial scope of the governance system—At this point, it is possible to combine the resulting governance and management priorities from the previous steps. The initial results were discussed with management, and adjusted for two management objectives: APO02 *Managed strategy* (whose priority increased) and APO09 *Managed service agreements* (whose priority decreased). These adjustments resulted in the following initial priorities for governance and management objectives in the governance system.

Figure 7.69—Example 3, Step 2.5: Initial Design Summary of Governance and Management Objectives Importance



The following governance and management objectives are likely to be important for the governance system of this agency, considering all governance and management objectives with a priority rating equal to or higher than 60:

- APO13 *Managed security* (100)
- APO12 *Managed risk* (80)
- DSS02 *Managed service requests and incidents* (75)
- BAI04 *Managed availability and capacity* (75)
- BAI09 *Managed assets* (60)

The following management objectives seem (for now) the least important (scoring less than -25):

- APO02 *Managed strategy*
- APO04 *Managed innovation*
- BAI08 *Managed knowledge*
- APO03 *Managed enterprise architecture*

The next step will determine which refinements are required to this initial scope of the governance system.

7.4.3 Step 3: Refine the Scope of the Governance System

In step 3, refinements to the initial scope are identified, based on the set of design factors included to be analyzed. Not all design factors might be applicable for each enterprise, in which case they can be ignored. **Figure 6.70** shows a summary of the design factors 5 through 11 that are applicable to the mid-sized innovation company in this example.When more than one value was applicable for a certain design factor, it is so indicated in the value column of the figure.

Figure 7.70—Governance System Scope Refinement Table Applied to Example 3

Ref	Design Factor	Value	Governance and Management Objectives Priority	Components	Focus Area Guidance
DF5	**Threat Landscape**				
	High	100%	Important governance and management objectives include: • EDM01, EDM03 • APO01, APO03, APO10, APO12, APO13, APO14 • BAI06, BAI10 • DSS02, DSS04, DSS05, DSS06 • MEA01, MEA03, MEA04	Important organizational structures include: • Security strategy committee • CISO Important culture and behavior aspects include: • Security awareness Information flows: • Security policy • Security strategy	Information security focus area[44]
DF6	**Compliance Requirements**				
	Low	100%	• *As per the initial scope definition*	• *N/A*	COBIT core model
DF7	**Role of IT**				
	Support	5 on a scale of 5	• *As per the initial scope definition*	• *N/A*	COBIT core model
DF8	**Sourcing Model for IT**				
	Insourced	100%	• *As per the initial scope definition*	• *N/A*	COBIT core model
DF9	**IT Implementation Methods**				
	Traditional	100%	• *As per the initial scope definition*	• *N/A*	COBIT core model
DF10	**Technology Adoption Strategy**				
	Follower	100%	Important governance and management objectives include: • APO02, APO04 • BAI01	Processes that can run at a slower pace	COBIT core model
DF11	**Enterprise Size**				
	Large		• *As per the initial scope definition*	• *N/A*	COBIT core model

[44] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, the Information security focus area content was in development and not yet released.

In both previous examples, the application of each Design Factor was fully detailed. This example does not include the detailed calculations and diagrams and presents only the end result. In addition to applying the design factors as explained in **figure 7.70**, the importance of aligning processes with their I&T strategy is stressed again.

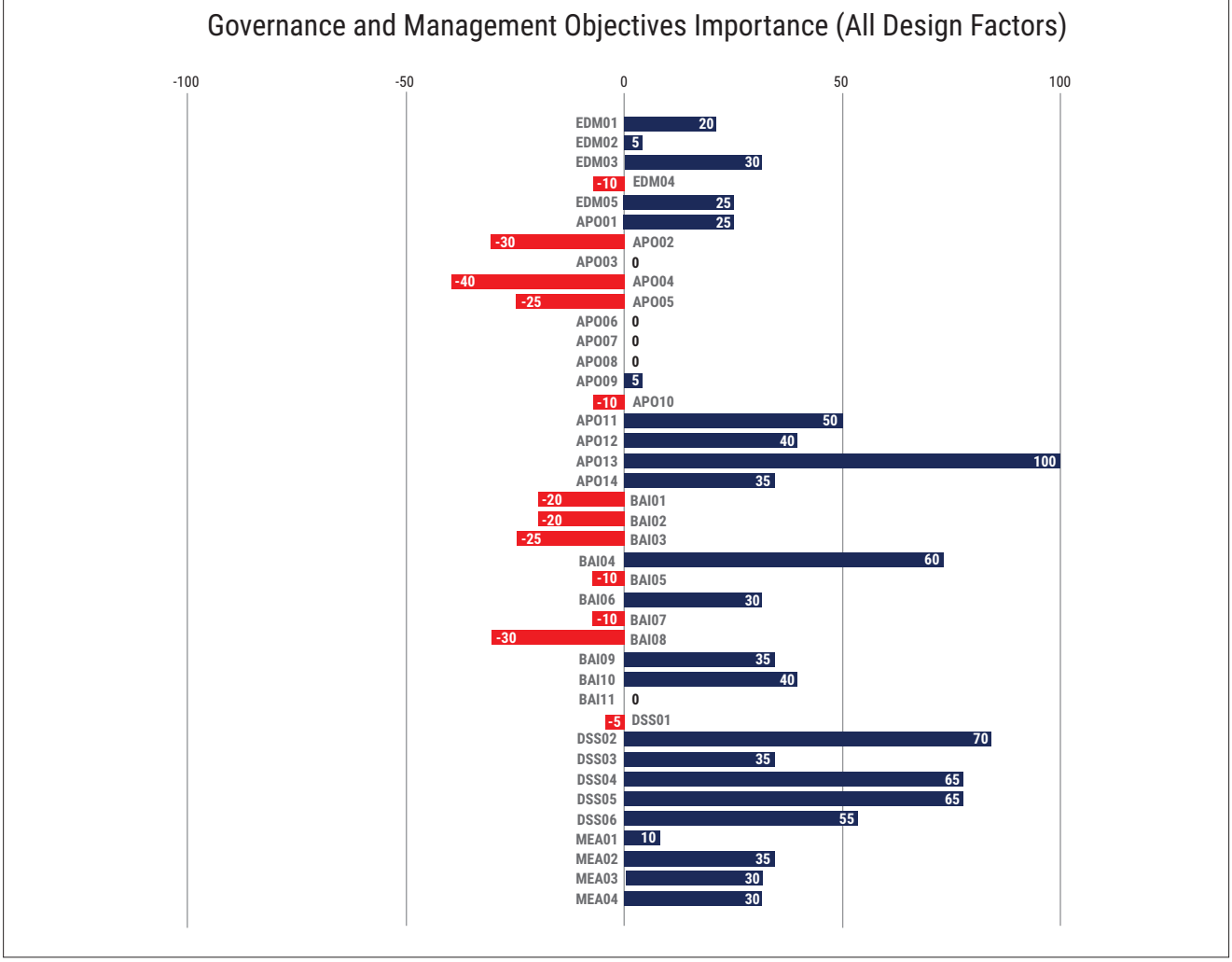
7.4.4 Step 4: Conclude the Governance Solution Design

The last step in the design process requires all inputs from previous steps to be discussed, conflicts resolved and a conclusion reached. The resulting governance system is the result of careful consideration of all inputs, taking into account that these inputs were sometimes conflicting and choices had to be made, including the discussion raising the importance of the APO02 *Managed strategy* objective.

7.4.4.1 Governance and Management Objectives

At this point, it is possible to combine the resulting governance and management priorities from steps 3.1 through 3.7 to the results obtained from the initial governance system design in steps 2.1 through 2.4. This results in the following adjusted priorities for governance and management objectives in the governance system.

Figure 7.71—Example 3, Step 4: Governance and Management Objectives Importance (All Design Factors)



The following governance and management objectives are likely to be important for the governance system of this agency, considering all governance and management objectives with a priority rating equal to or higher than 60:

- APO13 *Managed security* (100)
- DSS02 *Managed service requests and incidents* (70)
- DSS05 *Managed security services* (65)
- DSS04 *Managed continuity* (65)
- BAI04 *Managed availability and capacity* (60)

The following management objectives seem the least important (scoring less than -50):

- APO04 *Managed innovation* (-40)
- APO02 *Managed strategy* (-30)
- BAI08 *Manage knowledge* (-30)
- APO05 *Managed portfolio* (-25)
- BAI03 *Managed solutions identification and build* (-25)

The final result reflects several changes relative to priorities in the initial design (obtained after Step 2).

After discussion, the agency decided that its governance system design will consist of the prioritized list of governance and management objectives (with the underlying processes) shown in **figure 7.72**. The figure contains all the COBIT governance and management objectives, the suggested capability level based on the outcome of Step 3, and the actual decision management has taken about target capability levels.

Figure 7.72—Example 3 Governance and Management Objectives and Target Process Capability Levels

Reference	Governance/Management Objective	Suggested Target Process Capability Level	Decided Target Process Capability Level
EDM01	Ensured governance framework setting and maintenance	1	**3**
EDM02	Ensured benefits delivery	1	**3**
EDM03	Ensured risk optimization	2	**3**
EDM04	Ensured resource optimization	1	**3**
EDM05	Ensured stakeholder engagement	2	**3**
APO01	Managed IT management framework	2	**2**
APO02	Managed strategy	1	**3**
APO03	Managed enterprise architecture	1	**2**
APO04	Managed innovation	1	**1**
APO05	Managed portfolio	1	**3**
APO06	Managed budget and costs	1	**3**
APO07	Managed human resources	1	**2**
APO08	Managed relationships	1	**2**
APO09	Managed service agreements	1	**2**
APO10	Managed vendors	1	**2**
APO11	Managed quality	3	**3**
APO12	Managed risk	2	**4**
APO13	Managed security	4	**4**
APO14	Managed data	3	**4**
BAI01	Managed programs	1	**3**

Figure 7.72—Example 3 Governance and Management Objectives and Target Process Capability Levels *(cont.)*			
Reference	**Governance/Management Objective**	**Suggested Target Process Capability Level**	**Decided Target Process Capability Level**
BAI02	Managed requirements definition	1	**2**
BAI03	Managed solutions identification and build	1	**2**
BAI04	Managed availability and capacity	3	**2**
BAI05	Managed organizational change	1	**2**
BAI06	Managed IT changes	2	**2**
BAI07	Managed IT change acceptance and transitioning	1	**2**
BAI08	Managed knowledge	1	**1**
BAI09	Managed assets	2	**2**
BAI10	Managed configuration	2	**2**
BAI11	Managed projects	1	**3**
DSS01	Managed operations	1	**2**
DSS02	Managed service requests and incidents	3	**2**
DSS03	Managed problems	2	**2**
DSS04	Managed continuity	3	**2**
DSS05	Managed security services	3	**3**
DSS06	Managed business process controls	2	**3**
MEA01	Managed performance and conformance monitoring	1	**2**
MEA02	Managed system of internal control	2	**2**
MEA03	Managed compliance with external requirements	2	**2**
MEA04	Managed assurance	2	**2**

It is management's prerogative to define target levels that differ from the ones suggested by a (semi)automated approach, because mapping tables and generic goals and conditions may not always be suited to the enterprise's particular context. In **figure 7.72**, the suggested target capability level and the decided target level were identical—or varied by only one level—in almost 80 percent of the governance and management objectives.

The greatest deviations occurred in governance and management objectives related to cost and budgeting of IT, programs and projects, and strategy. Although the assessments of enterprise strategy, enterprise goals, risk, I&T issues and other design factors indicated lower priorities for governance and management objectives, management decided to give these objectives higher targets in order to address the agency's governance issues.

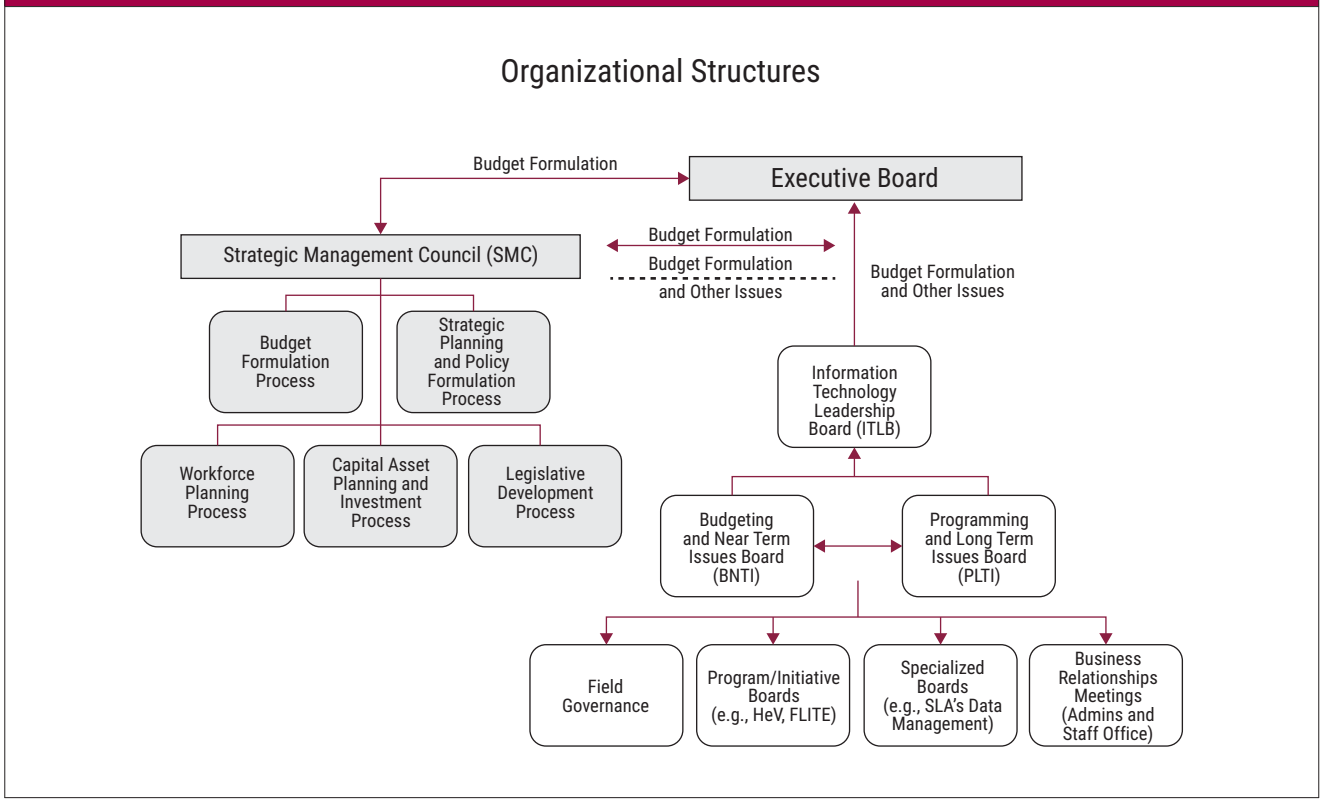
7.4.4.2 Other Components

The agency will pay specific attention to a strong implementation of the following roles and structures (along with other components) of the governance system:

- The agency will issue a top management policy expressing strong support for establishing an I&T governance structure, standards, policies and procedures, and for implementing the following structures and roles. (The actual I&T governance and organizational structures implemented by this high-profile large government agency follows in **figure 7.73**.)

- In terms of organizational structures, it was decided to implement the following roles:
  - Strategic management council
  - IT leadership board
  - Budgeting and near-term issues board
  - Programming and long-term issues board
  - Workforce planning process
  - Capital asset planning and investment process
  - Legislative development process

Figure 7.73—Example 3, Step 4: Organizational Structures



The agency will also ensure adequate risk, security and privacy awareness throughout the organization.

7.4.4.3 Specific Focus Area Guidance

The agency will use the following guidance to complement the core COBIT guidance:[45]

- Risk focus area content, given the high threat landscape, and the results of the risk analysis and current I&T issues
- Information security focus area guidance, given the high threat landscape, and the results of the risk analysis and the current I&T issues

[45] At the time of publication of the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, the risk and information security focus areas are in development and not yet released.

Page intentionally left blank

APPENDICES

The following appendices contain the mapping tables between the governance and management objectives and the design factors that were identified in Section 2.6.

The mappings express the degree to which design factor values influence the importance of a governance or management objective.

The mappings use a scale from zero (0) to four (4): 4 indicates the most influence, and 0 indicates the absence of any relationship.

Example: When an enterprise selects growth strategy for DF2 *Enterprise strategy*, the Appendix A mapping shows that management objective APO03 *Managed enterprise architecture* will be very important (a value of 4).

Appendix A: Mapping Table—Enterprise Strategies to Governance and Management Objectives

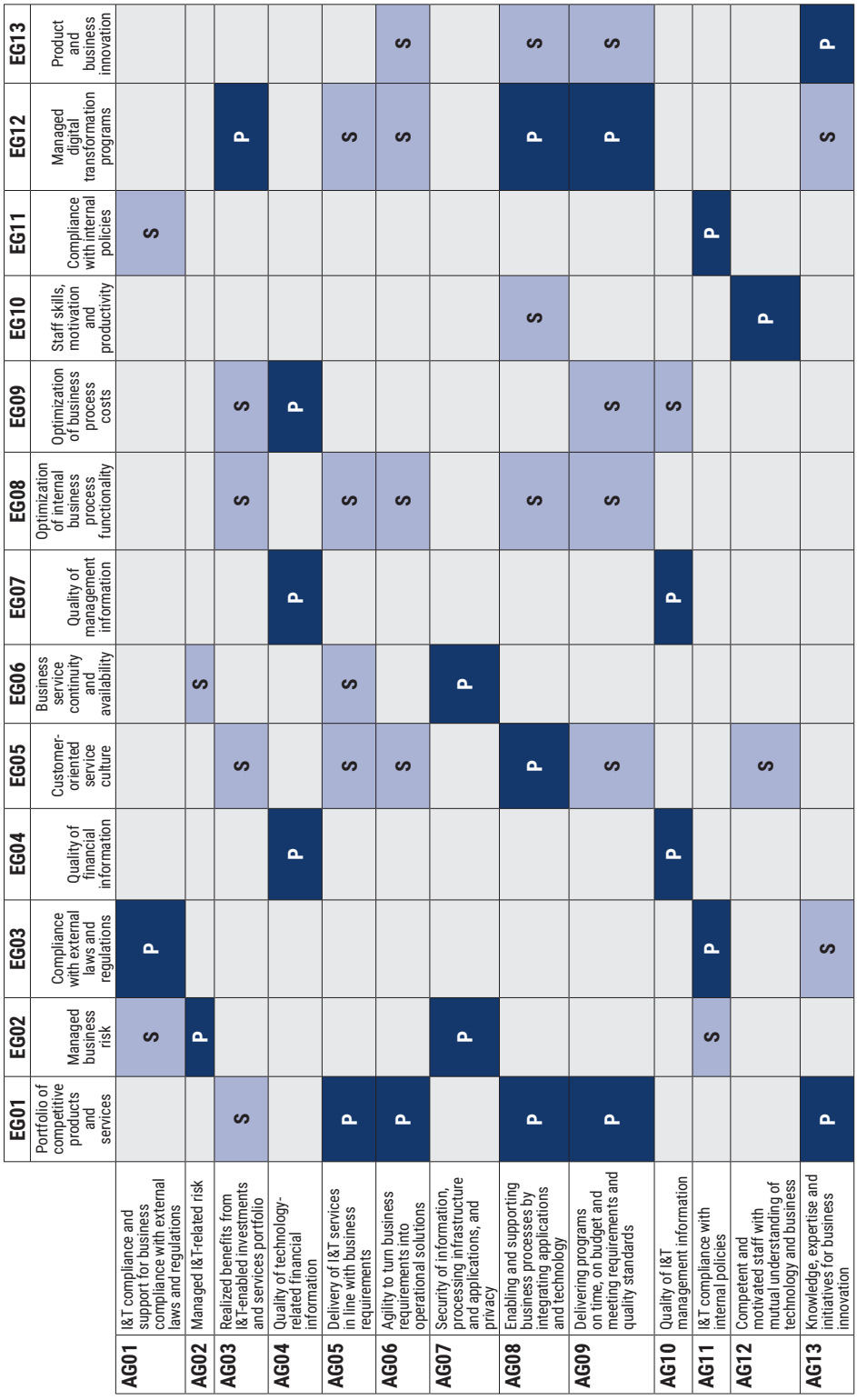
Figure A.1—Mapping Enterprise Strategies to Governance and Management Objectives

DF1	Growth/Acquisition	Innovation/Differentiation	Cost Leadership	ClientService/Stability
EDM01	1.0	1.0	1.5	1.5
EDM02	1.5	1.0	2.0	3.5
EDM03	1.0	1.0	1.0	2.0
EDM04	1.5	1.0	4.0	1.0
EDM05	1.5	1.5	1.0	2.0
APO01	1.0	1.0	1.0	1.0
APO02	3.5	3.5	1.5	1.0
APO03	4.0	2.0	1.0	1.0
APO04	1.0	4.0	1.0	1.0
APO05	3.5	4.0	2.5	1.0
APO06	1.5	1.0	4.0	1.0
APO07	2.0	1.0	1.0	1.0
APO08	1.0	1.5	1.0	3.5
APO09	1.0	1.0	1.5	4.0
APO10	1.0	1.0	3.5	1.5
APO11	1.0	1.0	1.0	4.0
APO12	1.0	1.5	1.0	2.5
APO13	1.0	1.0	1.0	2.5
APO14	1.0	1.0	1.0	1.0
BAI01	4.0	2.0	1.5	1.5
BAI02	1.0	1.0	1.5	1.0
BAI03	1.0	1.0	1.5	1.0
BAI04	1.0	1.0	1.0	3.0
BAI05	4.0	2.0	1.0	1.5
BAI06	2.0	2.0	1.0	1.5
BAI07	1.5	2.0	1.0	1.5
BAI08	1.0	3.5	1.0	1.0
BAI09	1.0	1.0	1.0	1.0

Figure A.1—Mapping Enterprise Strategies to Governance and Management Objectives *(cont.)*				
DF1	Growth/Acquisition	Innovation/Differentiation	Cost Leadership	ClientService/Stability
BAI10	1.0	1.0	1.0	1.0
BAI11	3.5	3.0	1.5	1.0
DSS01	1.0	1.0	1.0	1.5
DSS02	1.0	1.0	1.0	4.0
DSS03	1.0	1.0	1.0	3.0
DSS04	1.0	1.0	1.0	4.0
DSS05	1.0	1.0	1.0	2.5
DSS06	1.0	1.0	1.0	1.5
MEA01	1.0	1.0	1.0	1.0
MEA02	1.0	1.0	1.0	1.0
MEA03	1.0	1.0	1.0	1.0
MEA04	1.0	1.0	1.0	1.0

Appendix B: Mapping Table—Enterprise Goals to Alignment Goals

Figure A.2—Mapping Enterprise Goals to Alignment Goals



	EG01	EG02	EG03	EG04	EG05	EG06	EG07	EG08	EG09	EG10	EG11	EG12	EG13
	Portfolio of competitive products and services	Managed business risk	Compliance with external laws and regulations	Quality of financial information	Customer-oriented service culture	Business service continuity and availability	Quality of management information	Optimization of internal business process functionality	Optimization of business process costs	Staff skills, motivation and productivity	Compliance with internal policies	Managed digital transformation programs	Product and business innovation
AG01 I&T compliance and support for business compliance with external laws and regulations		S	P								S		
AG02 Managed I&T-related risk		P				S							
AG03 Realized benefits from I&T-enabled investments and services portfolio	S				S			S	S			P	
AG04 Quality of technology-related financial information				P			P		P				
AG05 Delivery of I&T services in line with business requirements	P				S	S		S				S	
AG06 Agility to turn business requirements into operational solutions	P				S			S				S	S
AG07 Security of information, processing infrastructure and applications, and privacy		P				P							
AG08 Enabling and supporting business processes by integrating applications and technology	P				P			S		S		P	S
AG09 Delivering programs on time, on budget and meeting requirements and quality standards	P				S			S	S			P	S
AG10 Quality of I&T management information				P			P		S				
AG11 I&T compliance with internal policies		S	P								P		
AG12 Competent and motivated staff with mutual understanding of technology and business					S					P			S
AG13 Knowledge, expertise and initiatives for business innovation	P		S										P

Appendix C: Mapping Table—Alignment Goals to Governance and Management Objectives

Figure A.3—Mapping Alignment Goals to Governance and Management Objectives

		AG01 I&T compliance and support for business compliance with external laws and regulations	AG02 Managed I&T-related risk	AG03 Realized benefits from I&T-enabled investments and services portfolio	AG04 Quality of technology-related financial information	AG05 Delivery of I&T services in line with business requirements	AG06 Agility to turn business requirements into operational solutions	AG07 Security of information, processing infrastructure and applications, and privacy	AG08 Enabling and supporting business processes by integrating applications and technology	AG09 Delivering programs on time, on budget and meeting requirements and quality standards	AG10 Quality of I&T management information	AG11 I&T compliance with internal policies	AG12 Competent and motivated staff with mutual understanding of technology and business	AG13 Knowledge, expertise and initiatives for business innovation
EDM01	Ensured governance framework setting and maintenance	P	S	P					S			S		
EDM02	Ensured benefits delivery			P		S	S		S					S
EDM03	Ensured risk optimization	S	P					P				S		
EDM04	Ensured resource optimization			S		S	S		S	P			S	
EDM05	Ensured stakeholder engagement				S						P	S		
APO01	Managed I&T management framework	S	S	P		S		S	S	S	S	P		
APO02	Managed strategy			S		S	S		P				S	S
APO03	Managed enterprise architecture			S		S	P	S	P					
APO04	Managed innovation			S			P		S				S	P
APO05	Managed portfolio			P		P	S		S	S				
APO06	Managed budget and costs			S	P					P	S			
APO07	Managed human resources			S		S				S			P	P
APO08	Managed relationships			S		P	P		S	S			P	P
APO09	Managed service agreements					P			S					
APO10	Managed vendors					P	S			S				
APO11	Managed quality			S	S	S				P	P			
APO12	Managed risk		P					P						
APO13	Managed security	S	S					P						
APO14	Managed data	S	S		S			S			P			
BAI01	Managed programs			P			S		S	P				
BAI02	Managed requirements definition			S		P	P		S	P			S	
BAI03	Managed solutions identification and build			S		P	P		S	P				
BAI04	Managed availability and capacity					P		S		S				
BAI05	Managed organizational changes			P		S	S		P	P			S	
BAI06	Managed IT changes		S			S	P		S					
BAI07	Managed IT change acceptance and transitioning		S				P			S				
BAI08	Managed knowledge			S			S		S	S			P	P
BAI09	Managed assets				P						S			
BAI10	Managed configuration					S		P						
BAI11	Managed projects			P		S	P			P				
DSS01	Managed operations					P			S					
DSS02	Managed service requests and incidents		S			P		S						
DSS03	Managed problems		S			P		S						
DSS04	Managed continuity		S			P		P						
DSS05	Managed security services	S	P			S		P				S		
DSS06	Managed business process controls		S			S		S	P			S		
MEA01	Managed performance and conformance monitoring	S		S		P				S	P	S		
MEA02	Managed system of internal control	S	S		S	S		S		S	S	P		
MEA03	Managed compliance with external requirements	P										S		
MEA04	Managed assurance	S	S		S	S		S			S	P		

Appendix D: Mapping Table—IT Risk to Governance and Management Objectives

Figure A.4—Mapping IT Risk to Governance and Management Objectives

DF3	RISKCAT01 IT Investment Decision Making, Portfolio Definition & Maintenance	RISKCAT02 Program & Projects Life Cycle Management	RISKCAT03 IT Cost & Oversight	RISKCAT04 IT Expertise, Skills & Behavior	RISKCAT05 "Enterprise/ IT Architecture "	RISKCAT06 IT Operational Infrastructure Incidents	RISKCAT07 Unauthorized Actions	RISKCAT08 "Software Adoption/ Usage Problems"	RISKCAT09 Hardware Incidents	RISKCAT10 Software Failures
EDM01	3	2	3	0	0	0	2	0	0	0
EDM02	3	2	0	0	2	0	0	0	0	0
ED0M3	2	2	0	0	0	0	0	0	0	1
EDM04	3	0	4	3	2	0	0	0	0	0
EDM05	3	1	3	0	0	0	2	0	0	1
APO01	2	3	2	0	2	2	4	2	0	2
APO02	2	0	0	0	3	0	0	2	1	0
APO03	2	0	0	0	4	0	0	2	0	2
AP0O4	0	0	0	0	1	0	0	0	0	0
APO05	4	2	2	0	2	0	0	2	2	0
APO06	2	3	4	0	0	0	0	0	0	0
APO07	0	0	0	4	0	2	3	3	0	0
APO08	0	0	0	2	2	0	0	4	0	0
APO09	0	0	2	0	0	0	2	3	0	1
APO10	0	2	3	0	0	0	2	2	3	2
APO11	0	3	0	0	0	0	0	2	0	4
APO12	0	0	0	0	0	0	3	0	0	2
APO13	0	0	0	0	0	0	4	0	0	0
APO14	0	0	0	0	0	0	3	2	0	0
BIA01	0	4	0	0	2	0	0	3	0	0
BAI02	2	2	0	0	2	0	0	3	0	2
BAI03	0	3	0	0	2	0	0	2	0	3
BAI04	0	1	0	0	0	0	0	0	0	0
BAI05	0	2	0	2	0	0	0	4	0	0
BAI06	0	0	0	0	0	3	4	0	0	2
BAI07	0	0	0	0	0	2	3	2	0	4
BAI08	0	0	0	2	0	3	0	3	0	3
BAI09	0	0	0	0	0	1	3	0	0	0
BAI10	0	0	0	0	0	2	4	0	0	2
BAI11	0	4	0	0	0	0	0	0	0	0
DSS01	0	0	0	0	0	4	3	0	4	0
DSS02	0	0	0	0	0	3	2	3	2	2
DSS03	0	0	0	0	0	3	1	4	0	3
DS0S4	0	0	0	0	0	3	3	0	3	0
DSS05	0	0	0	0	0	3	4	0	2	0
DSS06	0	0	0	0	0	3	4	2	0	0
MEA01	1	2	2	0	0	2	2	0	0	2
MEA02	1	2	2	0	0	3	3	0	0	2
MEA03	0	1	0	0	0	1	2	0	0	0
MEA04	1	2	0	0	0	0	3	0	0	2

Figure A.4—Mapping IT Risk to Governance and Management Objectives *(cont.)*

DF3	RISKCAT11 Logical Attacks (Hacking, Malware, etc.)	RISKCAT12 "Third-Party/ Supplier Incidents"	RISKCAT13 Noncompliance	RISKCAT14 Geopolitical Issues	RISKCAT15 Industrial Action	RISKCAT16 Acts of Nature	RISKCAT17 Technology-Based Innovation	RISKCAT18 Environmental	RISKCAT19 Data & Information Management
EDM01	0	0	3	2	0	0	2	2	2
EDM02	0	0	1	0	0	0	3	1	3
ED0M3	2	0	3	3	0	0	0	2	3
EDM04	0	2	1	0	2	0	0	2	3
EDM05	0	1	3	3	0	0	0	2	2
APO01	3	3	3	0	0	0	3	2	3
APO02	1	2	0	0	0	0	2	2	1
APO03	2	2	0	0	0	0	2	0	3
AP0O4	0	0	0	0	0	0	4	0	0
APO05	0	0	0	0	0	0	2	0	0
APO06	0	2	0	2	0	0	2	2	0
APO07	2	0	0	2	4	0	2	2	0
APO08	2	2	0	0	0	0	3	0	2
APO09	2	3	0	0	0	0	0	0	0
APO10	2	4	2	2	0	0	0	0	0
APO11	0	0	0	0	0	0	0	0	2
APO12	3	0	0	0	0	2	0	0	0
APO13	4	0	3	0	0	0	0	0	0
APO14	2	0	3	0	2	4	2	0	4
BIA01	0	0	0	0	0	0	0	0	0
BAI02	2	0	0	0	0	0	0	0	0
BAI03	3	0	0	0	0	0	0	0	0
BAI04	0	0	0	0	0	0	0	0	0
BAI05	0	0	0	0	0	0	0	0	0
BAI06	3	0	0	0	0	0	0	0	3
BAI07	2	0	0	0	0	0	0	0	0
BAI08	0	0	0	0	2	0	0	0	2
BAI09	0	0	0	0	0	0	0	0	0
BAI10	3	0	0	0	0	0	0	0	0
BAI11	0	0	0	0	0	0	0	0	0
DSS01	2	0	0	0	0	0	0	2	0
DSS02	4	0	0	0	0	0	0	0	0
DSS03	1	0	0	0	0	0	0	0	0
DS0S4	4	0	2	0	3	4	0	0	2
DSS05	4	0	3	0	3	2	0	0	3
DSS06	2	0	2	0	0	0	0	0	3
MEA01	3	2	2	2	0	2	0	0	2
MEA02	3	2	2	3	0	2	0	0	2
MEA03	3	2	4	2	0	0	0	0	2
MEA04	3	2	2	4	0	2	2	0	2

Appendix E: Mapping Table—I&T-Related Issues to Governance and Management Objectives

Figure A.5—Mapping I&T-Related Issues to Governance and Management Objectives

DF4	Frustration between different IT entities across the organization because of a perception of low contribution to business value	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	Significant IT-related incidents, such as data loss, security breaches, project failure and application errors, linked to IT	Service delivery problems by the IT outsourcer(s)	Failures to meet IT-related regulatory or contractual requirements	Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems	Substantial hidden and rogue IT spending, that is, IT spending by user departments or outside the control of the normal IT investment decision mechanisms and approved budgets	Duplications or overlaps between various initiatives or other forms of wasted resources	Insufficient IT resources, staff with inadequate skills or staff burnout / dissatisfaction	IT-enabled changes or projects frequently failing to meet business needs and delivered late or over budget
EDM01	3.0	3.0	1.0	1.0	2.0	2.0	2.0	1.0	1.0	1.0
EDM02	2.5	3.0	1.0	1.0	1.5	2.5	2.0	1.5	0.5	2.5
EDM03	1.0	1.0	2.0	1.0	2.0	2.0	1.0	1.0	0.0	0.5
EDM04	1.0	1.0	1.0	1.0	1.0	2.0	3.0	3.5	3.5	1.0
EDM05	1.0	1.0	1.0	1.0	1.5	2.0	1.0	1.0	0.0	1.0
APO01	2.0	1.0	2.0	1.0	2.0	2.0	1.0	1.0	0.0	0.5
APO02	1.5	1.5	1.5	1.5	1.0	1.5	1.0	1.0	0.0	1.0
APO03	1.0	1.5	1.0	2.0	0.5	1.5	2.0	1.5	1.0	3.5
APO04	1.0	1.0	1.0	1.0	0.5	0.5	0.5	0.5	0.0	0.0
APO05	3.0	3.0	1.0	1.5	2.0	2.0	1.5	3.5	0.5	2.0
APO06	3.5	2.0	1.0	1.5	1.5	2.0	4.0	3.0	1.0	2.0
APO07	1.5	1.0	1.0	1.0	1.0	1.5	2.0	2.0	4.0	1.0
APO08	2.5	2.0	1.0	2.5	1.5	1.0	2.5	2.0	1.5	1.0
APO09	2.0	1.5	2.0	4.0	1.0	2.5	1.5	2.0	0.5	1.0
APO10	1.0	1.0	2.0	4.0	1.5	1.5	1.5	0.0	1.5	1.0
APO11	1.0	1.0	3.0	1.5	1.0	3.0	0.0	0.0	0.0	2.0
APO12	1.0	0.5	2.5	1.5	2.0	2.0	1.0	1.0	0.5	1.0
APO13	0.0	0.0	3.5	1.0	2.0	1.0	0.0	1.0	0.0	0.5
APO14	1.0	1.5	3.0	1.0	2.5	1.5	1.0	1.5	0.0	1.5
BAI01	0.0	1.0	1.5	0.0	0.0	0.0	0.0	3.0	1.0	3.5
BAI02	0.0	3.0	0.0	0.0	0.5	2.0	0.0	2.0	0.0	3.5
BAI03	1.0	2.0	2.0	0.0	0.0	2.0	0.0	1.0	0.0	3.0
BAI04	0.5	0.0	2.0	3.0	0.0	2.0	0.0	0.0	0.0	0.0
BAI05	1.0	3.0	0.0	0.0	0.0	0.0	0.0	0.5	0.0	3.0
BAI06	0.0	0.0	2.5	3.0	0.5	1.5	0.0	1.0	0.0	1.5
BAI07	0.0	1.0	2.0	2.0	0.5	1.5	0.0	0.5	0.0	2.0
BAI08	0.0	0.0	0.0	1.5	0.5	0.5	0.0	1.0	2.0	0.5
BAI09	0.5	0.5	1.0	0.0	0.0	0.0	2.0	2.0	0.0	0.0
BAI10	0.0	0.0	2.5	2.0	0.5	0.0	0.0	0.5	0.0	0.0
BAI11	1.0	2.0	2.5	0.0	0.0	0.0	2.0	3.0	1.0	4.0
DSS01	0.0	0.0	2.5	2.0	1.0	2.0	0.0	0.5	0.0	0.0
DSS02	1.0	1.0	4.0	3.0	1.0	2.5	0.0	0.0	0.0	0.0
DSS03	0.0	1.0	3.0	3.0	0.0	3.0	0.0	0.0	0.0	0.0
DSS04	0.0	0.0	3.0	1.0	2.0	0.0	0.0	0.0	0.0	0.0
DSS5	0.0	0.0	4.0	2.0	2.0	0.0	0.0	0.0	0.0	0.0
DSS06	0.0	1.0	0.5	0.0	3.0	0.5	0.0	0.0	0.0	1.0
MEA01	1.0	1.5	2.0	2.0	2.5	3.0	1.0	2.0	1.5	1.0
MEA02	0.0	0.0	2.0	2.0	2.5	2.0	2.0	0.0	0.5	2.0
MEA03	0.0	0.0	2.0	2.0	4.0	0.5	0.0	0.0	0.0	0.0
MEA04	1.0	1.0	3.0	1.5	3.0	4.0	2.0	1.0	1.0	0.5

Figure A.5—Mapping I&T-Related Issues to Governance and Management Objectives *(cont.)*

DF4	Reluctance by board members, executives or senior management to engage with IT, or a lack of committed business sponsorship for IT	Complex IT operating model and/or unclear decision mechanisms for IT-related decisions	Excessively high cost of IT	Obstructed or failed implementation of new initiatives or innovations caused by the current IT architecture and systems	Gap between business and technical knowledge, which leads to business users and information and/or technology specialists speaking different languages	Regular issues with data quality and integration of data across various sources	High level of end-user computing, resulting (among other problems) a lack of oversight and quality control over the applications that are being developed and put in operation	Business departments implementing their own information solutions with little or no involvement of the enterprise IT department	Ignorance of and/or noncompliance with privacy regulations	Inability to exploit new technologies or innovate using I&T
EDM01	3.0	3.5	1.0	1.0	1.0	1.0	2.0	3.0	1.5	1.0
EDM02	1.5	1.0	3.0	2.0	1.0	1.0	2.0	2.0	1.0	2.5
EDM03	1.0	0.0	1.0	1.5	1.0	2.0	1.0	1.0	2.5	1.0
EDM04	1.5	0.0	4.0	2.0	1.0	1.5	2.0	2.5	0.0	1.0
EDM05	3.0	1.5	1.5	0.5	0.0	0.5	1.0	1.0	1.0	0.0
APO01	1.5	4.0	1.0	2.0	1.0	1.0	1.5	2.0	0.5	1.0
APO02	2.5	0.5	0.5	1.5	1.5	0.5	2.0	2.0	0.0	2.5
APO03	0.5	0.5	1.0	4.0	1.0	3.5	2.0	3.0	0.0	2.0
APO04	0.5	1.0	0.5	2.0	1.0	0.0	0.5	0.5	0.0	4.0
APO05	2.0	1.5	2.0	1.0	0.5	0.0	2.5	2.5	0.0	2.0
APO06	1.0	1.5	4.0	0.0	0.0	0.0	1.0	2.0	0.0	0.0
APO07	0.0	0.0	1.0	0.0	3.0	0.0	0.5	0.5	1.5	1.0
APO08	3.0	1.0	0.5	1.0	4.0	1.0	3.0	3.5	0.0	0.5
APO09	0.0	0.0	1.0	0.0	0.0	0.0	1.0	1.5	0.0	0.0
APO10	0.0	0.0	1.0	0.0	0.0	0.0	0.5	2.0	1.0	0.0
APO11	0.0	0.0	0.0	0.5	0.5	3.0	2.0	2.0	0.0	1.0
APO12	1.0	1.0	1.0	1.0	1.0	2.0	1.0	1.5	2.5	1.0
APO13	0.0	0.0	0.0	0.0	0.0	1.5	2.0	1.0	2.0	1.0
APO14	0.0	0.0	0.5	2.5	0.5	4.0	2.5	2.0	3.0	0.5
BAI01	0.0	0.0	1.5	0.5	1.0	0.0	1.5	2.0	0.0	1.0
BAI02	0.0	1.0	1.0	2.0	2.0	1.5	2.5	3.0	0.5	1.0
BAI03	0.0	0.5	1.0	1.0	1.0	0.5	2.0	2.0	1.0	0.5
BAI04	0.0	0.0	0.5	0.0	0.0	1.0	1.0	1.0	0.0	0.5
BAI05	1.0	0.0	0.0	0.5	2.0	0.0	0.5	1.5	0.0	1.0
BAI06	0.0	1.0	0.5	1.0	0.5	2.0	2.0	2.0	1.0	1.0
BAI07	0.0	1.0	0.0	1.0	0.5	2.0	2.0	2.0	0.0	1.0
BAI08	0.0	0.5	0.0	1.0	3.0	2.0	1.0	1.5	0.0	0.5
BAI09	0.0	0.0	2.0	1.0	0.0	0.0	1.0	1.5	0.0	0.0
BAI10	0.0	0.0	1.0	1.5	0.0	1.5	1.0	2.0	0.0	0.0
BAI11	0.0	0.0	1.5	2.0	0.5	0.0	1.0	1.5	0.0	0.5
DSS01	0.0	0.0	1.0	0.0	0.0	1.5	1.0	2.0	0.0	0.0
DSS02	0.0	0.0	1.0	0.0	0.0	1.0	1.0	1.0	0.0	0.0
DSS03	0.0	0.0	0.0	1.0	1.5	1.0	1.0	1.0	0.5	0.0
DSS04	0.0	0.0	0.0	0.0	0.0	1.5	1.0	2.0	0.0	0.0
DSS05	0.0	0.0	0.0	0.0	0.0	1.5	1.0	2.0	2.0	0.0
DSS06	0.0	0.0	0.0	0.0	1.5	2.5	1.5	1.0	2.0	0.0
MEA01	1.0	1.0	2.0	1.0	1.0	1.0	1.5	1.0	2.5	1.0
MEA02	1.0	1.0	1.5	1.0	0.0	2.0	1.0	1.0	2.5	0.0
MEA03	0.0	0.0	0.0	0.0	0.0	2.0	0.0	0.0	4.0	0.0
MEA04	1.0	1.0	1.5	0.0	1.0	1.0	1.0	1.0	2.5	1.0

Appendix F: Mapping Table—Threat Landscape to Governance and Management Objectives

Figure A.6—Mapping Threat Landscape to Governance and Management Objectives		
DF5	High	Normal
EDM01	3.0	1.0
EDM02	1.0	1.0
EDM03	4.0	1.0
EDM04	1.0	1.0
EDM05	2.0	1.0
APO01	3.0	1.0
APO02	1.0	1.0
APO03	3.0	1.0
APO04	1.0	1.0
APO05	1.0	1.0
APO06	1.0	1.0
APO07	2.0	1.0
APO08	1.0	1.0
APO09	2.0	1.0
APO10	3.0	1.0
APO11	2.0	1.0
APO12	4.0	1.0
APO13	4.0	1.0
APO14	3.0	1.0
BAI01	1.0	1.0
BAI02	1.0	1.0
BAI03	1.0	1.0
BAI04	2.0	1.0
BAI05	1.0	1.0
BAI06	3.0	1.0
BAI07	1.0	1.0
BAI08	1.0	1.0
BAI09	1.0	1.0
BAI10	3.0	1.0
BAI11	1.0	1.0
DSS01	1.0	1.0
DSS02	3.0	1.0
DSS03	2.0	1.0
DSS04	4.0	1.0
DSS05	3.0	1.0
DSS06	3.0	1.0
MEA01	3.0	1.0
MEA02	2.0	1.0
MEA03	3.0	1.0
MEA04	3.0	1.0

Appendix G: Mapping Table—Compliance Requirements to Governance and Management Objectives

Figure A.7—Mapping Compliance Requirements to Governance and Management Objectives			
DF6	High	Normal	Low
EDM01	3.0	2.0	1.0
EDM02	1.0	1.0	1.0
EDM03	4.0	2.0	1.0
EDM04	1.0	1.0	1.0
EDM05	1.5	1.0	1.0
APO01	2.0	1.5	1.0
APO02	1.0	1.0	1.0
APO03	1.0	1.0	1.0
APO04	1.0	1.0	1.0
APO05	1.0	1.0	1.0
APO06	1.0	1.0	1.0
APO07	1.0	1.0	1.0
APO08	1.0	1.0	1.0
APO09	1.0	1.0	1.0
APO10	1.5	1.0	1.0
APO11	1.0	1.0	1.0
APO12	4.0	2.0	1.0
APO13	1.5	1.0	1.0
APO14	2.0	1.5	1.0
BAI01	1.0	1.0	1.0
BAI02	1.0	1.0	1.0
BAI03	1.0	1.0	1.0
BAI04	1.0	1.0	1.0
BAI05	1.0	1.0	1.0
BAI06	1.0	1.0	1.0
BAI07	1.0	1.0	1.0
BAI08	1.0	1.0	1.0
BAI09	1.0	1.0	1.0
BAI10	1.0	1.0	1.0
BAI11	1.0	1.0	1.0
DSS01	1.0	1.0	1.0
DSS02	1.0	1.0	1.0
DSS03	1.0	1.0	1.0
DSS04	1.5	1.0	1.0
DSS05	2.0	1.0	1.0
DSS06	1.0	1.0	1.0
MEA01	1.0	1.0	1.0
MEA02	1.0	1.0	1.0
MEA03	4.0	2.0	1.0
MEA04	3.5	2.0	1.0

Appendix H: Mapping Table—Role of IT to Governance and Management Objectives

Figure A.8—Mapping Role of IT to Governance and Management Objectives				
DF7	Support	Factory	Turnaround	Strategic
EDM01	1.0	2.0	1.5	4.0
EDM02	1.0	1.0	2.5	3.0
EDM03	1.0	3.0	1.0	3.0
EDM04	1.0	1.0	1.0	2.0
EDM05	1.0	1.0	1.0	2.0
APO01	1.0	1.5	1.5	2.5
APO02	1.0	1.0	3.0	3.0
APO03	1.0	1.0	2.0	2.0
APO04	0.5	1.0	3.5	4.0
APO05	1.0	1.0	2.5	3.0
APO06	1.0	1.0	1.0	2.0
APO07	1.0	1.0	1.0	1.5
APO08	1.0	1.0	2.0	2.5
APO09	1.0	2.0	1.5	2.0
APO10	1.0	2.5	1.5	2.0
APO11	1.0	1.5	1.5	2.0
APO12	1.0	2.5	1.0	3.0
APO13	1.0	2.0	1.5	3.0
APO14	1.0	1.5	1.5	2.5
BAI01	1.0	1.0	2.0	2.5
BAI02	1.0	1.0	3.0	3.0
BAI03	1.0	1.0	3.0	3.0
BAI04	1.0	2.5	1.5	2.0
BAI05	1.0	1.0	1.0	2.0
BAI06	1.0	2.5	1.0	2.0
BAI07	1.0	1.0	2.0	2.0
BAI08	1.0	1.0	1.0	2.0
BAI09	1.0	1.0	1.0	2.0
BAI10	1.0	1.5	1.0	2.0
BAI11	1.0	1.0	2.0	2.0
DSS01	1.0	3.5	1.0	3.0
DSS02	1.0	3.0	1.5	3.0
DSS03	1.0	3.0	1.5	3.5
DSS04	1.0	3.0	1.5	3.5
DSS05	1.5	2.5	1.5	3.5
DSS06	1.0	1.0	1.0	2.5
MEA01	1.0	1.0	1.0	2.0
MEA02	1.0	1.0	1.0	2.0
MEA03	1.0	1.0	1.0	1.5
MEA04	1.0	1.0	1.0	2.0

Appendix I: Mapping Table—Sourcing Model for IT to Governance and Management Objectives

Figure A.9—Mapping Sourcing Model for IT to Governance and Management Objectives			
DF8	Outsourcing	Cloud	Insourcing
EDM01	1.0	1.0	1.0
EDM02	1.0	1.0	1.0
EDM03	1.0	2.0	1.0
EDM04	1.0	1.0	1.0
EDM05	1.0	1.0	1.0
APO01	1.0	1.0	1.0
APO02	1.0	1.0	1.0
APO03	1.0	1.0	1.0
APO04	1.0	1.0	1.0
APO05	1.0	1.0	1.0
APO06	1.0	1.0	1.0
APO07	1.0	1.0	1.0
APO08	1.0	1.0	1.0
APO09	4.0	4.0	1.0
APO10	4.0	4.0	1.0
APO11	1.0	1.0	1.0
APO12	2.0	2.0	1.0
APO13	1.0	1.0	1.0
APO14	1.0	1.0	1.0
BAI01	1.0	1.0	1.0
BAI02	1.0	1.0	1.0
BAI03	1.0	1.0	1.0
BAI04	1.0	1.0	1.0
BAI05	1.0	1.0	1.0
BAI06	1.0	1.0	1.0
BAI07	1.0	1.0	1.0
BAI08	1.0	1.0	1.0
BAI09	1.0	1.0	1.0
BAI10	1.0	1.0	1.0
BAI11	1.0	1.0	1.0
DSS01	1.0	1.0	1.0
DSS02	1.0	1.0	1.0
DSS03	1.0	1.0	1.0
DSS04	1.0	1.0	1.0
DSS05	1.0	1.0	1.0
DSS06	1.0	1.0	1.0
MEA01	3.0	3.0	1.0
MEA02	1.0	1.0	1.0
MEA03	1.0	1.0	1.0
MEA04	1.0	1.0	1.0

Appendix J: Mapping Table—IT Implementation Methods to Governance and Management Objectives

Figure A.10—Mapping IT Implementation Methods to Governance and Management Objectives			
DF9	Agile	DevOps	Traditional
EDM01	1.0	1.0	1.0
EDM02	1.0	1.0	1.0
EDM03	1.0	1.0	1.0
EDM04	1.0	1.0	1.0
EDM05	1.0	1.0	1.0
APO01	1.0	1.0	1.0
APO02	1.0	1.0	1.0
APO03	1.0	2.0	1.0
APO04	1.0	1.0	1.0
APO05	1.0	1.0	1.0
APO06	1.0	1.0	1.0
APO07	1.0	1.5	1.0
APO08	1.0	1.0	1.0
APO09	1.0	1.0	1.0
APO10	1.0	1.0	1.0
APO11	1.0	1.0	1.0
APO12	1.0	1.5	1.0
APO13	1.0	1.0	1.0
APO14	1.0	1.0	1.0
BAI01	2.0	1.5	1.0
BAI02	3.5	2.0	1.0
BAI03	4.0	3.0	1.0
BAI04	1.0	1.0	1.0
BAI05	2.5	1.5	1.0
BAI06	3.5	2.0	1.0
BAI07	2.5	2.5	1.0
BAI08	1.0	1.0	1.0
BAI09	1.0	1.0	1.0
BAI10	1.5	2.0	1.0
BAI11	2.5	1.0	1.0
DSS01	1.0	2.5	1.0
DSS02	1.0	1.5	1.0
DSS03	1.0	1.5	1.0
DSS04	1.0	1.0	1.0
DSS05	1.0	1.0	1.0
DSS06	1.0	1.0	1.0
MEA01	1.5	1.5	1.0
MEA02	1.0	1.0	1.0
MEA03	1.0	1.0	1.0
MEA04	1.0	1.0	1.0

Appendix K: Mapping Table—Technology Adoption Strategies to Governance and Management Objectives

Figure A.11—Mapping Technology Adoption Strategies to Governance and Management Objectives

DF10	First Mover	Follower	Slow Adopter
EDM01	3.5	2.5	1.5
EDM02	4.0	2.5	1.5
EDM03	1.5	1.0	1.0
EDM04	2.5	2.0	1.5
EDM05	1.5	1.0	1.0
APO01	2.5	1.5	1.0
APO02	4.0	3.0	1.5
APO03	2.0	1.0	1.0
APO04	4.0	3.0	1.0
APO05	4.0	2.5	1.0
APO06	1.0	1.5	1.0
APO07	2.5	1.0	1.0
APO08	3.0	1.5	1.0
APO09	1.5	1.5	1.0
APO10	2.5	1.5	1.0
APO11	1.5	1.5	1.0
APO12	2.0	1.5	1.0
APO13	1.0	1.0	1.0
APO14	2.5	2.0	1.0
BAI01	4.0	3.0	1.5
BAI02	3.5	2.5	1.0
BAI03	4.0	2.5	1.0
BAI04	1.5	1.5	1.0
BAI05	3.0	2.0	1.0
BAI06	2.5	2.0	1.0
BAI07	3.5	2.5	1.0
BAI08	1.5	1.0	1.0
BAI09	1.0	1.0	1.0
BAI10	1.5	1.0	1.0
BAI11	3.5	2.5	1.0
DSS01	1.0	1.0	1.0
DSS02	1.0	1.0	1.0
DSS03	1.5	1.0	1.0
DSS04	1.5	1.0	1.0
DSS05	1.5	1.0	1.0
DSS06	1.0	1.0	1.0
MEA01	3.0	2.0	1.0
MEA02	1.0	1.0	1.0
MEA03	1.0	1.0	1.0
MEA04	1.0	1.0	1.0