COBIT® 2019

IMPLEMENTATION GUIDE

Implementing and Optimizing 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 Implementation Guide: Implementing and Optimizing 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 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution
ISBN 978-1-60420-766-8

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, 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

Chapter 1. Introduction

Chapter 2. Positioning Enterprise Governance of I&T

Chapter 3. Taking the First Steps Toward EGIT

Chapter 4. Identifying Challenges and Success Factors

Chapter 5. Enabling Change

Chapter 6. Implementation Life Cycle

Appendix A. Example Decision Matrix

Chapter 1
Introduction

1.1 Improvement of Enterprise Governance of Information and Technology

In the light of digital transformation, information and technology (I&T)[1] have become crucial in the support, sustainability and growth of enterprises. Previously, governing boards (boards of directors) and senior management could delegate, ignore or avoid I&T-related decisions. In most sectors and industries, such attitudes are now ill-advised. Stakeholder value creation (i.e., realizing benefits at an optimal resource cost while optimizing risk) is often driven by a high degree of digitization in new business models, efficient processes, successful innovation, etc. Digitized enterprises are increasingly dependent on I&T for survival and growth.

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

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

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

For many years, ISACA® has researched this key area of enterprise governance to advance international thinking and provide guidance in evaluating, directing and monitoring an enterprise's use of I&T. ISACA has developed the COBIT® framework to help enterprises implement sound governance and management components. Indeed, implementing good EGIT is almost impossible without using an effective governance framework.

Effective EGIT will improve business performance and compliance with external requirements. Yet, successful implementation still eludes many enterprises. EGIT is complex and multifaceted. There is no silver bullet (or ideal way) to design, implement and maintain effective EGIT within an organization. As such, members of the governing boards and senior management typically need to tailor their EGIT measures and implementation to their own specific context and needs. They must also be willing to accept more accountability for I&T and drive a different mindset and culture for delivering value from I&T.

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

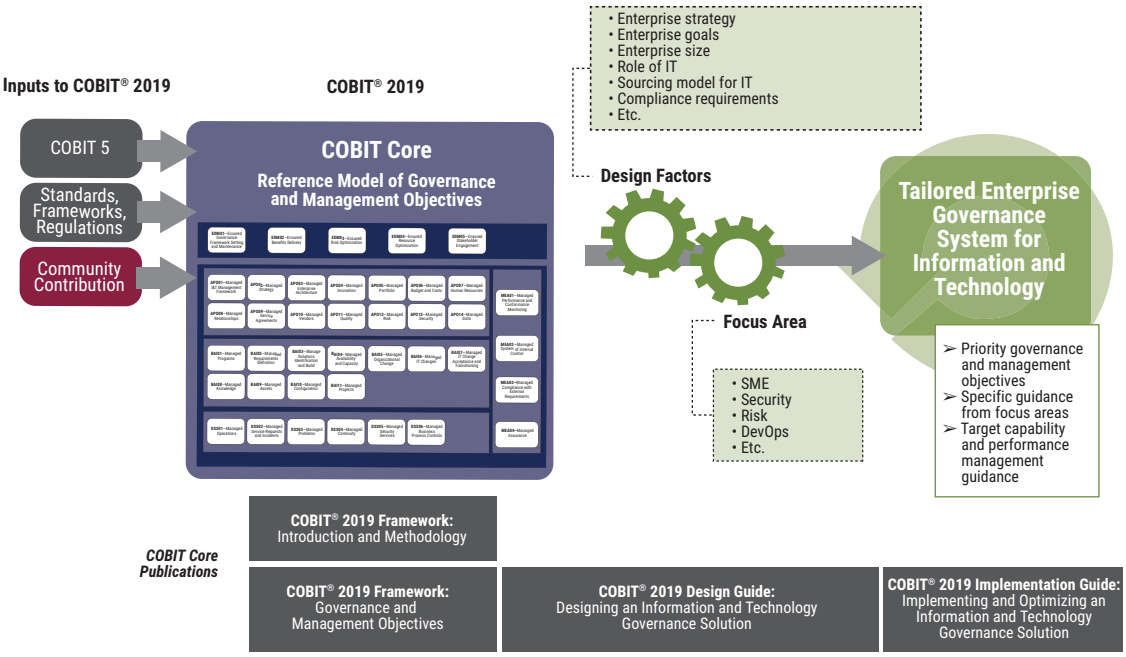
1.2 COBIT Overview

COBIT® 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution is the fourth publication in the COBIT® 2019 suite of products (see **figure 1.2**). Some of the other publications are described below.

- ***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.

The objective of this reference guide is to provide good practices for implementing and optimizing an I&T governance system, based on a continual improvement life cycle approach, which should be tailored to suit the enterprise's specific needs.

Figure 1.2—COBIT Overview



1.3 Objectives and Scope of the Implementation Guide

COBIT principles emphasize the enterprisewide view of governance of I&T (see *COBIT® 2019 Framework: Introduction and Methodology*). Information and technology are not confined to the IT department; they are pervasive throughout the enterprise. It is neither possible nor good practice to separate I&T-related activities from the

business. The governance and management of enterprise I&T should, therefore, be implemented as an integral part of enterprise governance, covering the full end-to-end business and IT functional areas of responsibility.

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

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

This publication is not intended to be a prescriptive approach or the complete solution, but rather a guide to avoid pitfalls, leverage the latest good practices, and assist in the creation of successful governance and management outcomes over time. To an important extent, it leverages the *COBIT® 2019 Design Guide*, which helps every enterprise to identify and apply its own specific plan or road map, depending on a number of design factors such as enterprise strategy, risk and threat issues, and role of IT.

Determining the current starting point is equally important. Few enterprises have no EGIT structures or processes in place, even if they are not recognized as such currently. Therefore, the emphasis must be on building on what the enterprise already has in place, especially leveraging existing successful enterprise-level approaches that can be adopted, and, if necessary, adapted for I&T governance, rather than inventing something different. Furthermore, any previous improvements created by applying COBIT® 5 or other standards and good practices need not be reworked. Instead, they can, and should be, enhanced by COBIT® 2019 as an ongoing part of continual improvement.

COBIT® 2019 is freely downloadable from *www.isaca.org/cobit*. Links to ISACA products supporting implementation are available on this page as well.

This publication reflects enhanced understanding of and practical experience with EGIT implementations, lessons learned while applying and using previous versions of COBIT, and updates made to ISACA's guidance. However, I&T never stand still, so users of this guide should anticipate ISACA's professional publications and other organizations' standards and good practices that may be released from time to time to address newly emerging topics. New, forthcoming focus area content will become part of the COBIT product family and will provide important guidance on these emerging topics.[2]

1.4 Structure of This Publication

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

- Chapter 2 explains the positioning of EGIT within the enterprise.
- Chapter 3 discusses the first steps toward improving EGIT.
- Chapter 4 describes implementation challenges and success factors.
- Chapter 5 covers EGIT-related organizational and behavioral change.
-

[2] At the time of publication of this *COBIT® 2019 Implementation Guide*, focus area content is planned, but not yet released.

- Chapter 6 describes the implementation life cycle, including change enablement and program management.
- The appendix provides an example decision matrix.

1.5 Target Audience for This Publication

The target audience for this publication is experienced professionals throughout the enterprise, including business departments, audit, security, privacy, risk management, IT professionals, external professionals and others involved (or planning to be involved) in the implementation of EGIT.

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 the core COBIT guidance—which is generic in nature—into tailored and focused guidance for the enterprise, taking into account the enterprise's context.

1.6 Related Guidance: *COBIT® 2019 Design Guide*

The *COBIT® 2019 Design Guide* is related to this publication. It defines design factors that can influence a governance system and includes a workflow for designing a tailored governance system for the enterprise. The workflow explained in the *COBIT® 2019 Design Guide* has a number of connection points with the *COBIT® 2019 Implementation Guide;* the design guide elaborates a set of tasks defined in this implementation guide.

Chapter 5 of the *COBIT® 2019 Design Guide* explores the links between the two publications and illustrates how to use them together.

Chapter 2
Positioning Enterprise Governance of I&T

2.1 Understanding the Context

Enterprise governance of information and technology (EGIT) does not occur in a vacuum. Implementation takes place in different conditions and circumstances determined by numerous factors in the internal and external environment, such as:

- The community's ethics and culture
- Governing laws, regulations and policies
- International standards
- Industry practices
- The economic and competitive environment
- Technology advancements and evolution
- The threat landscape
- The enterprise's:
  - Reason for existence, mission, vision, goals and values
  - Governance policies and practices
  - Culture and management style
  - Models for roles and responsibilities
  - Business plans and strategic intentions
  - Operating model and level of maturity

The implementation of EGIT for each enterprise is, therefore, different, and the context needs to be understood and considered to design the optimal new or improved EGIT environment. This is fully elaborated in the *COBIT® 2019 Design Guide*.

2.1.1 What is EGIT?

The terms governance, enterprise governance and EGIT may have different meanings depending on organizational context (maturity, industry and regulatory environment) or individual context (job role, education and experience), among other factors. Explanations in this chapter provide a foundation for the rest of the guide, but it should be recognized that different points of view do exist. It is better to build on and enhance existing approaches to include I&T than to develop a new approach just for I&T.

The term governance derives from the Greek verb *kubernáo*, meaning "to steer." A governance system enables multiple stakeholders in an enterprise to have an organized say in evaluating conditions and options, setting direction, and monitoring performance against enterprise objectives. Setting and maintaining the appropriate governance approach are the responsibility of the board of directors or equivalent body.

COBIT defines governance as follows:

> *Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives.*[3]

[3] See *COBIT® 2019 Framework: Introduction and Methodology*, Section 1.3.

EGIT is not an isolated discipline, but an integral part of enterprise governance. The need for governance at an enterprise level is driven primarily by delivery of stakeholder value and demand for transparency and effective management of enterprise risk. The significant opportunities, costs and risk associated with I&T call for a dedicated, yet integrated, focus on EGIT. EGIT enables the enterprise to take full advantage of I&T, maximizing benefits, capitalizing on opportunities and gaining competitive advantage.

2.1.2 Why is EGIT so Important?

Globally, enterprises—whether public or private, large or small—increasingly understand that information is a key resource and technology is a strategic asset, both critical to success.

I&T can be powerful resources to help enterprises achieve their most important objectives. For example, I&T can drive cost savings for large transactions such as mergers, acquisitions and divestitures. I&T can enable automation of key processes, such as the supply chain. I&T can be the cornerstone of new business strategies or business models, thereby increasing competitiveness and enabling innovation, such as digital delivery of products (e.g., music sold and delivered online). I&T can enable greater customer intimacy, for example, by collating and mining data in diverse systems and providing a 360-degree view of customers. I&T are the foundation of the networked economy that cuts through geographic locations and organizational silos to provide new and innovative ways of creating value. Most enterprises recognize information and the use of I&T as critical assets that need to be governed properly.

While I&T has the potential for business transformation, it often represents a very significant investment at the same time. In many cases, true IT cost is not transparent, and budgets are spread across business units, functions and geographic locations, without central oversight. The greatest portion of spending often just keeps the lights on, funding maintenance and operations post-implementation, rather than innovative or transformational initiatives. When funds are spent on strategic initiatives, they often fail to deliver expected outcomes. Many enterprises still fail to demonstrate concrete, measurable business value for IT-enabled investments and focus on EGIT as a mechanism to address this situation.

The networked economy presents a spectrum of IT-related risk, including compromise of customer-facing business systems, disclosure of customer or proprietary data, or missed business opportunities due to inflexible IT architecture. Managing these and other types of I&T-related risk is another driver for better EGIT.

EGIT can address the complex regulatory environment faced by enterprises in many industries and jurisdictions today, often extending directly to IT. Requirements and scrutiny around financial reporting drive significant focus on IT-related controls. The use of good practices such as COBIT has been mandated in some countries and industries. For example, the Banking Regulation and Supervision Agency (BRSA) of Turkey has mandated that all banks operating in Turkey must adopt COBIT's good practices when managing IT-related processes, as has the Australian Prudential Regulation Authority. The report on corporate governance in South Africa—King IV—includes a principle to implement EGIT and recommends the adoption of frameworks such as COBIT. A governance framework for I&T can facilitate compliance in a more effective and efficient way.

Research has long demonstrated the value of EGIT. In a large case study of an international airline company, EGIT's benefits were demonstrated to include: lower IT-related continuity costs, increased IT-enabled innovation capacity, increased alignment between digital investments and business goals and strategy, increased trust between business and IT, and a shift toward a "value mindset" around digital assets.[4]

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

Research has shown that enterprises with poorly designed or adopted approaches to EGIT perform worse in aligning business and I&T strategies and processes. As a result, such enterprises are much less likely to achieve their intended business strategies and realize the business value they expect from digital transformation.[5]

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

2.1.3 What Should EGIT Deliver?

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

- **Benefits realization**—This consists of creating value for the enterprise through I&T, maintaining and increasing value derived from existing I&T[6] investments, and eliminating IT initiatives and assets that are not creating sufficient value. The basic principle of I&T value are delivery of fit-for-purpose services and solutions, on time and within budget, that generate the intended financial and nonfinancial benefits. The value that I&T delivers should be aligned directly with the values on which the business is focused. IT value should also be measured in a way that shows the impact and contributions of IT-enabled investments in the value creation process of the enterprise.
- **Risk optimization**—This entails addressing the business risk associated with the use, ownership, operation, involvement, influence and adoption of I&T within an enterprise. I&T-related business risk consists of I&T-related events that could potentially impact the business. While value delivery focuses on the *creation* of value, risk management focuses on the *preservation* of value. The management of I&T-related risk should be integrated within the enterprise risk management approach to ensure a focus on IT by the enterprise. It should also be measured in a way that shows the impact and contributions of optimizing I&T-related business risk on preserving value.
- **Resource optimization**—This ensures that the appropriate capabilities are in place to execute the strategic plan and sufficient, appropriate and effective resources are provided. Resource optimization ensures that an integrated, economical IT infrastructure is provided, new technology is introduced as required by the business, and obsolete systems are updated or replaced. Because it recognizes the importance of people, in addition to hardware and software, it focuses on providing training, promoting retention and ensuring competence of key IT personnel. An important resource is data and information, and exploiting data and information to gain optimal value is another key element of resource optimization.

Throughout implementation and exercise of EGIT, strategic alignment and performance measurement are of paramount importance and apply overall to all activities to ensure that I&T-related objectives are aligned with the enterprise goals.

2.2 Leveraging COBIT and Integrating Frameworks, Standards and Good Practices

COBIT is based on an enterprise view, and it aligns with enterprise governance good practices. COBIT is a single, overarching framework whose consistent, integrated guidance is expressed in nontechnical and technology-agnostic language. The board should mandate adoption of an EGIT framework like COBIT as an essential part of enterprise governance development.

[5] De Haes S.; A. Joshi; W. van Grembergen; "State and Impact of Governance of Enterprise IT in Organizations: Key Findings of an International Study," *ISACA® Journal*, vol. 4, 2015, *https://www.isaca.org/Journal/archives/2015/Volume-4/Pages/state-and-impact-of-governance-of-enterprise-itin-organizations.aspx*. See also *op cit* De Haes and van Grembergen, *Enterprise Governance of IT: Achieving Alignment and Value, Featuring COBIT 5.*

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

Working within a framework and leveraging good practices enables development and optimization of appropriate governance processes and other components of the governance system. Tailored appropriately, EGIT will operate effectively as part of an enterprise's normal business practice, provided there is a supporting culture, demonstrated by top management.

COBIT® 2019 not only outlines a general approach, but also references other detailed standards. *COBIT® 2019 Framework: Introduction and Methodology*, Chapter 10, lists all standards that align to COBIT® 2019; these standards reappear, elaborated by detailed references, under the governance and management objectives, their associated practices, and components in *COBIT®2019 Framework: Governance and Management Objectives*.

Aligning with COBIT should also result in faster and more efficient external audits since COBIT is widely accepted as a basis for IT audit procedures.

The COBIT framework sets out the overall approach; guidance provided by specific standards and good practices can then be applied to specific processes, practices, policies and procedures, as the enterprise tailors its implementation. Specifically, the governance system and its components should align and harmonize with the:

- Enterprise policies, strategies, governance and business plans, and audit approaches
- Enterprise risk management (ERM) framework
- Existing enterprise governance organization, structures and processes

2.2.1 Governance Principles

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

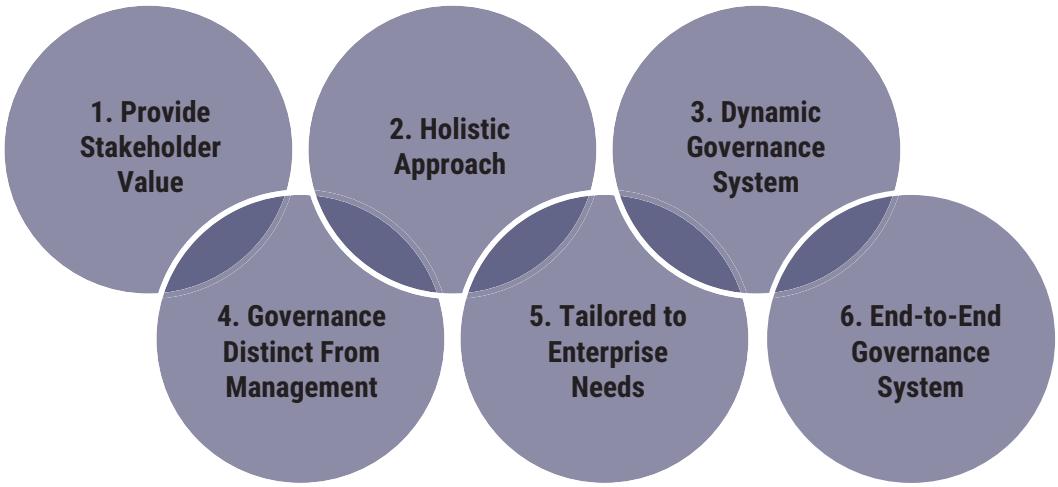
- Principles that describe the core requirements of a **governance system** for enterprise information and technology.
- Principles for a **governance framework** that can be used to build a governance system for the enterprise.

The six principles for a governance system (**figure 2.1**) are:

1. Each enterprise needs a governance system to satisfy stakeholder needs and to generate value from the use of I&T. Value reflects a balance among benefits, risk and resources, and enterprises need an actionable strategy and governance system to realize this value.
2. A governance system for enterprise I&T is built from a number of components that can be of different types and that work together in a holistic way.
3. A governance system should be dynamic. This means that each time one or more of the design factors are changed (e.g., a change in strategy or technology), the impact of these changes on the EGIT system must be considered. A dynamic view of EGIT leads toward a viable and future-proof EGIT system.
4. A governance system should clearly distinguish between governance and management activities and structures.
5. A governance system should be customized to the enterprise's needs, using a set of design factors as parameters to customize and prioritize the governance system components.
6. A governance system should cover the enterprise end to end, focusing on not only the IT function but on all technology and information processing the enterprise puts in place to achieve its goals, regardless of its location in the enterprise.[7]

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

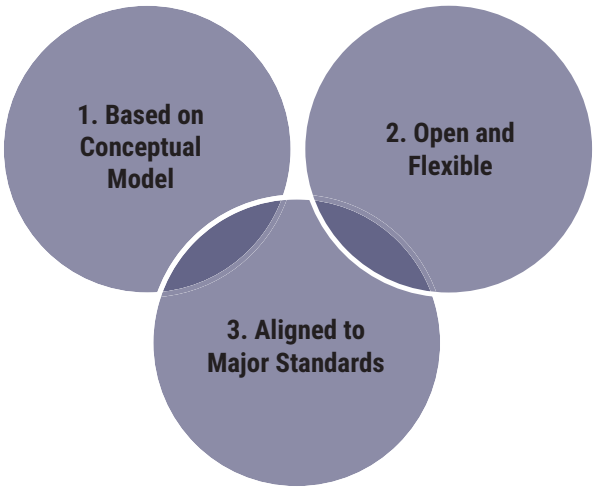
Figure 2.1—Governance System Principles



The three principles for a governance framework (**figure 2.2**) are:

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

Figure 2.2—Governance Framework Principles



2.2.2 Governance System and Components

To satisfy governance and management objectives, each enterprise needs to establish, tailor and sustain a governance system built from a number of components. Several basic concepts pertaining to governance systems are:

- Components can be of different types. The most familiar are processes, but organizational structures; information items; skills and competencies; culture and behavior; policies and procedures; and services, infrastructure and applications are also components of a governance system and need to be considered.
- Components of all types can be generic or can be variants of generic components.
- Generic components are described in the COBIT core model (see *COBIT® 2019 Framework: Introduction and Methodology*, Figure 4.2), and apply in principle to any situation. However, they are generic in nature and generally need customization before being practically implemented.
- Variants are based on generic components but are tailored for a specific purpose or context within a focus area (e.g., for information security, DevOps, a particular regulation).

2.2.3 Governance and Management Objectives

COBIT includes governance and management objectives and underlying processes that help guide the creation and maintenance of the governance system and its different components. In that respect, the two key governance and management objectives are:

- EDM01 *Ensured governance framework setting and maintenance* (culture, ethics and behavior; principles, policies and frameworks; organizational structures; and processes)
- APO01 *Managed I&T management framework* (culture, ethics and behavior; principles, policies and frameworks; organizational structures; and processes)

COBIT governance and management objectives ensure that enterprises organize their I&T-related activities in a repeatable and reliable way. The COBIT core model—with five domains, 40 governance and management objectives, and underlying processes that form the structure for detailed COBIT guidance—is described and elaborated in *COBIT®2019 Framework: Governance and Management Objectives.*

Chapter 3
Taking the First Steps Toward EGIT

3.1 Creating the Appropriate Environment

It is important for the appropriate context to exist when implementing EGIT improvements. This helps ensure that the initiative is governed and adequately guided and supported by management. Major I&T initiatives often fail due to inadequate management direction, support and oversight. EGIT implementations are no different; they have more chance of success if they are well governed and well managed.

Inadequate support and direction from key stakeholders can, for example, result in EGIT initiatives that produce new policies and procedures without proper ownership or lasting effect. Improvements are unlikely to become normal business practices without a management structure that assigns roles and responsibilities, commits to their continued operation, and monitors conformance.

An appropriate environment should, therefore, be created and maintained to ensure that EGIT is implemented as an integral part of an overall governance approach within the enterprise. This should include adequate direction and oversight of the implementation initiative, including guiding principles. The objective is to provide sufficient commitment, direction and control of activities so that there is alignment with enterprise objectives and appropriate implementation support from the board and executive management.

Experience has shown that, in some cases, an EGIT initiative identifies significant weaknesses in overall enterprise governance. Success of EGIT is much more difficult within a weak enterprise governance environment, so active support and participation of senior executives become even more critical. The board and executives should be aware of corporate governance concepts, should understand the need to improve overall governance, and should acknowledge the risk of EGIT failing if weaknesses are not addressed.

Whether the implementation is a small or major initiative, executive management must be involved in, and drive creation of, the appropriate governance structures. The initial activities usually include assessment of current practices and the design of improved structures. In some cases, the initiative can lead to reorganization of the business as well as the IT function and its relationship to business units.

Executive management should set and maintain the governance framework. This means specifying the structures, processes and practices for EGIT in line with agreed governance design principles, decision-making models, authority levels and the information required for informed decision making.[8]

Executive management should also allocate clear roles and responsibilities for directing the EGIT improvement program.

A common approach to formalize EGIT and provide a mechanism for executive and board oversight and direction of I&T-related activities is to establish an I&T governance board.[9] This I&T governance board acts on behalf of the board of directors (to which it is accountable). The I&T governance board is responsible for how I&T is used within the enterprise and for making key I&T-related decisions affecting the enterprise. It should have a clearly defined mandate and is best chaired by a business executive (ideally a board member). It should be staffed by senior business executives representing the major business units, as well as the chief information officer (CIO), chief digital officer (CDO) and/or chief technology officer (CTO), and, if required, other senior IT managers. Internal audit, information security and risk functions should provide an advisory role.

[8] See the appendix for an example decision matrix.
[9] The I&T governance board may also be called an IT steering committee, IT council, IT executive committee or IT governance committee.

Executives need to make decisions based on facts; reliable information; and diverse, well-founded opinions from business and IT managers, auditors, customers, users and others. The COBIT framework facilitates these communications by providing a common language for executives to express goals, objectives and expected results.

Figures 3.1 and **3.2** illustrate generic roles for key stakeholders and outline responsibilities for implementing the appropriate environment to sustain governance and ensure successful outcomes. Similar figures are provided for each phase of the implementation life cycle introduced in the next section.

Figure 3.1—Roles in Creating the Appropriate Environment

When you are...	Your role in creating the appropriate environment is to...
Board and executives	• Set direction for the program • Ensure alignment with enterprisewide governance and risk management • Approve key program roles and define responsibilities • Give visible support and commitment • Sponsor, communicate and promote the agreed initiative
Business management	• Provide appropriate stakeholders and champions to drive commitment and support the program • Nominate key program roles and define and assign responsibilities
IT management	• Ensure that the business and executives understand and appreciate the high-level I&T-related issues and objectives • Nominate key program roles and define and assign responsibilities • Nominate a person to drive the program in agreement with the business
Internal audit	• Agree on the role and reporting arrangements for audit participation • Ensure an adequate level of audit participation through the duration of the program
Risk, compliance and legal	• Ensure an adequate level of participation through the duration of the program

Figure 3.2—Responsibilities of Implementation Role Players

Key Activities	Board	I&T Governance Board	CIO	Business Executive	IT Managers	IT Process Owners	IT Audit	Risk and Compliance	Program Steering
	Responsibilities of Implementation Role Players								
Set direction for the program.	A	R	R	C	C	I	C	C	C
Provide program management resources.	C	A	R	R	C	C	R	R	I
Establish and maintain direction and oversight structures and processes.	C	A	C	I	I	I	I	I	R
Establish and maintain program.	I	A	R	C	C	I	I	I	R
Align approaches with enterprise approaches.	I	A	R	C	C	I	C	C	R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or Informed.

3.2 Applying a Continual Improvement Life Cycle Approach

The continual improvement life cycle approach allows enterprises to address the complexity and challenges typically encountered during EGIT implementation. There are three interrelated components to the life cycle, as illustrated in **figure 3.3**:

1. The core EGIT continual improvement life cycle
2. Change enablement (addressing behavioral and cultural aspects of implementation or improvement)
3. Program management

Figure 3.3 depicts the initiatives as continual life cycles to emphasize the fact that they are not isolated, discontinuous or one-off activities. Instead, they form an ongoing process of implementation and improvement that ultimately becomes business as usual—at which point, the program can be retired.

Figure 3.3—Applying a Continual Improvement Life Cycle Approach

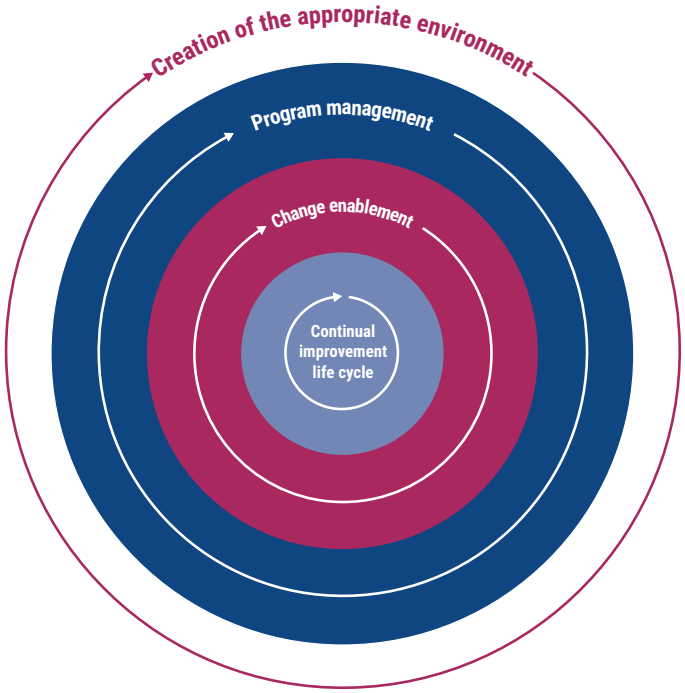
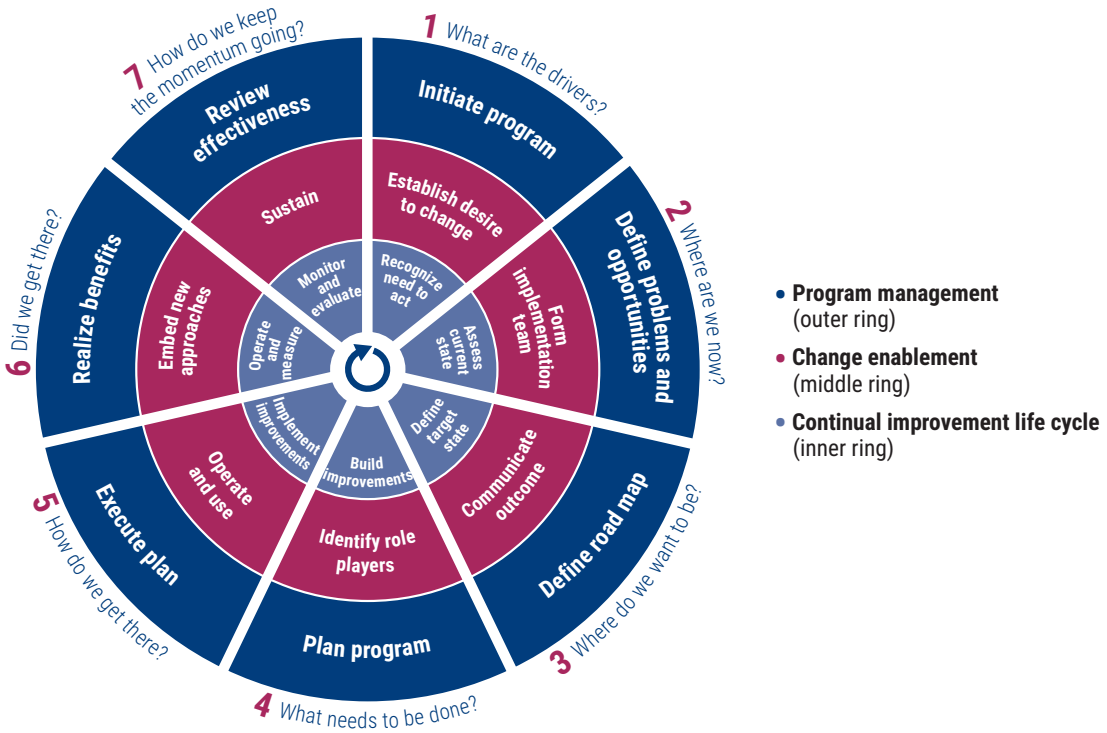


Figure 3.4 illustrates the seven phases of the implementation road map. High-level health checks, assessments and audits often trigger consideration of an EGIT initiative, and their results can become input to phase 1. An implementation and improvement program is typically continual and iterative. During its last phase, new objectives and requirements often surface, and a new cycle may begin.

Figure 3.4—COBIT Implementation Road Map



3.2.1 Phase 1—What Are the Drivers?

Phase 1 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 stimulus for change. Events, trends (industry, market or technical), performance shortfalls, software implementations and even the goals of the enterprise can 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 the improvement of the governance system. They ensure a continuous focus on the benefits of the program and their realization.

3.2.2 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 governance and management objectives. The *COBIT® 2019 Design Guide* provides several design factors to help with the selection.

Based on the selected enterprise and alignment 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.

3.2.3 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.

3.2.4 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.

3.2.5 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.

3.2.6 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.

3.2.7 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.

The time spent per phase will differ greatly depending on the enterprise environment, its maturity, and the scope of the implementation or improvement initiative (among other factors). However, the overall time spent on each iteration of the full life cycle ideally should not exceed six months, with improvements applied progressively. Otherwise, the program risks losing momentum, focus and buy-in from stakeholders. The goal is to establish a rhythm of regular improvement. Larger-scale initiatives should be structured as multiple iterations of the life cycle.

Over time, the life cycle will be followed iteratively while building a sustainable approach. Phases of the life cycle become everyday activities; continual improvement occurs naturally and becomes normal business practice.

3.3 Getting Started—Identify the Need to Act: Recognizing Pain Points and Trigger Events

Many factors can indicate a need for new or revised EGIT practices—and when studied closely, they sometimes reveal complex networks of underlying issues. For example, if the business has the perception that I&T costs are unacceptably high, this may be due to governance and/or management issues (e.g., the use of inappropriate criteria in managing IT investment). But, the pain point may be a symptom of long-term, legacy underinvestment in I&T that now manifests in significant, new or ongoing cost.

Using pain points or trigger events to launch EGIT initiatives makes it possible to relate the business case for improvement to concrete stakeholder issues, and thereby improve buy-in. A sense of urgency within the enterprise may be necessary to kick-start implementation. In addition, it can support quick wins and demonstrate the addition of value in areas that are the most visible or recognizable in the enterprise. Quick wins, in turn, provide a platform for introducing further changes and can help consolidate widespread commitment from senior management, along with support for more pervasive improvement.

3.3.1 Typical Pain Points

New or revised EGIT practices can typically solve—or help to address—the following symptoms, which were also listed in the *COBIT® 2019 Design Guide* under Design Factor 4 *I&T-related issues*. (Please note that this list is not exhaustive, and that each organization has their own issues to address.)

- **Frustration between different IT entities across the organization because of a perception of low contribution to business value**—More and more enterprises have decentralized or decoupled IT entities; each provides specific (and often discontinuous) services to its stakeholders. Dependencies may persist among the groups; when dependencies are not carefully managed, they may compromise IT effectiveness and efficiency.
- **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**—While many enterprises continue to increase their investments in I&T, the value of these investments and overall performance of IT are often questioned and/or not fully understood. This frustration can indicate an EGIT issue, and suggests improving communication between IT and the business, and/or establishing a common view on the role and value of IT. It can also be a consequence of suboptimal portfolio and project formulation, proposal and approval mechanisms.
- **Significant I&T-related incidents, such as data loss, security breaches, project failure, application errors, linked to IT**—Significant incidents (including data loss, security breaches, project failure and application errors linked to IT) are often the tip of the iceberg and their impact can be exacerbated if they receive public and/or media attention. Further investigation often leads to the identification of deeper, structural misalignments—or even the complete lack of an IT risk-aware culture within the enterprise. Stronger EGIT practices are typically required to understand and manage IT-related risk comprehensively.
- **Service delivery problems by the IT outsourcer(s)** —Issues with service delivery from external service providers (e.g., consistent failure to meet agreed service levels) may be due to governance issues. For example, defined third-party service management processes may be lacking or inadequately tailored (including control and monitoring), and/or lack proper responsibilities and accountabilities to fulfill business and IT-service requirements.
- **Failure to meet IT-related regulatory or contractual requirements**—In many enterprises, ineffective or inefficient governance mechanisms prevent complete integration of relevant laws, regulations and contractual terms into organizational systems. Alternatively, laws, regulations and contractual terms may be integrated, but the enterprise still lacks an approach for managing them. (Regulations and compliance requirements continue to proliferate globally, and often affect IT-enabled activities directly.)

- **Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems** —Poor assessments may indicate that service levels are not in place or not functioning well, or that the business is not adequately involved in IT decision making.
- **Substantial hidden and rogue IT spending**—Excessive spending outside of normal IT investment decision mechanisms and approved budgets often indicates a lack of sufficiently transparent and comprehensive control over IT expenditures and investments. IT spending can be hidden or misclassified in business-unit budgets, creating an overall biased view of IT costs.
- **Duplications or overlaps between various initiatives, or other forms of wasted resources** —Duplicative projects and/or redundant deployment of resources may result when I&T initiatives are not fully represented in a single, comprehensive view of the portfolio. Process and decision-structure capabilities around portfolio and performance management may not be in place.
- **Insufficient IT resources, staff with inadequate skills and staff burnout/dissatisfaction**—These are significant IT human resource management issues that require effective oversight and good governance to address people management and skills development effectively. They may also indicate underlying weaknesses in IT-demand management and internal service-delivery practices (among other latent issues).
- **IT-enabled changes or projects frequently failing to meet business needs and delivered late or over budget**—These pain points could relate to problems with business-IT alignment, poor definition of business requirements, lack of a benefit-realization process, suboptimal implementation or issues in project/program management processes.
- **Multiple and complex IT assurance efforts**—This scenario could indicate poor coordination between the business and IT regarding the need for, and execution of, IT-related assurance reviews. A low level of business trust in IT may prompt the business to initiate its own reviews. Alternatively, it could suggest a lack of business accountability for, or involvement in, IT-assurance reviews, if the business is simply not aware when reviews take place.
- **Reluctance of board members, executives or senior management to engage with IT, or lack of committed business sponsors for IT**—These pain points often indicate a lack of business understanding and insight into IT, insufficient IT visibility at appropriate levels, or ineffective management structures. The pain points may also indicate issues with board mandates, which are often caused by poor communication between the business and IT, and/or misunderstanding of the business and IT by the business sponsors for I&T.
- **Complex IT operating model and/or unclear decision mechanisms for IT-related decisions**—Decentralized or federated IT organizations often have different structures, practices and policies. The resulting complexity requires a strong focus on EGIT to ensure optimal IT decision making, and effective and efficient operations. This pain point often becomes more significant with globalization: each territory or region may have specific (and potentially unique) internal and external environmental factors to be addressed.
- **Excessively high cost of IT**—IT is often perceived as a cost to the organization—a cost that should be kept as low as possible. This issue typically occurs when IT budgets are spent primarily on projects that bring little value to the business, keeping the lights on, instead of bringing new opportunities and innovation. Lack of a holistic, portfolio view of all I&T initiatives can contribute to excess cost and may indicate that process and decision-structure capabilities around portfolio and performance management are not in place.
- **Obstructed or failed implementation of new initiatives or innovations caused by the current IT architecture and systems** —In many organizations, legacy IT architecture does not allow much flexibility in the implementation of new, innovative solutions. Digitization often requires fast action and agile responses to changing circumstances. It requires a new, more flexible approach to IT development and operations, and therefore directly implicates the governance system.
- **Gap between business and technical knowledge**—Business users and IT specialists often speak different languages. When business users lack sufficient understanding of I&T, or fail to grasp how I&T can improve the business—or conversely, when IT specialists misconstrue challenges and opportunities in the business context—the enterprise cannot grow and innovate as it should to be successful. This situation requires good governance to ensure that people management and skills development are addressed effectively.

- **Regular issues with data quality and integration of data across various sources**—Enterprises increasingly realize the potential value that may be hidden in their information. All issues of data quality or data integration can have a substantial impact on the success of the enterprise. EGIT is key to establishing the right processes, roles, responsibilities, culture, etc., to deliver business value from information.
- **High level of end-user computing, creating (among other issues) a lack of oversight and quality control over the applications that are being developed and put in operation**—A high level of end-user computing may strain communication between IT and the business, and could entail loose controls around installation of business applications. It may result from suboptimal portfolio and project formulation, and/or inadequate proposal and approval mechanisms. EGIT can help establish a common view on the role and value of IT to optimize security and functionality of end-user devices.
- **Business departments implementing their own information solutions with little or no involvement of the enterprise IT department** —This pain point may relate to the end-user computing issue and the optimal use of data and information; however, it primarily results when the business attempts to implement more robust solutions and services in the normal course of pursuing business advantage. Lack of communication or trust between business and IT can contribute to unsanctioned, independent development, or exacerbate its symptoms (in the form of service issues, etc.).
- **Ignorance of and/or noncompliance with security and privacy regulations**—Mitigating new security and privacy threats should be on the agenda of every enterprise, not only for compliance reasons but also to preserve the value the enterprise generates. Ignorance and/or noncompliance with regulations can seriously impair the enterprise and should be managed through proper EGIT.
- **Inability to exploit new technologies or innovate using I&T**—A common business complaint casts IT in a supporting role, whereas the enterprise needs IT to innovate and provide a competitive edge. Such complaints may point to a lack of true bidirectional alignment between business and IT, which could reflect communication issues or a need to increase business involvement in IT decision making. Alternatively, the business may involve IT too late in its strategic planning or business initiatives. The issue often arises most emphatically when economic conditions require rapid enterprise responses, such as the introduction of new products or services.

3.3.2 Trigger Events in the Internal and External Environments

In addition to the paint points described in Section 3.3.1, other events in the enterprise's internal and external environments can signal or trigger a focus on EGIT and drive it high on the enterprise agenda.

- **Merger, acquisition or divestiture**—These transactions may result in significant strategic and operational consequences relating to I&T. Due diligence reviews must gain an understanding of IT issues in the environment(s). Integration or restructuring requirements may prescribe EGIT mechanisms appropriate for the new environment.
- **Shifts in the market, economy or competitive position**—An economic downturn could lead enterprises to revise EGIT mechanisms to facilitate large-scale cost optimization or performance improvement.
- **Changes in business operating model or sourcing arrangements**—Moving from a decentralized or federated model to a more centralized operating model will require changes to EGIT practices to enable more centralized IT decision making. Implementation of shared service centers for areas like finance, human resources (HR) or procurement can also require increased EGIT. Fragmented IT application or infrastructure domains may be consolidated, with associated changes in the IT decision-making structures or processes that govern them. The outsourcing of some IT functions and business processes may similarly lead to a renewed focus on EGIT. A change in risk appetite can influence EGIT arrangements, if, for example, an enterprise decides to accept more risk in pursuing its objectives.
- **New regulatory or compliance requirements**—Complying with laws and regulations often has EGIT ramifications. For example, expanded corporate governance reporting requirements and financial regulations often trigger a need for better EGIT as well as a focus on information privacy, given the pervasiveness of IT.

- **Significant technology change or paradigm shifts**—Some enterprises have migrated to a service-oriented architecture (SOA) and cloud computing. These kinds of initiatives fundamentally change the way that infrastructure and application functionality are developed and delivered, and may require changes in the governance and management of associated processes and other components.
- **Enterprisewide governance focus or project**—Large-scale projects, including, for example, broad changes in company policies, are likely to trigger initiatives in the EGIT area.
- **New leadership**—The appointment of new C-level representatives, including the chief information officer (CIO), chief financial officer (CFO), chief executive officer (CEO) or board members, often triggers an assessment of current EGIT mechanisms and initiatives to address any weak areas.
- **External audit or consultant assessments**—An assessment against appropriate practices, performed by an independent third party, can be the starting point of an EGIT improvement initiative.
- **New business strategy or priority**—Pursuing a new business strategy often has EGIT implications. For example, a business strategy of being close to customers—knowing who they are, understanding their requirements and responding in the best possible manner—may require more freedom of IT decision making (for a given business unit or country), as opposed to centralized decision making at the corporate or holding-company level.
- **Desire to significantly improve the value gained from I&T**—A need to improve competitive advantage, innovate, optimize assets or create new business opportunities can call attention to EGIT.

These triggers have a direct link to the design factors that are explained in detail in the *COBIT® 2019 Design Guide*. The enterprise builds and tailors its governance system based on a number of design factors. Changes in those design factors trigger a review of EGIT. For example, enterprise strategy is an important design factor and correlates directly to trigger events such as acquisitions, shifts in the market or a new business strategy. Another important design factor is the level of compliance requirements to which the enterprise is subject, which directly links to trigger events such as new regulatory or compliance requirements.

The identification of pain points and internal or external trigger events leads to recognition, solicitation and communication of the need to act. This communication can take the form of a wake-up call (when pain points are experienced), or express the improvement opportunity and benefits that may be realized. Current EGIT pain points or trigger events provide starting points. They can typically be identified through high-level health checks, diagnostics or capability assessments. These techniques have the added benefit of creating consensus on the issues to be addressed. It can be beneficial to obtain a third party's independent and objective high-level review of the current situation (which may increase buy-in to act).

It is critical to strive for commitment and buy-in from the board and executive management from the beginning. To do this, the EGIT program and its objectives and benefits need to be clearly expressed in business terms. The correct level of urgency must be instilled. The board and executive management should be made aware of the value that well-governed and -managed I&T can bring to the enterprise and the risk of not taking action. Engagement of the board and senior management also supports up-front consideration of alignment among the EGIT program, enterprise objectives and strategy, enterprise objectives for IT, enterprise governance, and ERM initiatives (if existing). Identifying and realizing some quick wins (visible issues that can be addressed relatively quickly, and help establish credibility of the overall initiative by demonstrating benefits) can be a useful mechanism for obtaining board commitment.

Once the direction has been set at the top, an overall view of change enablement at all levels should be established. The wider scale and scope of change must be understood first in hard business terms, but the human and behavioral perspective cannot be overlooked. All stakeholders involved in, or affected by, the change need to be identified, and their position relative to the change should be established.

3.3.3 Stakeholder Involvement

Many stakeholders need to collaborate to achieve the overall objective of improved IT performance. The approach provided in this guide will help to develop an agreed and common understanding of what needs to be achieved to satisfy specific stakeholder concerns in a coordinated and harmonized way. The most important stakeholders and their concerns are:

- **Board and executive management**—How do we set and define enterprise direction for the use of I&T and monitor the establishment of relevant and required EGIT components, so that business value is delivered, and IT-related risk is mitigated?
- **Senior business management, IT management**[10] **and process owners**—How do we enable the enterprise to define alignment goals to ensure that business value is delivered from the use of I&T and that IT-related risk is mitigated?
- **Business management, IT management and process owners**—How do we plan, build, deliver and monitor information and IT solutions and service capabilities as required by the business and directed by the board?
- **Risk, compliance and legal experts**—How do we ensure that the enterprise complies with policies, regulations, laws and contracts, and that risk is identified, assessed and mitigated?
- **Internal audit**—How do we provide independent assurance on value delivery and risk mitigation?

Key success factors for implementation are:

- Board provides direction, and executive management provides the mandate and resources.
- All parties understand the enterprise and I&T-related objectives.
- Effective communication and enablement of the necessary organizational and process changes exist.
- Frameworks and good practices are tailored to fit the purpose and design of the enterprise.
- The initial focus is on quick wins and the prioritization of the most beneficial improvements that are easiest to implement. This demonstrates benefits and builds confidence for further improvement.

3.4 Recognizing Stakeholders' Roles and Requirements

3.4.1 Internal Stakeholders

Figure 3.5 provides an overview of internal stakeholders, their most important high-level responsibilities and accountabilities in the improvement process, and their interest in the outcomes of the implementation program. The following stakeholders represent generic examples; some adaptation, extension and customization will be required.

[10] IT management includes all roles within the IT function at a management level.

Figure 3.5—Overview of Internal EGIT Stakeholders		
Internal Stakeholders	**Important High-Level Accountabilities and Responsibilities**	**Interest in the Implementation Program Outcomes**
Board and executive management	Set the overall direction, context and objectives for the improvement program and ensure alignment with the enterprise business strategy, governance and risk management. Provide visible support and commitment for the initiative, including the roles of sponsoring and promoting the initiative. Approve the outcomes of the program, and ensure that envisioned benefits are attained and corrective measures are taken as appropriate. Ensure that the required resources (financial, human and other) are available to the initiative. Set the direction at the top and lead by example.	The board and executive management are interested in obtaining the maximum business benefits from the implementation program. They want to ensure that all relevant, required issues and areas are addressed; required activities are undertaken; and expected outcomes are successfully delivered.
Business management and business process owners	Provide applicable business resources to the core implementation team. Work with IT to ensure that the outcomes of the improvement program are aligned to and appropriate for the business environment of the enterprise, value is delivered, and risk is managed. Visibly support the improvement program and work with IT to address any issues that are experienced. Ensure that the business is adequately involved during implementation and in the transition to use.	These stakeholders would like the program to result in better alignment of I&T with the overall business environment and their specific areas.
Chief information officer (CIO)	Provide leadership to the program and applicable IT resources to the core implementation team. Work with business management and executives to set the appropriate objectives, direction and approach for the program.	The CIO wants to ensure that all EGIT implementation objectives are attained. For the CIO, the program should result in mechanisms that will continually improve the relationship with, and alignment to, the business (including having a shared view on I&T performance); lead to better management of IT supply and demand; and improve the management of I&T-related business risk.
IT management and IT process owners (such as the head of operations, chief architect, IT security manager, privacy officer, business continuity management specialist)	Provide leadership for applicable work streams of the program and resources to the implementation team. Give key input into the assessment of current performance and setting of improvement targets for process areas with the respective domains. Provide input on relevant good practices that should be incorporated and related expert advice. Ensure that the business case and program plan are realistic and achievable.	These stakeholders are interested in ensuring that the improvement initiative results in better governance of I&T overall and in their individual areas, and the business inputs required to do so are obtained in the best possible way.
Compliance, risk management and legal experts	Participate as required throughout the program and provide compliance, risk management and legal inputs on relevant issues. Ensure alignment with the overall ERM approach and confirm that relevant compliance and risk management objectives are met, issues are considered and benefits are attained. Provide guidance as required during implementation.	These stakeholders want to ensure that the initiative establishes or improves the mechanisms for ensuring legal and contract compliance and effective I&T-related business risk management, and alignment of these mechanisms to any enterprisewide approaches that may exist.

Figure 3.5—Overview of Internal EGIT Stakeholders *(cont.)*		
Internal Stakeholders	**Important High-Level Accountabilities and Responsibilities**	**Interest in the Implementation Program Outcomes**
Internal audit	Participate as required throughout the program and provide audit inputs on relevant issues. Provide advice on current issues being experienced and input on control practices and approaches. Review the feasibility of business cases and implementation plans. Provide advice and guidance as required during implementation. Potentially verify assessment results independently.	These stakeholders are interested in the outcomes of the implementation program related to control practices and approaches, and how the mechanisms that are established or improved will enable current audit findings to be addressed.
Implementation team (combined business and IT team, consisting of individuals from previously listed stakeholder categories)	Direct, design, control, drive and execute the end-to-end program from the identification of objectives and requirements to the eventual evaluation of the program against business case objectives and the identification of new triggers and objectives for further implementation or improvement cycles. Ensure skills transfer during the transition from the implementation environment to the operation, use and maintenance environments.	The team wants to ensure that all envisioned outcomes of the EGIT initiative are obtained and maximized.
Users	Support EGIT by performing specific roles and responsibilities as assigned to them.	These stakeholders are interested in the impact(s) the initiative will have on their day-to-day lives—their jobs, roles and responsibilities, and activities.
Customers		Customers are part of the extended value chain and have expectations regarding delivery of services, products, etc.

3.4.2 External Stakeholders

In addition to the internal stakeholders listed in **figure 3.5**, there are also several external stakeholders. While these stakeholders do not have any direct accountabilities or responsibilities in the improvement program, they may have requirements that need to be satisfied. **Figure 3.6** presents generic examples.

Figure 3.6—Overview of External EGIT Stakeholders	
External Stakeholders	**Interest in the Implementation Program Outcomes**
Customers and society	Organizations exist to serve customers. Thus, customers are directly affected by the degree to which an enterprise's EGIT objectives are met. If an enterprise is exposed in the security and privacy domain, such as through loss of customer banking data, the customer will be affected, and thus has an interest in the successful outcomes of the EGIT implementation program.
IT service providers	Enterprise management should ensure that there is alignment and interface between the enterprise's own overall EGIT and the governance and management of the services provided by IT service providers.
Regulators	Regulators are interested in whether the implementation program outcomes satisfy and/or provide structures and mechanisms to satisfy all applicable regulatory and compliance requirements.
Shareholders (where relevant)	Shareholders may partially base investment decisions on the state of an enterprise's corporate and EGIT governance and its record of accomplishment in this area.

Figure 3.6—Overview of External EGIT Stakeholders *(cont.)*	
External Stakeholders	**Interest in the Implementation Program Outcomes**
External auditors	External auditors may be able to rely on I&T-related controls more fully as a result of an effective implementation program, as substantiated by an audit. They are also interested in regulatory compliance aspects and financial reporting.
Business partners (e.g., suppliers)	Business partners that use automated electronic transactions with the enterprise could have an interest in the outcomes of the implementation program with respect to improved information security, integrity and timeliness. They may also be interested in regulatory compliance and international standards certifications that could be outcomes of the program.

3.4.3 Independent Assurance and the Role of Auditors

IT managers and stakeholders need to be aware of the role of assurance professionals. Assurance professionals can be internal auditors, external auditors, International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) standards auditors, or any professionals commissioned to provide an assessment on IT services and processes. It is important to take these stakeholders and their interests into account when defining the EGIT implementation plan. Increasingly, boards and executive management seek independent advice and opinions regarding critical I&T functions and services. There is also a general increase in the need to demonstrate compliance with national and international regulations.

Page intentionally left blank

Chapter 4
Identifying Challenges and Success Factors

4.1 Introduction

Experiences from EGIT implementations have shown that several practical issues need to be overcome for the initiative to be successful and for continual improvement to be sustained. This chapter describes several of these challenges, their likely root causes and the factors that should be considered to ensure successful outcomes.

4.2 Creating the Appropriate Environment

4.2.1 Phase 1—What Are the Drivers?

Figure 4.1 lists challenges, their root causes and success factors for phase 1.

Figure 4.1—Challenges, Root Causes and Success Factors for Phase 1

Phase 1—What Are the Drivers?	
Challenges	• Lack of senior management buy-in, commitment and support • Difficulty in demonstrating value and benefits
Root causes	• Lack of understanding (and evidence) of the importance, urgency and value of improved governance to the enterprise • Lack of resources • Poor understanding of the scope of EGIT and the differences between governance and management of I&T • Implementation driven by a short-term reaction to a problem rather than a proactive, broader justification for improvement • Concern about "another project likely to fail"; lack of trust in IT management • Poor communication of governance issues and benefits; benefits and time frames not clearly articulated • No senior executive willing to sponsor or be accountable • Poor perception of the credibility of the IT function; CIO does not command enough respect • Executive management's belief that EGIT is the responsibility of IT management only • Not having the appropriate team (role players) responsible for EGIT or adequate skills to undertake the task • Lack of use of recognized frameworks/lack of training and awareness • Incorrect positioning of EGIT in the context of current enterprise governance • Initiative driven by enthusiastic "converts" who preach textbook approaches
Success factors	• Make EGIT a board, audit committee and risk committee agenda item for discussion. • Create a committee or leverage an existing committee, such as the I&T governance board, to provide a mandate and accountability for action. • Avoid making EGIT appear to be a solution looking for a problem. There must be a real need and potential benefit. • Identify leader(s) and sponsor(s) with the authority, understanding and credibility to take ownership of implementation success. • Identify and communicate pain points that can motivate a desire to change the status quo. • Use language, approaches and communications appropriate to the audience. Avoid jargon and terms the audience members cannot recognize. • Jointly (with the business) define and agree on expected value from IT. • Express benefits in (agreed) business terms/metrics. • Obtain support from, and augment skills with, external auditors, consultants and advisors, if required. • Develop guiding principles that set the tone and scene for the transformation effort.

Figure 4.1—Challenges, Root Causes and Success Factors for Phase 1 *(cont.)*	
Phase 1—What Are the Drivers?	
	• Produce imperatives based on the transformation effort particular to the enterprise, building in the trust and partnership necessary for success. • Produce a business case tailored for a targeted audience that demonstrates the business benefits of the proposed IT investment. • Prioritize and align the business case based on the strategic focus and current enterprise pain points. • Align the business case with overall enterprise governance objectives. • Gain education and training in EGIT issues and frameworks.
Challenges	• Difficulty in getting the required business participation • Difficulty in identifying stakeholders and role players
Root causes	• EGIT not a priority for business executives (not a key performance indicator [KPI]) • IT management's preference to work in isolation (proving the concept before involving the customer) • Barriers between IT and the business, inhibiting participation • No clear roles and responsibilities for business involvement • Key business individuals and influencers not involved or engaged • Business executives' and process owners' limited understanding of the benefits and value of EGIT
Success factors	• Encourage top management and the I&T governance board to set mandates and insist on business roles and responsibilities in EGIT. • Put in place a process for engaging stakeholders. • Explain and sell business benefits clearly. • Explain the risk of noninvolvement. • Identify critical services or major IT initiatives to use as pilots/models for business involvement in improved EGIT. • Find the believers (business users who recognize the value of better EGIT). • Promote free thinking and empowerment, but only within well-defined polices and a governance structure. • Ensure that those who are responsible for and need to drive change are the ones to gain sponsor support. • Create forums for business participation—for example, the I&T governance board—and run workshops to openly discuss current problems and opportunities for improvement. • Involve business representatives in high-level current-state assessments.
Challenge	• Lack of business insight among IT management
Root causes	• Poor corporate governance performance • IT leadership with an operational technical background—not involved enough in enterprise business issues • IT management isolated within the enterprise—not involved at senior levels • Weak business relationship process • Legacy of perceived poor performance that has driven IT and the CIO into a defensive mode of operation • CIO and IT management in a vulnerable position, unwilling to reveal internal weaknesses
Success factors	• Enhance credibility by building on successes and performance of respected IT staff. • Make IT management a permanent member of the enterprise executive committee (if possible), to ensure that IT management has adequate business insight and is involved early in new initiatives. • Implement an effective business relationship process. • Invite business participation and involvement. Consider placing business people in IT and vice versa to gain experience and improve communications. • If necessary, reorganize IT management roles and implement formal links to other business functions, such as finance and HR. • Ensure that the CIO has business experience. Consider appointment of a CIO from the business. • Use consultants to create a stronger business-oriented EGIT strategy. • Create governance mechanisms, such as business relationship managers within IT, to enable greater business insight.

Figure 4.1—Challenges, Root Causes and Success Factors for Phase 1 *(cont.)*	
Phase 1—What Are the Drivers?	
Challenges	• Lack of current enterprise policy and direction • Weak current enterprise governance
Root causes	• Commitment and leadership issues, possibly due to organizational immaturity • Autocratic leadership based on individual commands rather than on enterprise policy • Culture's promotion of free thinking and informal approaches rather than a control environment • Weak enterprise risk management
Success factors	• Raise issues and concerns with board-level executives and nonexecutives about the risk of poor governance, based on real issues related to compliance and enterprise performance. • Raise issues with the audit committee or internal audit. • Obtain input and guidance from external auditors. • Consider how the culture might need to be changed to enable improved governance practices. • Raise the issue with the CEO and board of directors. • Ensure that risk management is applied across the enterprise.

4.2.2 Phase 2—Where Are We Now? and Phase 3—Where Do We Want to Be?

Figure 4.2 lists the challenges, their root causes and success factors for phases 2 and 3.

Figure 4.2—Challenges, Root Causes and Success Factors for Phases 2 and 3	
Phase 2—Where Are We Now? Phase 3—Where Do We Want to Be?	
Challenges	• Inability to gain and sustain support for improvement objectives • Communication gap between IT and the business
Root causes	• Compelling reasons to act not clearly articulated or nonexistent • Failure of perceived benefits to sufficiently justify required investment (cost) • Concern about loss of productivity or efficiency due to change • Lack of clear accountabilities for sponsoring and committing to improvement objectives • Lack of appropriate structures with business involvement from strategy to tactical and operational levels • Inappropriate way of communicating (not sufficiently simple, not sufficiently brief, not conveyed in business language, not suited to politics and culture) or not adapting style to different audiences • Business case for improvements not well developed or articulated • Insufficient focus on change enablement and obtaining buy-in at all required levels
Success factors	• Develop agreed understanding of the value of improved EGIT. • Have the appropriate structures, such as an IT steering committee and an audit committee, facilitate communication and agreement of objectives and establish meeting schedules to exchange strategy status, clarify misunderstandings and share information. • Implement an effective business-relationship process. • Develop and execute a change enablement strategy and communication plan explaining the need to reach a higher level of maturity. • Use the correct language and common terminology with a style adapted to audience subgroups. Make it interesting, use visuals. • Develop the initial EGIT business case into a detailed business case for specific improvements, with clear articulation of risk. Focus on added value for the business (expressed in business terms) as well as costs. • Educate and train in COBIT and this implementation method.
Challenge	• Cost of improvements outweighing perceived benefits
Root causes	• Tendency to focus solely on controls and performance improvements, not on efficiency improvements and innovation • Improvement program inadequately phased and failing to clearly associate improvement benefits and cost • Prioritization of complex, expensive solutions rather than lower-cost, easier solutions • Significant IT budget and workforce already committed to maintenance of existing infrastructure, resulting in a limited appetite to direct funds or staff time left to deal with EGIT

Figure 4.2—Challenges, Root Causes and Success Factors for Phases 2 and 3 *(cont.)*	
Phase 2—Where Are We Now? Phase 3—Where Do We Want to Be?	
Success factors	• Identify areas in infrastructure, processes and HR—such as standardization, higher maturity levels and fewer incidents—where efficiencies and direct cost savings can be made by better governance. • Prioritize based on benefit and ease of implementation, especially quick wins.
Challenge	• Lack of trust and good relationships between IT and the enterprise
Root causes	• Legacy issues underpinned by poor IT track record on project and service delivery • Lack of IT understanding of business issues and vice versa • Scope and expectations not properly articulated and managed • Unclear governance roles, responsibilities and accountabilities in business, causing abdication of key decisions • Lack of supporting information and metrics illustrating the need to improve • Reluctance to be proven wrong, general resistance to change
Success factors	• Foster open and transparent communication about performance, with links to corporate performance management. • Focus on business interfaces and service mentality. • Publish positive outcomes and lessons learned to help establish and maintain credibility. • Ensure that the CIO has credibility and leadership in building trust and relations. • Formalize governance roles and responsibilities in the business so that accountability for decisions is clear. • Identify and communicate evidence of real issues, risk that needs to be avoided and benefits to be gained (in business terms), relating to proposed improvements. • Focus on change enablement planning.

4.2.3 Phase 4—What Needs to Be Done?

Figure 4.3 lists the challenges, their root causes and success factors for phase 4.

Figure 4.3—Challenges, Root Causes and Success Factors for Phase 4	
Phase 4—What Needs to Be Done?	
Challenge	• Failure to understand the environment
Root causes	• Insufficient consideration of changes needed in the organization and its culture, as well as stakeholder perceptions • Insufficient consideration of existing governance strengths and practices within IT and the wider enterprise
Success factors	• Perform a stakeholder assessment and focus on developing a change enablement plan. • Build on and use existing strengths and good practices within IT and the wider enterprise. Avoid reinventing wheels just for IT. • Understand the different constituencies, their objectives and mindsets.
Challenge	• Various levels of complexity (technical, organizational, operating model)
Root causes	• Poor understanding of EGIT practices • Attempting to implement too much at once • Prioritizing critical and difficult improvements with little practical experience • Complex and/or multiple corporate operating models
Success factors	• Educate and train in COBIT and this implementation method. • Break down into smaller projects, building a step at a time. Prioritize quick wins. • Collect the needs for improvement from different constituencies. Correlate and prioritize them and map them to the change enablement program. • Focus on business priorities to phase implementation.

Figure 4.3—Challenges, Root Causes and Success Factors for Phase 4 *(cont.)*	
Phase 4—What Needs to Be Done?	
Challenge	• Difficulty in understanding COBIT and associated frameworks, procedures and practices
Root causes	• Inadequate skills and knowledge • Copying good practices, not adapting them • Focusing only on procedures, not on other enablers such as roles and responsibilities and skills applied
Success factors	• Educate and train in COBIT, other related standards and good practices, and this implementation method. • If required, obtain qualified and experienced external guidance and support. • Adapt and tailor good practices to suit the enterprise environment. • When designing processes, consider and deal with required skills, roles and responsibilities, process ownership, goals and objectives, and other governance components.
Challenge	• Resistance to change
Root causes	• Resistance is a natural behavioral response when the status quo is threatened, but it may also indicate underlying concerns such as: ▪ Misunderstanding of what is required and why it is useful ▪ Perception that workload and cost will increase ▪ Reluctance to admit shortcomings ▪ Not-invented-here syndrome underpinned by forcing generic governance frameworks onto the enterprise ▪ Entrenched thinking, threat to role or power base, not understanding “what’s in it for me”
Success factors	• Focus awareness communications on specific pain points and drivers. • Raise awareness by educating business and IT managers and stakeholders. • Use an experienced change agent with business and IT skills. • Follow up at regular milestones to ensure that implementation benefits are realized by involved parties. • Go for quick and relatively easy wins as eye-openers to boost recognition of values provided. • Make generic frameworks such as COBIT relevant to the context of the enterprise. • Focus on change enablement planning such as: ▪ Development ▪ Training ▪ Coaching ▪ Mentoring ▪ Transferring skills • Organize communication sessions/road shows and find champions to promote the benefits.
Challenge	• Failure to adopt improvements
Root causes	• External experts designing solutions in isolation or imposing solutions without adequate explanation • Internal EGIT team operating in isolation and acting as an informal proxy for real process owners, causing misunderstandings and resistance to change • Inadequate support and direction from key stakeholders, resulting in EGIT projects producing new policies and procedures that have no valid ownership
Success factors	• Engage process owners and other stakeholders during design. • Use pilots and demos, where appropriate, to educate and obtain buy-in and support. • Start with quick wins, demonstrate benefits and build from there. • Look for champions who understand resistance, and want to improve, rather than forcing people who resist. • Encourage a management structure that assigns roles and responsibilities, commits to their continued operation, and monitors compliance. • Enforce knowledge transfer from the external experts to process owners. • Delegate responsibility and empower the process owners.
Challenge	• Difficulty in integrating internal governance approach with the governance models of outsourcing partners
Root causes	• Fear of revealing inadequate practices • Failure to define and/or share EGIT requirements with the outsource provider • Unclear division of roles and responsibilities • Differences in approach and expectations • Contractual arrangements in outsourcing contracts

Figure 4.3—Challenges, Root Causes and Success Factors for Phase 4 *(cont.)*	
Phase 4—What Needs to Be Done?	
Success factors	• Involve suppliers/third parties in implementation and operational activities where appropriate. • Incorporate conditions and the right to audit in contracts. • Look for ways to integrate frameworks and approaches. • Address roles, responsibilities and governance structures with third parties up front, not as an afterthought. • Match evidence (via audit and document review) of service provider processes, people and technology with required EGIT practices and levels.

4.2.4 Phase 5—How Do We Get There?

Figure 4.4 lists the challenges, their root causes and success factors for phase 5.

Figure 4.4—Challenges, Root Causes and Success Factors for Phase 5	
Phase 5—How Do We Get There?	
Challenge	• Failure to realize implementation commitments
Root causes	• Overly optimistic goals, underestimation of effort required • IT in fire-fighting mode and focused on operational issues • Lack of dedicated resources or capacity • Priorities incorrectly allocated • Scope misaligned with requirements or misinterpreted by implementers • Program management principles, such as business case, not well applied • Insufficient insight into business environment (for example, operating model)
Success factors	• Manage expectations. • Follow guiding principles. • Keep it simple, realistic and practical. • Break down the overall project into small, achievable projects. Build experience and benefits. • Ensure that the implementation scope underpins the requirements and all stakeholders have the same understanding of what the scope will deliver. • Focus on implementations that enable business value. • Ensure that dedicated resources are allocated. • Apply program management and governance principles. • Leverage existing mechanisms and ways of working. • Ensure adequate insight into the business environment.
Challenge	• Trying to do too much at once; tackling overly complex, overly difficult or simply too many problems
Root causes	• Lack of understanding of scope and effort (also for human aspects, lack of common language) • Not understanding capacity to absorb change (too many other initiatives) • Lack of formal program planning and management; not building a foundation and maturing the effort from there • Undue pressure to implement • Not capitalizing on quick wins • Reinventing the wheel and not using what is there as a base • Lack of insight into organizational landscape • Lack of skills
Success factors	• Apply program and project management principles. • Use milestones. • Prioritize 80/20 tasks (80 percent of the benefit with 20 percent of the effort) and be careful about sequencing in the correct order. Capitalize on quick wins. • Build trust/confidence. Have the skills and experience to keep it simple and practical. • Reuse what is there as a base.

Figure 4.4—Challenges, Root Causes and Success Factors for Phase 5 *(cont.)*	
Phase 5—How Do We Get There?	
Challenge	• IT and/or business in fire-fighting mode
Root causes	• Lack of resources or skills • Lack of internal processes, internal inefficiencies • Lack of strong IT leadership • Too many workarounds
Success factors	• Apply good management skills. • Gain commitment and drive from top management so people are made available to focus on EGIT. • Address root causes in the operational environment (external intervention, management prioritizing IT). • Apply tighter discipline over and management of business requests. • Use external resources where appropriate. • Obtain external assistance.
Challenge	• Lack of required skills and competencies, such as understanding governance, management, business, processes, soft skills
Root causes	• Insufficient understanding of COBIT and IT management good practices • Business and management skills often not included in training • IT staff not interested in business areas • Business staff not interested in IT
Success factors	• Focus on change enablement planning: ▪ Development ▪ Training ▪ Coaching ▪ Mentoring ▪ Feedback into recruitment process ▪ Cross-skilling

4.2.5 Phase 6—Did We Get There? and Phase 7—How Do We Keep the Momentum Going?

Figure 4.5 lists the challenges, root causes and success factors for phases 6 and 7.

Figure 4.5—Challenges, Root Causes and Success Factors for Phases 6 and 7	
Phase 6—Did We Get There? Phase 7—How Do We Keep the Momentum Going?	
Challenge	• Failure to adopt or apply improvements
Root causes	• Solutions too complex or impractical • Solutions developed in isolation by consultants or an expert team • Good practices copied, but not tailored to suit the enterprise operation • Solutions not owned by process owners/team • Organization lacking clear roles and responsibilities • Management not mandating and supporting change • Resistance to change • Poor understanding of how to apply the new processes or tools that have been developed • Skills and profile not matched with the requirements of the role

Figure 4.5—Challenges, Root Causes and Success Factors for Phases 6 and 7 *(cont.)*	
Phase 6—Did We Get There? Phase 7—How Do We Keep the Momentum Going?	
Success factors	• Focus on quick wins and manageable projects. • Make small improvements to test the approach and make sure it works. • Involve the process owners and other stakeholders in development of the improvement. • Make sure roles and responsibilities are clear and accepted. Change roles and job descriptions if required. • Drive the improvement from management down throughout the enterprise. • Apply adequate training where required. • Develop processes before attempting to automate. • Reorganize to enable better ownership of processes, if required. • Match roles (especially those that are key for successful adoption) to individual capabilities and characteristics. • Provide effective education and training.
Challenge	• Difficulty in showing or proving benefits
Root causes	• Goals and metrics not established or working effectively • Benefits tracking not applied after implementation • Loss of focus on benefits and value to be gained • Poor communication of successes
Success factors	• Set clear, measurable and realistic goals (outcome expected from the improvement). • Set practical performance metrics (to monitor whether the improvement is driving achievement of goals). • Produce scorecards showing how performance is being measured. • Communicate, in business impact terms, the results and benefits that are being gained. • Implement quick wins and deliver solutions in short time scales.
Challenge	• Lost interest and momentum, change fatigue
Root causes	• Continual improvement not part of the culture • Management not driving sustainable results • Resources focused on fire-fighting and service delivery, not on improvement • Personnel not motivated, cannot see the personal benefit in adopting and driving change
Success factors	• Ensure that management regularly communicates and reinforces the need for robust and reliable services, solutions and good governance. Communicate to all stakeholders the successful improvements already achieved. • Revisit stakeholders and get their support to fuel momentum. • Take opportunities to implement improvements on the job. if resources are scarce, as part of daily routine. • Focus on regular and manageable improvement tasks. • Obtain external assistance, but remain engaged. • Align personal reward systems with process and organization performance improvement targets and metrics.

Chapter 5
Enabling Change

5.1 The Need for Change Enablement

Successful implementation or improvement depends on implementing the appropriate change in the correct way. In many enterprises, there is a significant focus on the first aspect (implementing the good practices), but not enough on the second aspect, implementing change in the correct way by emphasizing management of the human, behavioral and cultural aspects of the change, and motivating stakeholders to buy into the change. Change enablement, which includes stakeholder management, is one of the biggest challenges to EGIT implementation.

It should not be assumed that the various stakeholders involved in, or affected by, new or revised governance arrangements will necessarily readily accept and adopt the change. The possibility of ignorance, resistance to change or change fatigue needs to be addressed through a structured and proactive approach.[11] Also, optimal awareness of the program should be achieved through a communication plan that defines what will be communicated, in what way, by whom and to whom, throughout the various phases of the program.

COBIT defines change enablement as a holistic and systematic process of ensuring that relevant stakeholders are prepared and committed to the changes involved in moving from a current state to a desired future state.

All key stakeholders should be involved. At a high level, change enablement typically entails:

- Assessing the impact of the change on the enterprise, its people and other stakeholders
- Establishing the future state (vision) in human/behavioral terms and the associated measures that describe it
- Building change response plans to manage change impacts proactively and maximize engagement throughout the process. These plans may include training, communication, organization design (job content, organizational structure), process redesign and updated performance management systems.
- Continually measuring the progress of change toward the desired future state

Although every EGIT implementation is different, a common objective of change enablement is having enterprise stakeholders from the business and IT lead by example, and encourage staff at all levels to work according to the desired new way. Examples of desired behavior include:

- Following agreed processes
- Participating in defined EGIT structures such as a change approval or advisory board
- Enforcing defined guiding principles, policies, standards, processes or practices (such as a policy regarding new investments or security)

This can be best achieved by gaining the commitment of the stakeholders (diligence and due care, leadership, and communicating and responding to the workforce) and selling the benefits. If necessary, it may be required to enforce compliance. In other words, human, behavioral and cultural barriers must be overcome to establish a common interest in properly adopting the new way, instill the will to adopt it and ensure the ability to adopt it. It may be useful to draw on change enablement skills within the enterprise or, if necessary, from external consultants to facilitate the change in behavior.

[11] When reviewing a major IT transformation initiative, the US Department of Veterans Affairs (VA) noted, "The primary challenge the VA will face in achieving this transformation will be gaining the acceptance and support of all VA personnel, including leadership, middle managers and field staff." See Walters, J.; "Transforming Information Technology at the Department of Veterans Affairs," IBM Center for the Business of Government, USA, 2009, *http://www.isaca.org/Knowledge-Center/cobit/Documents/WaltersVAReport-June09.pdf.* The VA has stated that its effort cannot succeed if it addresses only technological transformation; it recognizes that the human factor that is needed to achieve acceptance, change the organization and change the way business is conducted is critical to success.

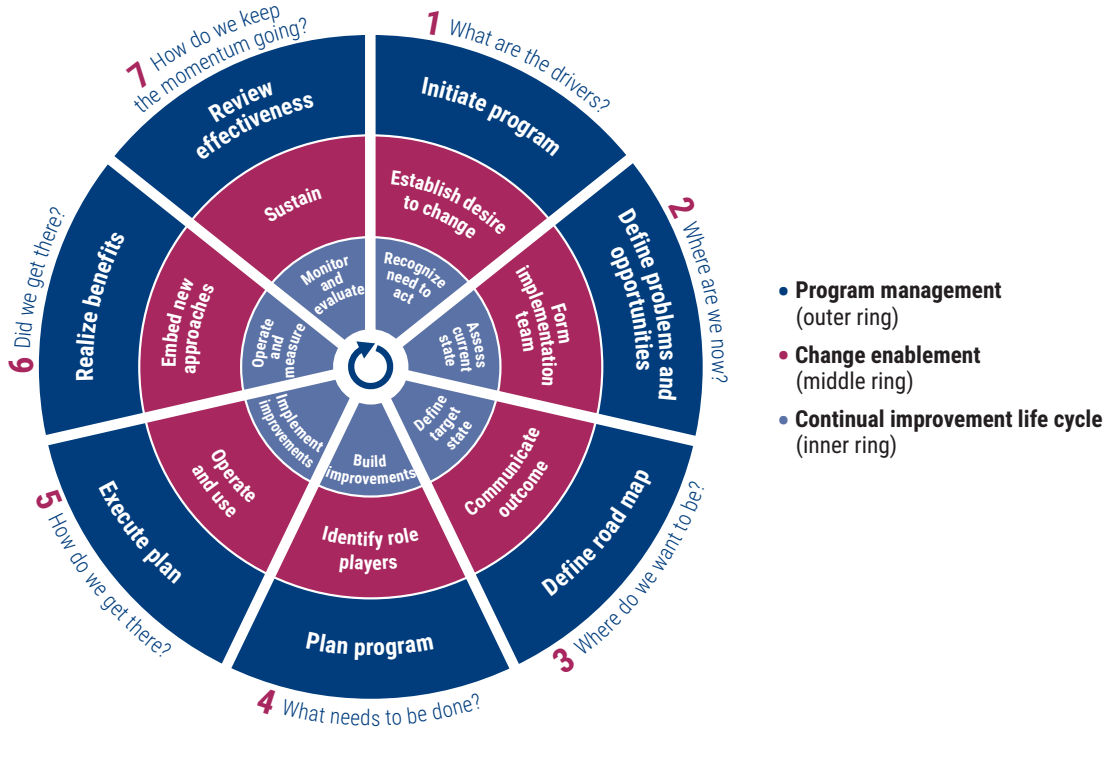
5.1.1 Change Enablement of EGIT Implementation

Various approaches to enabling change have been defined over the years, and they provide valuable input that could be utilized during the implementation life cycle. One of the most widely accepted approaches to change enablement has been developed by John Kotter:[12]

1. Establish a sense of urgency.
2. Form a powerful guiding coalition.
3. Create a clear vision that is expressed simply.
4. Communicate the vision.
5. Empower others to act on the vision.
6. Plan for and create short-term wins.
7. Consolidate improvements and produce more change.
8. Institutionalize new approaches.

The Kotter approach was chosen as an example and adapted for the specific requirements of an EGIT implementation or improvement, as described in this publication. Kotter's adapted precepts are illustrated by the change enablement life cycle in **figure 5.1**.

Figure 5.1—Change Enablement Life Cycle



[12] Kotter, J.; *Leading Change*, Harvard Business School Press, USA, 1996, *https://www.kotterinc.com/book/leading-change/*

The following subsections create a high-level, but holistic, overview by discussing briefly each phase of the change enablement life cycle, as applied to a typical EGIT implementation.

5.2 Phases in the Change Enablement Life Cycle Create the Appropriate Environment

The overall enterprise environment should be analyzed to determine the most appropriate change enablement approach. This includes aspects such as the management style, culture, formal and informal relationships, and attitudes. It is also important to understand other I&T or enterprise initiatives that are ongoing or planned, to ensure that dependencies and impacts are considered.

It should be ensured from the start that the required change enablement skills, competencies and experience are available and utilized. For example, this may entail involving resources from the HR function or obtaining external assistance.

As an outcome of this phase, the appropriate balance of directive and inclusive change enablement activities required to deliver sustainable benefits can be designed.

5.2.1 Phase 1—Establish the Desire to Change

The purpose of this phase is to understand the breadth and depth of the envisioned change, the various stakeholders that are affected, the nature of the impact on, and involvement required from, each stakeholder group, and the current readiness and ability to adopt the change.

Current pain points and trigger events can provide a good foundation for establishing the desire to change. The wake-up call, an initial communication on the program, can be related to real-world issues the enterprise may be experiencing. Also, initial benefits can be linked to areas that are highly visible to the enterprise, creating a platform for further changes and more widespread commitment and buy-in.

While communication is a common thread throughout the implementation or improvement initiative, the initial communication is one of the most important, and should demonstrate the commitment of senior management. Therefore, the initial communication should ideally be communicated by the executive committee or CEO.

5.2.2 Phase 2—Form an Effective Implementation Team

Dimensions to consider in assembling an effective core implementation team include involving the appropriate areas from business and IT and identifying the knowledge and expertise, experience, credibility, and authority of team members. Obtaining an independent, objective view, as provided by external parties (such as consultants and a change agent), could also be highly beneficial by aiding the implementation process or addressing skill gaps that may exist within the enterprise. Therefore, another dimension to consider is the appropriate mix of internal and external resources.

The essence of the team should be a commitment to:

- A clear vision of success and desired goals
- Engaging the best in all team members, all the time
- Clarity and transparency of team processes, accountabilities and communications
- Integrity, mutual support and commitment to each other’s success
- Mutual accountability and collective responsibility

- Ongoing measurement of its own performance and the way it behaves as a team
- Living out of its comfort zone, always looking for ways to improve, uncovering new possibilities and embracing change

It is important to identify potential change agents within different parts of the business, with whom the core team can work, to support the vision and cascade changes down.

5.2.3 Phase 3—Communicate Desired Vision

In this phase, a high-level change enablement plan is developed, in conjunction with the overall program plan. A key component of the change enablement plan is the communication strategy, which addresses who the core audience groups are, and their behavioral profiles and information requirements, communication channels, and principles.

The desired vision for the implementation or improvement program should be communicated in the language of those affected by it. The communication should include the rationale for, and benefits of, the change, the impacts of not making the change (purpose), the vision (picture), the road map to achieving the vision (plan) and the involvement required of the various stakeholders (part).[13] Senior management should deliver key messages (such as the desired vision). The communication should note that both behavioral/cultural and logical aspects will be addressed, and the emphasis is on two-way communication. Reactions, suggestions and other feedback should be captured, and appropriate action taken.

5.2.4 Phase 4—Empower Role Players and Identify Quick Wins

As improvements are designed and built, change response plans are developed to empower various role players. The scope of these may include:

- Organizational design changes, such as job content or team structures
- Operational changes, such as process flows or logistics
- People management changes, such as required training and/or changes to performance management and reward systems

Realization of quick wins is important from a change enablement perspective. These could be related to the pain points and trigger events discussed in Chapter 3. Visible and unambiguous quick wins can build momentum and credibility for the program and help to address any skepticism that may exist.

It is imperative to use a participative approach in the design and building of the improvements. Engaging those affected by the change in the actual design—for example, through workshops and review sessions—can increase buy-in.

5.2.5 Phase 5—Enable Operation and Use

As initiatives are implemented within the core implementation life cycle, the change response plans are also implemented. Quick wins that have been realized are built on, and the behavioral and cultural aspects of the broader transition are addressed (issues such as dealing with fears of loss of responsibility, new expectations and unknown tasks).

It is important to balance group and individual interventions to increase buy-in and engagement and to ensure that all stakeholders obtain a holistic view of the change.

[13] Regarding the four Ps (purpose, picture, plan and part), see Bridges, W.; *Managing Transitions: Making the Most of Change*, Addison-Wesley, USA, 1999.

During the process of solution rollout, mentoring and coaching are critical to ensure uptake in the user environment. The change requirements and objectives that had been set during the start of the initiative should be revisited to ensure that they were adequately addressed.

Success measures should be defined and should include both hard business measures and perception measures that track how people feel about a change.

5.2.6 Phase 6—Embed New Approaches

As concrete results are achieved, new ways of working should become part of the enterprise's culture and be rooted in its norms and values ("the way we do things around here"). One way to accomplish this is by implementing appropriate policies, standards and procedures. The implemented changes should be tracked, the effectiveness of the change response plans should be assessed, and corrective measures taken as appropriate. This might include enforcing compliance where still required.

The communication strategy should be maintained to sustain ongoing awareness.

5.2.7 Phase 7—Sustain

Changes are sustained through conscious reinforcement, an ongoing communication campaign and continued top management commitment.

In this phase, corrective action plans are implemented, lessons learned are captured and knowledge is shared with the broader enterprise.

Page intentionally left blank

Chapter 6
Implementation Life Cycle

6.1 Introduction

Continual improvement of EGIT is accomplished using the seven-phase implementation life cycle outlined in Chapter 3. Each phase is supported by:

- A chart summarizing the responsibilities of each group of role players in the phase. The roles defined are generic. Not every role necessarily must exist as a specific function.
- A table containing:
  - Phase objective
  - Phase description
  - Continual improvement (CI) tasks
  - Change enablement (CE) tasks
  - Program management (PM) tasks
  - Examples of the inputs likely to be required
  - Suggested ISACA and other framework items to be utilized
  - The outputs that need to be produced
- A chart describing who is responsible, accountable, consulted and informed (RACI) for key activities selected from the continual improvement (CI), change enablement (CE) and program management (PM) tasks, with corresponding cross references. Activities covered in the RACI chart are the most important ones: those that produce deliverables or outputs to the next phase, have a milestone attached to them, or are critical to the success of the overall initiative. Not all activities are included, in the interest of keeping this guidance concise.

This guidance is not intended to be prescriptive. Rather, it constitutes a generic phase and task plan that should be adapted to suit a specific implementation.

This chapter refers to a number of steps in the *COBIT® 2019 Design Guide* for CI tasks in phases 1 through 3. The *COBIT® 2019 Design Guide* includes more detailed guidance on the CI tasks described in this chapter. Both guides should be used in conjunction during the initial phases of a governance improvement program.

6.2 Phase 1—What Are the Drivers?

Figure 6.1—Phase 1 *What Are the Drivers?*

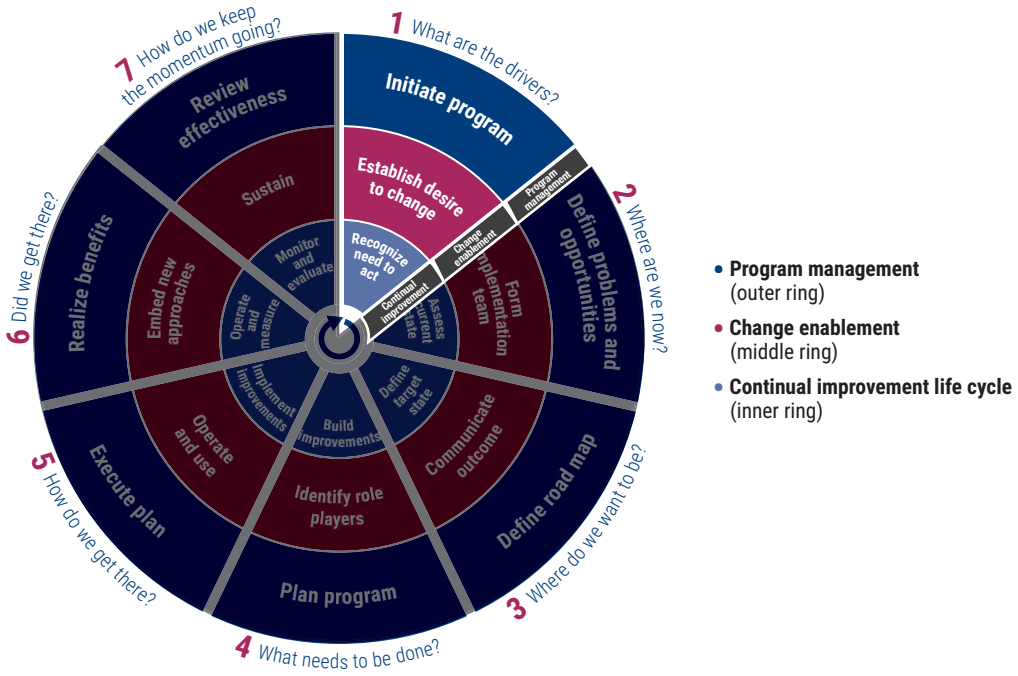


Figure 6.2—Phase 1 Roles

When you are...	Your role in this phase is to...
Board and executive	Provide guidance regarding stakeholder needs (including customer needs), business strategy, priorities, objectives and guiding principles with respect to EGIT. Approve the high-level approach.
Business management	Together with IT, ensure that stakeholder needs and business objectives are stated with sufficient clarity to enable translation into business goals for I&T. Provide input to understanding of risk and priorities.
IT management	Gather requirements and objectives from all stakeholders, gaining consensus on approach and scope. Provide expert advice and guidance regarding IT matters.
Internal audit	Provide advice and challenge proposed activities and actions, ensuring that objective and balanced decisions are made. Provide input on current issues. Provide advice regarding controls and risk management practices and approaches.
Risk, compliance and legal	Provide advice and guidance regarding risk, compliance and legal matters. Ensure that the management-proposed approach is likely to meet risk, compliance and legal requirements.

Figure 6.3—Phase 1 Objectives, Descriptions, Tasks, Inputs, Resources and Outputs	
Description of Phase 1—What Are the Drivers?	
Phase objective	Obtain an understanding of the program background and objectives and current governance approach. Define the initial program concept business case. Obtain the buy-in and commitment of all key stakeholders.
Phase description	This phase articulates the compelling reasons to act within the organizational context. In this context, the program background, objectives and current governance culture are defined. The initial program concept business case is defined. The buy-in and commitment of all key stakeholders is obtained.
Continual improvement (CI) tasks	A number of the CI tasks are equivalent to the activities defined in the *COBIT® 2019 Design Guide*. This guide should be consulted for more detailed guidance on the first three tasks, and in particular, the design guide's Steps 1.1 *Understand enterprise strategy*, 1.2 *Understand enterprise goals*, 1.3 *Understand the risk profile* and 1.4 *Understand current I&T-related issues*. Recognize the need to act: **1.** Identify current governance context, business and IT pain points, events, and symptoms triggering the need to act. **2.** Identify the business and governance drivers and compliance requirements for improving EGIT and assess current stakeholder needs. **3.** Identify business priorities and business strategy dependent on IT, including any current significant projects. **4.** Align with enterprise policies, strategies, guiding principles and any ongoing governance initiatives. **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.
Change enablement (CE) tasks	Establish the desire to change: **1.** Ensure integration with enterprise-level change enablement approaches or programs, if any exist. **2.** Analyze the general organizational environment in which the change needs to be enabled. This includes organization structure, management style(s), culture, ways of working, formal and informal relationships, and attitudes. **3.** Determine other ongoing or planned enterprise initiatives to determine change dependencies or impacts. **4.** Understand the breadth and depth of the change. **5.** Identify stakeholders involved in the initiative from different areas of the enterprise (e.g., business, IT, audit, risk management) as well as different levels (e.g., executives, middle management) and consider their needs. **6.** Determine the level of support and involvement required from each stakeholder group or individual, their influence, and the impact of the change initiative on them. **7.** Determine the readiness and ability to implement the change for each stakeholder group or individual. **8.** Establish a wake-up call, using the pain points and trigger events as a starting point. Use the I&T governance board (or an equivalent governance structure) to communicate the message to create awareness of the program, its drivers and its objectives among all stakeholders. **9.** Eliminate any false signs of security or complacency by, for example, highlighting compliance or exception figures. **10.** Instill the appropriate level of urgency, depending on the priority and impact of the change.
Program management (PM) tasks	Initiate the program: **1.** Provide high-level strategic direction and set high-level program objectives in agreement with the I&T governance board or equivalent (if one exists). **2.** Define and assign high-level roles and responsibilities within the program, starting with the executive sponsor and including the program manager and all the important stakeholders. **3.** Develop an outline business case indicating the success factors to be used to enable performance monitoring and reporting of the success of the governance improvement. **4.** Obtain executive sponsorship.

Figure 6.3—Phase 1 Objectives, Descriptions, Tasks, Inputs, Resources and Outputs *(cont.)*	
Description of Phase 1—What Are the Drivers?	
Input	• Enterprise policies, strategies, governance and business plans, and audit reports • Other major enterprise initiatives on which there may be dependencies or impacts • I&T governance board performance reports help desk statistics, IT customer surveys or other inputs that indicate current IT pain points • Any useful and relevant industry overviews, case studies and success stories (see *www.isaca.org/cobitcasestudies*) • Specific customer requirements, marketing and servicing strategy, market position, enterprise vision and mission statements
ISACA materials and other frameworks	• *COBIT® 2019 Design Guide* (design factors) • *COBIT® 2019 Framework: Governance and Management Objectives* (particularly EDM01, APO01, MEA01) and *COBIT® 2019 Framework: Introduction and Methodology*, Chapter 9, Getting Started With COBIT: Making the Case, *www.isaca.org/cobit* • The example decision matrix in the appendix of this publication • ISACA supporting products currently listed at *www.isaca.org*
Output	• Business case outline • High-level roles and responsibilities • Identified stakeholder map, including support and involvement required, influence and impact, and agreed understanding of the efforts required to manage human change • Program wake-up call (all stakeholders) • Program kick-off communication (key stakeholders)

Figure 6.4—Phase 1 RACI Chart

Key Activities	Responsibilities of Implementation Role Players: Board	I&T Governance Board	CIO	Business Executive	IT Managers	IT Process Owners	IT Audit	Risk and Compliance	Program Steering
Identify issues triggering need to act (CI1).	C/I	A	R	R	C	C	C	C	R
Identify business priorities and strategies affecting IT (CI3).	C	A	R	R	C	C	C	C	R
Gain management agreement to act and obtain executive sponsorship (CI7).	C	A/R	R	C	I	I	I	I	R
Instill the appropriate level of urgency to change (CE10).	I	A	R	R	C	C	C	C	R
Produce convincing outline business case (PM3).	I	A	R	C	C	C	C	C	R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or Informed.

6.3 Phase 2—Where Are We Now?

Figure 6.5—Phase 2 *Where Are We Now?*

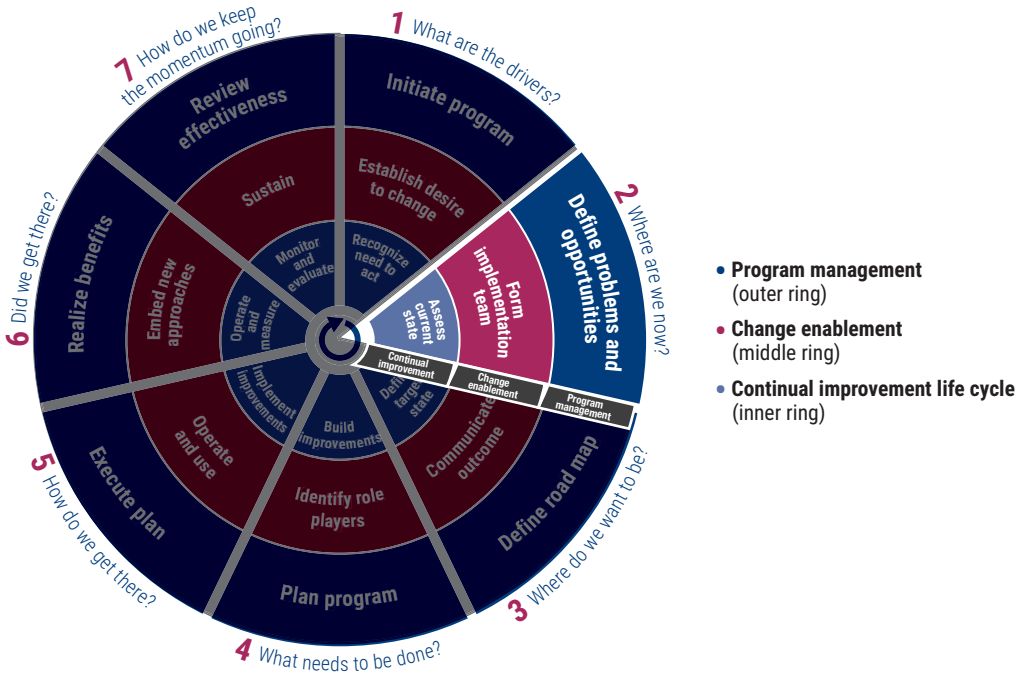


Figure 6.6—Phase 2 Roles	
When you are...	**Your role in this phase is to...**
Board and executive	Verify and interpret the results/conclusions of assessments.
Business management	Assist IT in determining the reasonableness of current assessments by providing the customer view.
IT management	Ensure open and fair assessment of IT activities. Guide assessment of current practice. Obtain consensus.
Internal audit	Provide advice, input and assistance to current-state assessments. If required, independently verify assessment results.
Risk, compliance and legal	Review assessments to ensure that risk, compliance and legal issues have been considered adequately.

Figure 6.7—Phase 2 Objectives, Descriptions, Tasks, Inputs, Resources and Outputs	
Description of Phase 2—Where Are We Now?	
Phase objective	Ensure that the program team knows and understands the enterprise goals and how the business and IT function need to deliver value from I&T in support of the enterprise goals, including any current significant projects. Identify the critical processes or other enablers that will be addressed in the improvement plan. Identify the appropriate management practices for each selected process. Obtain an understanding of the enterprise's present and future attitude toward risk and the IT-risk position, and determine how it will impact the program. Determine the current capability of the selected processes. Understand the enterprise's capacity and capability for change.

Figure 6.7—Phase 2 Objectives, Descriptions, Tasks, Inputs, Resources and Outputs *(cont.)*	
Description of Phase 2—Where Are We Now?	
Phase description	This phase identifies the enterprise and alignment goals and illustrates how I&T contributes to enterprise goals via solutions and services. The focus is on identifying and analyzing how I&T creates value for the enterprise by enabling business transformation in an agile way, making the current business processes more efficient, making the enterprise more effective, and meeting governance-related requirements such as managing risk, ensuring security, and complying with legal and regulatory requirements. Based on the enterprise risk profile, its risk history and appetite, and actual benefit/value enablement risk, definitions are created for benefit/value enablement risk, program/project delivery and service delivery/IT operations risk to the enterprise and alignment goals. The *COBIT® 2019 Design Guide* contains a table mapping generic risk scenarios to COBIT governance and management objectives that can be used to support this analysis. The understanding of business and governance drivers and a risk assessment are used to focus on the governance and management objectives critical to ensuring that alignment goals are met. Then, the performance level of the different governance components that support each governance and management objective are established, based on process descriptions, policies, standards, procedures and technical specifications, to determine whether they are likely to support the business and I&T requirements. The presence of specific IT-related issues in an enterprise could also contribute to the selection of governance and management objectives on which to focus. The *COBIT® 2019 Design Guide* contains an example mapping of common IT-related issues (as discussed in Chapter 3) to COBIT governance and management objectives.
Continual improvement (CI) tasks	Assess current state: Understand how I&T needs to support the current enterprise goals. (A detailed discussion on enterprise strategies and the COBIT goals cascade is included in the *COBIT® 2019 Design Gui*de.) A number of the CI tasks are equivalent to the activities defined in the *COBIT® 2019 Design Guide*. This guide should be consulted for more detailed guidance on most of the CI tasks described below. **Identify key enterprise and supporting alignment goals**—For more detailed guidance, see the *COBIT® 2019 Design Guide*, Section 4, Steps 2.1 *Consider enterprise strategy* and 2.2 *Consider enterprise goals and apply the COBIT goals cascade*. **1. Establish the significance and nature of I&T's contribution (solutions and services) required to support business objectives**—For more detailed guidance, see the *COBIT® 2019 Design Guide*, Section 4, Steps 2.2 *Consider enterprise goals and apply the COBIT goals cascade*, Step 3.1 *Consider enterprise size*, Step 3.4 *Consider the role of IT*, Step 3.5 *Consider the sourcing model*, Step 3.6 *Consider IT implementation methods*, and Step 3.7 *Consider the IT adoption strategy*. **2. 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**—For more detailed guidance, see the *COBIT® 2019 Design Guide*, Section 4, Step 2.4 *Consider current I&T-related issues*. **3. Identify and select the governance and management objectives critical to support IT-related goals and, if appropriate, key management practices for each selected process**—For more detailed guidance, see the *COBIT® 2019 Design Guide*, Section 4, Steps 2.1 *Consider enterprise strategy* and 2.2 *Consider enterprise goals and apply the COBIT goals cascade*. **4. Assess benefit/value enablement risk, program/project delivery and service delivery/IT operations risk related to critical governance and management objectives**—For more detailed guidance, see the *COBIT® 2019 Design Guide*, Section 4, Step 2.3 *Consider the risk profile of the enterprise*. **5. Identify and select governance and management objectives critical to ensure that risk is avoided**—For more detailed guidance, see the *COBIT® 2019 Design Guide*, Section 4, Step 2.3 *Consider the risk profile of the enterprise*. **6. Understand the risk acceptance position as defined by management**—For more detailed guidance, see the *COBIT® 2019 Design Guide*, Section 4, Steps 1.3 *Understand the risk profile* and 2.3 *Consider the risk profile of the enterprise*.

Figure 6.7—Phase 2 Objectives, Descriptions, Tasks, Inputs, Resources and Outputs *(cont.)*	
Description of Phase 2—Where Are We Now?	
	Assess actual performance (refer to *COBIT® 2019 Framework: Introduction and Methodology*, Chapter 6, Performance Management in COBIT): **1.** Define the method for executing the assessment. See *COBIT® 2019 Framework: Introduction and Methodology*, Chapter 6, Performance Management in COBIT. **2.** Document understanding of how the current governance components actually addresses the management practices selected earlier. See the *COBIT® 2019 Design Guide*, all of Steps 2 and 3. **3.** Analyze the current level of capability. See the *COBIT® 2019 Design*, Section 4, Step 4, and *COBIT® 2019 Framework: Introduction and Methodology*, Chapter 6, Performance Management in COBIT. **4.** Define the current process capability rating and the performance levels of other components. See the *COBIT® 2019 Design Guide*, Section 4, Step 4, and *COBIT® 2019 Framework: Introduction and Methodology*, Chapter 6, Performance Management in COBIT.
Change enablement (CE) tasks	Form a powerful implementation team: **1.** Assemble a core team from the business and IT with the appropriate knowledge, expertise, profile, experience, credibility and authority to drive the initiative. Identify the most desirable person (effective leader and credible to the stakeholders) to lead this team. Consider the use of external parties, such as consultants, as part of the team to provide an independent and objective view or to address any skill gaps that may exist. **2.** Identify and manage any potential vested interests that may exist within the team to create the required level of trust. **3.** Create the appropriate environment for optimal teamwork. This includes ensuring that the necessary time and involvement can be given. **4.** Hold a workshop to create consensus (shared vision) within the team and adopt a mandate for the change initiative. **5.** Identify change agents with whom the core team can work, using the principle of cascading sponsorship (having sponsors at various hierarchical levels supporting the vision, spreading the word on quick wins, cascading changes down, and working with any blockers and cynics that may exist). This will help to ensure widespread stakeholder buy-in during each phase of the life cycle. **6.** Document strengths identified during the current-state assessment that can be used for positive elements in communications as well as potential quick wins that can be leveraged from a change enablement perspective.
Program management (PM) tasks	Define problems and opportunities: **1.** Review and evaluate the outline business case, program feasibility and potential return on investment (ROI). **2.** Assign roles, responsibilities and process ownership. Ensure commitment and support of affected stakeholders in the definition and execution of the program. **3.** Identify challenges and success factors.
Input	• Outline business case • High-level roles and responsibilities • Identified stakeholder map, including support and involvement required, influence and impact, and readiness and ability to implement or buy into the change • Program wake-up call (all stakeholders) • Program kick-off communication (key stakeholders) • Business and IT plans and strategies • IT process descriptions, policies, standards, procedures, technical specifications • Understanding of business and IT contribution • Audit reports, risk management policy, IT performance reports/dashboards/scorecards • Business continuity plans (BCPs), impact analyses, regulatory requirements, enterprise architectures, service level agreements (SLAs), operational level agreements (OLAs) • Investment program and project portfolios, program and project plans, project management methodologies, project reports

Figure 6.7—Phase 2 Objectives, Descriptions, Tasks, Inputs, Resources and Outputs *(cont.)*	
Description of Phase 2—Where Are We Now?	
Output	• Agreed alignment goals and impact on I&T • Agreed understanding of the risk and impacts resulting from misaligned alignment goals and service and project delivery failures • Selected governance and management objectives • Current performance levels of selected governance and management objectives, including process capability levels • Risk acceptance position and risk profile • Benefit/value enablement risk, program/project delivery and service delivery/IT operations risk assessments • Strengths on which to build • Change agents in different parts and at different levels in the enterprise • Core team and assigned roles and responsibilities • Evaluated outline business case • Agreed understanding of the issues and challenges (including process capability levels)
ISACA resources	• *COBIT® 2019 Framework: Introduction and Methodology* (governance and management objectives, goals cascade, enterprise goals-alignment goals cascade), *www.isaca.org/cobit* • *COBIT® 2019 Framework: Governance and Management Objectives* (APO01, APO02, APO05, APO12, BAI01, BAI11, MEA01, MEA02, MEA03, MEA04, used for process selection and process capability assessment, as well as implementation and program planning) • Chapter 5, Enabling Change, in this publication • ISACA supporting products as currently listed at *www.isaca.org*

Figure 6.8—Phase 2 RACI Chart

Key Activities	Board	I&T Governance Board	CIO	Business Executive	IT Managers	IT Process Owners	IT Audit	Risk and Compliance	Program Steering
	Responsibilities of Implementation Role Players								
Identify key IT goals supporting business goals (CI1).	I	C	R	C	R	C	C	C	A
Identify processes critical to support IT and business goals (CI4).		I	R	C	R	C	C	C	A
Assess risk related to achievement of goals (CI5).		I	R	C	R	R	C	R	A
Identify processes critical to ensure that key risk is avoided (CI6).		I	R	R	R	C	C	R	A
Assess current performance of critical processes (CI1 to CI11).		I	R	C	R	R	C	C	A
Assemble a core team from the business and IT (CE1).		I	R	R	C	C	C	C	A
Review and evaluate the business case (PM1).	I	A	R	R	C	C	C	C	R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or Informed.

6.4 Phase 3—Where Do We Want to Be?

Figure 6.9—Phase 3 *Where Do We Want to Be?*

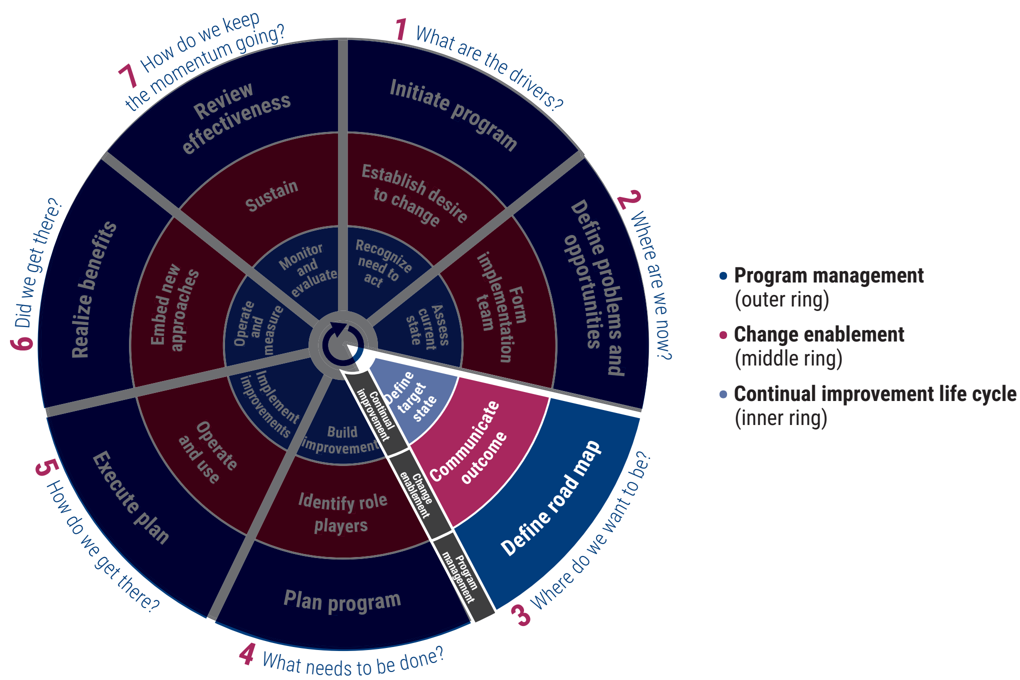


Figure 6.10—Phase 3 Roles	
When you are...	**Your role in this phase is to...**
Board and executive	Set priorities, time scales and expectations regarding the future capability required from I&T.
Business management	Assist IT with the setting of capability targets. Ensure that the envisaged solutions are aligned to enterprise goals.
IT management	Apply professional judgment in formulating improvement priority plans and initiatives. Obtain consensus on a required capability target. Ensure that the envisaged solution is aligned to alignment goals.
Internal audit	Provide advice and assist with target-state positioning and gap priorities. If required, independently verify assessment results.
Risk, compliance and legal	Review plans to ensure that risk, compliance and legal issues have been addressed adequately.

Figure 6.11—Phase 3 Objectives, Descriptions, Tasks, Inputs, Resources and Outputs	
Description of Phase 3—Where Do We Want to Be?	
Phase objective	Determine the targeted capability for the processes within each of the selected governance and management objectives. Determine gaps between the as-is and the to-be positions of the selected processes and translate these gaps into improvement opportunities. Use this information to create a detailed business case and high-level program plan.
Phase description	Based on the assessed current-state process capability levels, and using the results of the enterprise goals-to-alignment goals analysis and identification of process importance performed earlier, an appropriate target capability level should be determined for each process. The chosen level should consider available external and internal benchmarks. It is important to ensure the appropriateness to the business of the level chosen. After the current capability of the process has been determined and the target capability planned, the gaps between the current state and the desired future state should be evaluated and opportunities for improvement identified. After the gaps have been defined, the root causes, common issues, residual risk, existing strengths and good practices to close those gaps need to be determined. This phase may identify some relatively easy-to-achieve improvements such as improved training, sharing good practices and standardizing procedures. However, the gap analysis is likely to require considerable experience in business and IT-management techniques to develop practical solutions. Experience in undertaking behavioral and organizational change will also be needed. Understanding of process techniques, advanced business and technical expertise, and knowledge of business and system management software applications and services may be needed. To ensure that this phase is executed effectively, it is important for the team to work with the business and IT process owners and other required stakeholders, engaging internal expertise. If necessary, external advice should also be obtained. Risk that will not be mitigated after closing the gaps should be identified and formally accepted by management.
Continual improvement (CI) tasks	CI tasks 1 and 2, described as follows, can build on the results of the governance system design approach as described in the *COBIT® 2019 Design Guide*. This is especially true of governance system design workflow Step 4 (which consists of Steps 4.1 *Resolve Inherent priority conflicts* and 4.2 *Conclude the governance system design*). This step outlines taking an informed and substantiated decision on target capability and performance levels for the components of the governance system, which is equivalent to the following CI tasks. 1. Define target for improvement: ● Based on enterprise requirements for performance and conformance, decide initial, ideal short- and long-term target capability levels for each process. ● Benchmark internally (to the extent possible) to identify better practices that can be adopted. ● Benchmark externally (to the extent possible) with competitors and peers, to help decide appropriateness of the chosen target level. ● Do a sanity check on the reasonableness of the targeted levels (individually and as a whole), looking at what is achievable and desirable, and what can have the greatest positive impact within the chosen time frame. 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. Seek guidance from COBIT management practices and activities and other specific good practices and standards, such as ITIL®, ISO/IEC 27000, The Open Group Architectural Framework (TOGAF®) and Project Management Body of Knowledge (PMBOK®) to close other gaps. ● Look for patterns that indicate root causes to be addressed. 3. Identify potential improvements: ● Collate gaps into potential improvements. ● Identify unmitigated residual risk and ensure its formal acceptance.

Figure 6.11—Phase 3 Objectives, Descriptions, Tasks, Inputs, Resources and Outputs *(cont.)*	
Description of Phase 3—Where Do We Want to Be?	
Change enablement (CE) tasks	Describe and communicate desired outcomes: **1.** Describe the high-level change enablement plan and objectives, which will include the following tasks and components. **2.** Develop a communication strategy to optimize awareness and buy-in. The strategy should include core audience groups, a behavioral profile and information requirements for each group, core messages, optimal communication channels, and communication principles. **3.** Secure willingness to participate (picture of the change). **4.** Articulate the rationale for, and benefits of, the change to support the vision. Describe the impact(s) of not making the change (purpose of the change). **5.** Link back to objectives for the initiative in the communications and demonstrate how the change will realize the benefit. **6.** Describe the high-level road map to achieve the vision (plan for the change) as well as the involvement required of various stakeholders (role within the change). **7.** Set the tone at the top by using senior management to deliver key messages. **8.** Use change agents to communicate informally, in addition to formal communications. **9.** Communicate through action. The guiding team should set an example. **10.** Appeal to people's emotions to encourage them to change behaviors, when required. **11.** Capture initial communication feedback (reactions and suggestions) and adapt the communication strategy accordingly.
Program management (PM) tasks	Define the road map: **1.** Set program direction, scope, benefits and objectives at a high level. **2.** Ensure alignment of the objectives with business and IT strategies. **3.** Consider risk and adjust the scope accordingly. **4.** Consider change enablement implications. **5.** Obtain necessary budgets and define program accountabilities and responsibilities. **6.** Create and evaluate a detailed business case, budget, time lines and high-level program plan.
Input	• Agreed enterprise goals and impact on alignment goals • Current capability rating for selected processes • Definition of alignment goals • Selected processes and goals • Risk acceptance position and risk profile • Assessed benefit/value enablement risk, program/project delivery and service delivery/IT operations risk assessment • Strengths on which to build • Change agents in different parts and at different levels in the enterprise • Core team and assigned roles and responsibilities • Evaluated outline business case • Challenges and success factors • Internal and external capability benchmarks • Good practices from COBIT and other references • Stakeholder analysis
Output	• Target capability rating for selected processes • Description of improvement opportunities • Risk response document, including risk not mitigated • Change enablement plan and objectives • Communication strategy and communication of the change vision covering the four Ps (picture, purpose, plan, part) • Detailed business case • High-level program plan • Key metrics that will be used to track program and operational performance
ISACA resources	• *COBIT® 2019 Framework: Introduction and Methodology* (enterprise goals), *www.isaca.org/cobit* • *COBIT® 2019 Framework: Governance and Management Objectives* (management practices and activities for the target-state definition and gap analysis, APO01, APO02) • ISACA supporting products, as currently listed at *www.isaca.org*

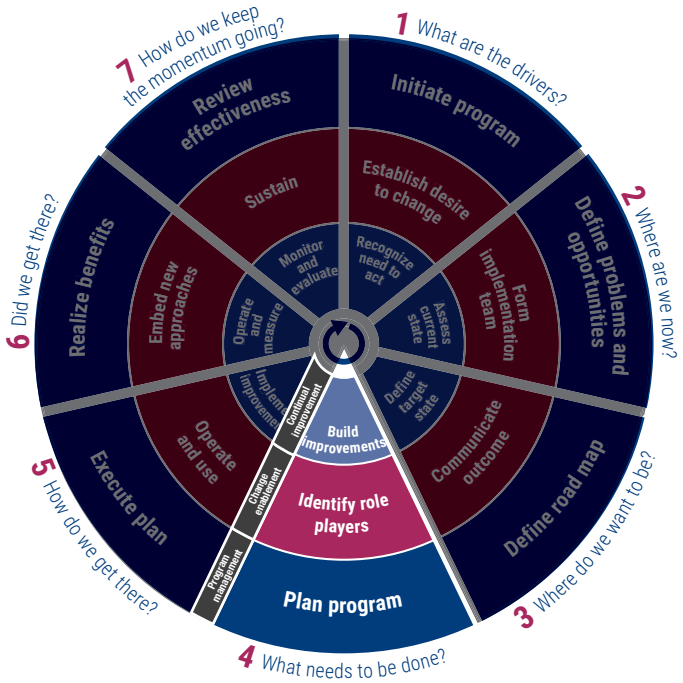
Figure 6.12—Phase 3 RACI Chart

Key Activities	Board	I&T Governance Board	CIO	Business Executive	IT Managers	IT Process Owners	IT Audit	Risk and Compliance	Program Steering
	Responsibilities of Implementation Role Players								
Agree on target for improvement (CI1).	I	A	R	C	R	R	C	C	R
Analyze gaps (CI2).		I	R	C	R	R	C	C	A
Identify potential improvements (CI3).		I	R	C	R	R	C	C	A
Communicate change vision (CE3).		A	R	R	C	I	I	I	R
Set program direction and prepare detailed business case (PM1, PM6).	I	A	R	C	C	C	I	I	R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or Informed.

6.5 Phase 4—What Needs to Be Done?

Figure 6.13—Phase 4 *What Needs to Be Done?*



- **Program management** (outer ring)
- **Change enablement** (middle ring)
- **Continual improvement life cycle** (inner ring)

Figure 6.14—Phase 4 Roles	
When you are...	**Your role in this phase is to...**
Board and executive	Consider and challenge proposals, support justified actions, provide budgets, and set priorities as appropriate.
Business management	Together with IT, ensure that the proposed improvement actions are aligned with agreed enterprise and IT-related goals and that any activities requiring business input or action are supported. Ensure that required business resources are allocated and available. Agree with IT on the metrics for measuring the outcomes of the improvement program.
IT management	Ensure viability and reasonableness of the program plan. Ensure that the plan is achievable, and resources are available to execute the plan. Consider the plan together with priorities of the enterprise's portfolio of I&T-enabled investments to decide a basis for investment funding.
Internal audit	Provide independent assurance that issues identified are valid, business cases are objectively and accurately presented, and plans appear achievable. Provide expert advice and guidance where appropriate.
Risk, compliance and legal	Ensure that any identified risk, compliance and legal issues are being addressed, and that proposals conform with any relevant policies or regulations.

Figure 6.15—Phase 4 Objectives, Descriptions, Tasks, Inputs, Resources and Outputs	
Description of Phase 4—What Needs to Be Done?	
Phase objective	Translate improvement opportunities into justifiable contributing projects. Prioritize and focus on high-impact projects. Integrate the improvement projects into the overall program plan. Execute quick wins.
Phase description	When all the potential initiatives for improvement have been identified, they should be prioritized into formal and justifiable projects. The projects that are of high benefit and relatively easy to implement should be selected first, and translated into formal and justifiable projects. Each should have a project plan that includes the project's contribution to program objectives. It is important to check whether the objectives still conform to the original value and risk drivers. The projects will be included in an updated business case for the program. Details of any unapproved project proposals should be recorded in a register for potential future consideration. Sponsors may reappraise, and, when appropriate, resubmit new recommendations at a later date. Based on an opportunity grid, the project definitions, the resource plan and the I&T budget, the identified and prioritized improvements are now turned into a set of documented projects that support the overall improvement program. The impact on the enterprise of executing the program is determined and a change plan is prepared that describes the program activities that will ensure, in practical terms, that the improvements delivered by the projects will be rolled into the enterprise in a sustainable manner. An important element in this phase is the definition of metrics—that is, the program's success metrics—that will measure whether the process improvements are likely to deliver the original business benefits. The complete improvement program schedule should be documented on a Gantt chart. New projects may identify a need to change or improve the organizational structures or other enablers required to sustain effective governance. If required, it may be necessary to include actions to improve the environment (as described in Chapter 5).

Figure 6.15—Phase 4 Objectives, Descriptions, Tasks, Inputs, Resources and Outputs *(cont.)*	
Description of Phase 4—What Needs to Be Done?	
Continual improvement (CI) tasks	Design and build improvements: **1.** Consider potential benefit and ease of implementation (cost, effort and sustainability) for each improvement. **2.** Plot improvements onto an opportunity grid to identify priority actions (based on benefit and ease of implementation). **3.** Focus on alternatives showing high benefit/high ease of implementation. **4.** Consider alternatives showing high benefit/low ease of implementation for possible scaled-down improvements. Decompose them into smaller improvements and look again at benefits and ease of implementation. **5.** Prioritize and select improvements. **6.** Analyze selected improvements to the detail required for high-level project definition. Consider approach, deliverables, resources required, estimated costs, estimated time scales, dependencies and project risk. Use available good practices and standards to further refine detailed improvement requirements. Discuss with managers and teams responsible for the process area. **7.** Consider feasibility, link back to the original value and risk drivers, and agree on projects to be included in the business case for approval. **8.** Record unapproved projects and initiatives in a register for potential future consideration.
Change enablement (CE) tasks	Empower role players and identify quick wins: **1.** Obtain buy-in by engaging affected users through mechanisms such as workshops or review processes. Give them responsibility to accept the quality of results. **2.** Design change response plans to proactively manage change impacts and maximize engagement throughout the implementation process. This could include organizational changes, such as job content or organizational structure; people management changes, such as training; performance management systems; or incentives/remuneration and reward systems. **3.** Identify quick wins that prove the concept of the improvement program. These should be visible and unambiguous, build momentum, and provide positive reinforcement of the process. **4.** Build on any existing strengths identified in phase 2 to realize quick wins, where possible. **5.** Identify strengths in existing enterprise processes that could be leveraged. For example, strengths in project management may exist in other areas of the business, such as product development. Avoid reinventing the wheel and align wherever possible to current enterprisewide approaches.
Program management (PM) tasks	Develop the program plan: **1.** Organize potential projects into the overall program, in preferred sequence, considering contribution to desired outcomes, resource requirements and dependencies. **2.** Use portfolio management techniques to ensure that the program conforms to strategic goals and that I&T has a balanced set of initiatives. **3.** Identify the impact of the improvement program on the IT and business organizations and indicate how the improvement momentum is to be maintained. **4.** Develop a change plan documenting any migration, conversion, testing, training, process or other activities that must be included within the program as part of implementation. **5.** Identify and agree on metrics for measuring the outcomes of the improvement program in terms of the original program success factors. **6.** Guide the allocation and prioritization of business, IT and audit resources necessary to achieve program and project objectives. **7.** Define a portfolio of projects that will deliver required outcomes for the program. **8.** Define required deliverables, considering the full scope of activities needed to meet objectives. **9.** Nominate project steering committees for specific projects within the program, if required. **10.** Establish project plans and reporting procedures to enable progress to be monitored.

Figure 6.15—Phase 4 Objectives, Descriptions, Tasks, Inputs, Resources and Outputs *(cont.)*

Description of Phase 4—What Needs to Be Done?	
Input	• Target maturity rating for selected processes • Description of improvement opportunities • Risk response document • Change enablement plan and objectives • Communication strategy and communication of the change vision covering four Ps (picture, purpose, plan, part) • Detailed business case • Opportunity worksheet, good practices and standards, external assessments, technical evaluations • Opportunity grid, project definitions, project portfolio management plan, resource plan, I&T budget • Strengths identified in earlier phases
Output	• Improvement project definitions • Defined change response plans • Identified quick wins • Record of unapproved projects • Program plan that sequences individual plans with allocated resources, priorities and deliverables • Project plans and reporting procedures enabled through committed resources such as skills and investment • Success metrics
ISACA resources	• *COBIT® 2019 Framework: Introduction and Methodology* (governance and management objectives, components of the governance system), *www.isaca.org/cobit* • *COBIT® 2019 Framework: Governance and Management Objectives* (APO5, APO12, BAI01, BAI11, goals and metrics) • ISACA supporting products as currently listed at *www.isaca.org*

Figure 6.16—Phase 4 RACI Chart

Key Activities	Responsibilities of Implementation Role Players: Board	I&T Governance Board	CIO	Business Executive	IT Managers	IT Process Owners	IT Audit	Risk and Compliance	Program Steering
Prioritize and select improvements (CI5).		A	R	C	C	R	C	C	R
Define and justify projects (CI6 and CI7).		I	R	C	R	R	C	C	A
Design change response plans (CE2).		I	R	R	C	C	C	C	A
Identify quick wins and build on existing strengths (CE3).		I	C	C/I	R	R	C/I	C/I	A
Develop program plan with allocated resources and project plans (PM1 to PM10).		A	C	C	R	C	I	I	R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or Informed.

6.6 Phase 5—How Do We Get There?

Figure 6.17—Phase 5 *How Do We Get There?*

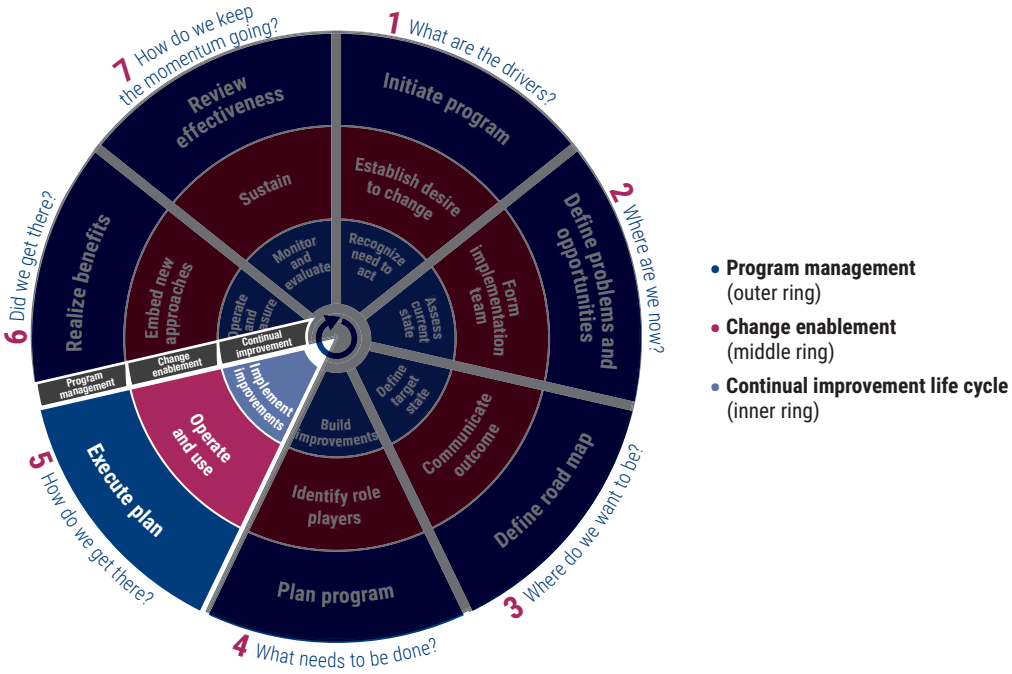


Figure 6.18—Phase 5 Roles	
When you are...	**Your role in this phase is to...**
Board and executive	Monitor implementation and provide support and direction as required.
Business management	Take ownership for business participation in the implementation, especially where business processes are affected, and IT processes require user/customer involvement.
IT management	Make sure that the implementation includes the full scope of activities required (e.g., policy and process changes, technology solutions, organizational changes, new roles and responsibilities, other enablers); ensure that implementations are practical, achievable, and likely to be adopted and used. Make sure that process owners are involved, buy into the new approach and own the resulting processes. Resolve issues and manage risk as encountered during the implementation.
Internal audit	Review and provide input during implementation to avoid after-the-fact identification of missing enablers and especially key controls. Provide guidance on implementation of control aspects. If required, provide a project/implementation risk review service, monitoring risk that could jeopardize implementation and providing independent feedback to the program and project teams.
Risk, compliance and legal	Provide guidance as required on risk, compliance and legal aspects during implementation.

Figure 6.19—Phase 5 Objectives, Descriptions, Tasks, Inputs, Resources and Outputs	
Description of Phase 5—How Do We Get There?	
Phase objective	Implement the detailed improvement projects, leveraging enterprise program and project management capabilities, standards and practices. Monitor, measure and report on project progress.
Phase description	The approved improvement projects, including required change activities, are now ready for implementation, so the solutions defined by the program can now be acquired or developed and implemented into the enterprise. In this way, projects become part of the normal development life cycle and should be governed by established program and project management methods. The rollout of the solution should align with the established project definitions and change plan to support the improvements' sustainability. This phase typically involves the most effort and longest elapsed time of all the life cycle phases. However, it is important to ensure that the phase is manageable and benefits are delivered in a reasonable time frame, so excessive size and overall time taken should be avoided. This is especially true for the first few iterations, which will also be a learning experience for all involved. Performance of each project must be monitored to ensure that goals are being achieved. Reporting back to stakeholders at regular intervals ensures that progress is understood and on track.
Continual improvement (CI) tasks	Implement improvements: **1.** Develop and, where necessary, acquire solutions that include the full scope of activities required. These may include culture, ethics and behavior; organizational structures; principles and policies; processes; service capabilities; skills and competencies; and information. **2.** When using good practices, adopt and adapt available guidance to suit the enterprise's approach to policies and procedures. **3.** Test the practicality and suitability of the solutions in the real working environment. **4.** Roll out the solutions, considering any existing processes and migration requirements.
Change enablement (CE) tasks	Enable operation and use: **1.** Build on the momentum and credibility that can be created by quick wins, then introduce more widespread and challenging change aspects. **2.** Communicate quick-win successes and recognize and reward those involved in them. **3.** Implement the change response plans. **4.** Ensure that the broader base of role players has the skills, resources and knowledge, as well as buy-in and commitment to the change. **5.** Balance group and individual interventions to ensure that key stakeholders obtain a holistic view of the change. **6.** Plan cultural and behavioral aspects of the broader transition (dealing with fears of loss of responsibility/independence/decision authority, new expectations and unknown tasks). **7.** Communicate roles and responsibilities for use. **8.** Define measures of success, including those from a business viewpoint and perception measures. **9.** Set in place mentoring and coaching to ensure uptake and buy-in. **10.** Close the loop and ensure that all change requirements have been addressed. **11.** Monitor the change enablement effectiveness and take corrective action where necessary.
Program management (PM) tasks	Execute the plan: **1.** Ensure that the execution of the program is based on an up-to-date and integrated (business and IT) plan of the projects within the program. **2.** Direct and monitor the contribution of all the projects in the program to ensure delivery of the expected outcomes. **3.** Provide regular update reports to stakeholders to ensure that progress is understood and on track. **4.** Document and monitor significant program risk and issues and agree on remediation actions. **5.** Approve the initiation of each major program phase and communicate it to all stakeholders. **6.** Approve any major changes to the program and project plans.

Figure 6.19—Phase 5 Objectives, Descriptions, Tasks, Inputs, Resources and Outputs *(cont.)*	
Description of Phase 5—How Do We Get There?	
Input	• Improvement project definitions • Defined change response plans • Identified quick wins • Record of unapproved projects • Program plan with allocated resources, priorities and deliverables • Project plans and reporting procedures • Success metrics • Project definitions, project Gantt chart, change response plans, change strategy • Integrated program and project plans
Output	• Implemented improvements • Implemented change response plans • Realized quick wins and visibility of change success • Success communications • Defined and communicated roles and responsibilities in the business-as-usual environment • Project change logs and issue/risk logs • Defined business and perception success measures • Benefits tracked to monitor realization
ISACA resources	• *COBIT® 2019 Framework: Governance and Management Objectives* (all objectives as good practice input, BAI01, BAI11), *www.isaca.org/cobit* • ISACA supporting products as currently listed at *www.isaca.org*

Figure 6.20—Phase 5 RACI Chart

Key Activities	Responsibilities of Implementation Role Players: Board	I&T Governance Board	CIO	Business Executive	IT Managers	IT Process Owners	IT Audit	Risk and Compliance	Program Steering
Develop and, if required, acquire solutions (CI1).		A	C	C	R	R	C	C	R
Adopt and adapt good practices (CI2).		I	R	C	R	R	C	C	A
Test and roll out solutions (CI3 and CI4).		I	R	C	R	R	C	C	A
Capitalize on quick wins (CE1 and CE2).		I	C	C/I	R	R	C/I	C/I	A
Implement change response plans (CE3).	I	I	R	C	R	R	I	I	A
Direct and monitor projects within the program (PM2).	I	A	C	C	R	C	I	I	R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or Informed.

6.7 Phase 6—Did We Get There?

Figure 6.21—Phase 6 *Did We Get There?*

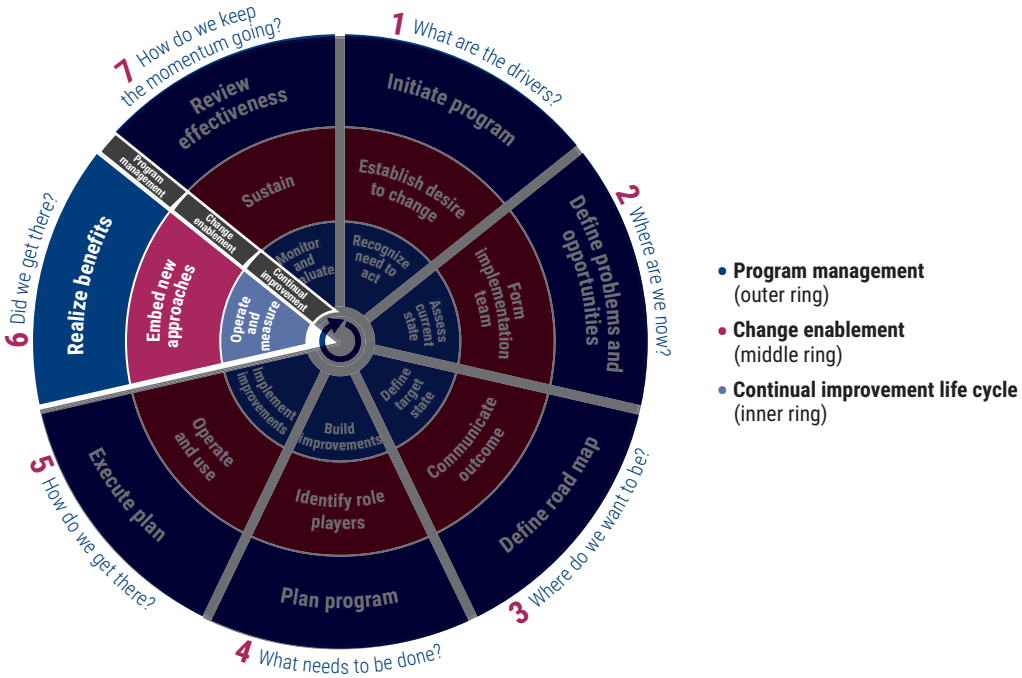


Figure 6.22—Phase 6 Roles

When you are...	Your role in this phase is to...
Board and executive	Assess performance in meeting the original objectives and confirm realization of desired outcomes. Consider the need to redirect future activities and take corrective action. Assist in the resolution of significant issues, if required.
Business management	Provide feedback and consider the effectiveness of the business's contribution to the initiative. Use positive results to improve current business-related activities. Use lessons learned to adapt and improve the business's approach to future initiatives.
IT management	Provide feedback and consider the effectiveness of IT's contribution to the initiative. Use positive results to improve current IT-related activities. Monitor projects based on project criticality as they are developing, using both program management and project management techniques. Be prepared to change the plan and/or cancel one or more projects or take other corrective action, if early indications show that a project is off track and may not meet critical milestones. Use lessons learned to adapt and improve IT's approach to future initiatives.
Internal audit	Provide independent assessment of the overall efficiency and effectiveness of the initiative. Provide feedback and consider the effectiveness of audit's contribution to the initiative. Use positive results to improve current audit-related activities. Use lessons learned to adapt and improve audit's approach to future initiatives.
Risk, compliance and legal	Assess whether the initiative has improved the ability of the enterprise to identify and manage risk and legal, regulatory and contractual requirements. Provide feedback and make any necessary recommendations for improvements.

Figure 6.23—Phase 6 Objectives, Descriptions, Tasks, Inputs, Resources and Outputs	
Description of Phase 6—Did We Get There?	
Phase objective	Integrate the metrics for project performance and benefits realization of the overall governance improvement program into the performance measurement system for regular and ongoing monitoring.
Phase description	It is essential that the improvements described in the program be monitored via alignment goals and process goals using suitable techniques such as an IT balanced scorecard (BSC) and benefits register to verify that the change outcomes have been achieved. This ensures that the initiatives remain on track according to original enterprise and alignment goals and continue to deliver the desired business benefits. For each metric, targets need to be set, compared regularly against reality and communicated using a performance report. To ensure success, it is crucial that positive and negative results from performance measurements be reported to all stakeholders, to build confidence and enable any corrective actions to be taken on time. Projects should be monitored as they are developing, using both program management and project management techniques. Preparation should be made to change the plan and/or cancel the project, if early indications show that a project is off track and may not meet critical milestones.
Continual improvement (CI) tasks	Operate and measure: **1.** Set targets for each metric for an agreed time period. Targets should enable monitoring of I&T performance and improvement actions and determine success or failure. **2.** Obtain current, actual measures for these metrics, where possible. **3.** Gather actual measures and compare them to targets on a regular basis (e.g., monthly). Investigate any significant variances. **4.** Develop and agree on proposed corrective measures, wherever variances indicate that corrective actions are required. **5.** Adjust long-term targets based on experience, if required. **6.** Communicate both positive and negative results from performance monitoring to all interested stakeholders. Include recommendations for any corrective measures.
Change enablement (CE) tasks	Embed new approaches: **1.** Ensure that new ways of working become part of the enterprise's culture. They should be rooted in the enterprise's norms and values. This is important for concrete results to be achieved. **2.** In transitioning from project mode to business as usual, shape behaviors through revised job descriptions, job performance criteria and associated incentive and reward systems, KPIs, and operating procedures as implemented through the change-response plans. **3.** Monitor whether assigned roles and responsibilities have been assumed. **4.** Track the change and assess the effectiveness of the change-response plans, linking the results back to the original change objectives and goals. This should include both hard business measures and perception measures, such as perception surveys, feedback sessions and training evaluation forms. **5.** Leverage pockets of excellence to provide a source of inspiration. **6.** Maintain the communication strategy to achieve ongoing awareness and highlight successes. **7.** Ensure that there is open communication among all role players to resolve issues. **8.** Escalate to sponsors, if issues cannot be resolved. **9.** Enforce change through management authority, where still required. **10.** Document change enablement lessons learned for future implementation initiatives.
Program management (PM) tasks	Realize benefits: **1.** Monitor overall performance of the program against business case objectives. **2.** Monitor investment performance (cost against budget, realization of benefits). **3.** Document lessons learned (both positive and negative) for subsequent improvement initiatives.

Figure 6.23—Phase 6 Objectives, Descriptions, Tasks, Inputs, Resources and Outputs *(cont.)*	
Description of Phase 6—Did We Get There?	
Input	• Implemented improvements • Implemented change response plans • Realized quick wins and success communications • Defined and communicated roles and responsibilities in the business-as-usual environment • Project change logs and issue/risk logs • Defined business and perception success measures • Alignment goals and IT process goals identified as a result of requirements analysis • Existing measures and/or scorecards • Business case benefits • Change response plans and communication strategy
Output	• Updated project and program scorecards • Change effectiveness measures (both business and perception measures) • Report explaining scorecard results • Improvements entrenched in operations • Key metrics added into ongoing IT performance measurement approach
ISACA resources	• *COBIT® 2019 Framework: Governance and Management Objectives* (as good practice input and EDM05, APO05, BAI01, BAI11, MEA01), *www.isaca.org/cobit* • ISACA supporting products as currently listed at *www.isaca.org*

Figure 6.24—Phase 6 RACI Chart

Key Activities	Board	I&T Governance Board	CIO	Business Executive	IT Managers	IT Process Owners	IT Audit	Risk and Compliance	Program Steering
	Responsibilities of Implementation Role Players								
Operate the solutions and gain performance feedback (CI1 to CI3).		I	A	R	R	R	I	I	I
Monitor performance against success metrics (CI4 to CI5).		I	A	C	R	R	C	C	I
Communicate positive and negative results (CI6).	I	I	A	C	R	C	I	I	I
Monitor ownership of roles and responsibilities (CE3).		A	R	C	C	C	C	C	I
Monitor program results (achievement of goals and realization of benefits) (PM1 and PM2).	I	A	C	C	C	C	C	C	R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or Informed.

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

Figure 6.25—Phase 7 *How Do We Keep the Momentum Going?*

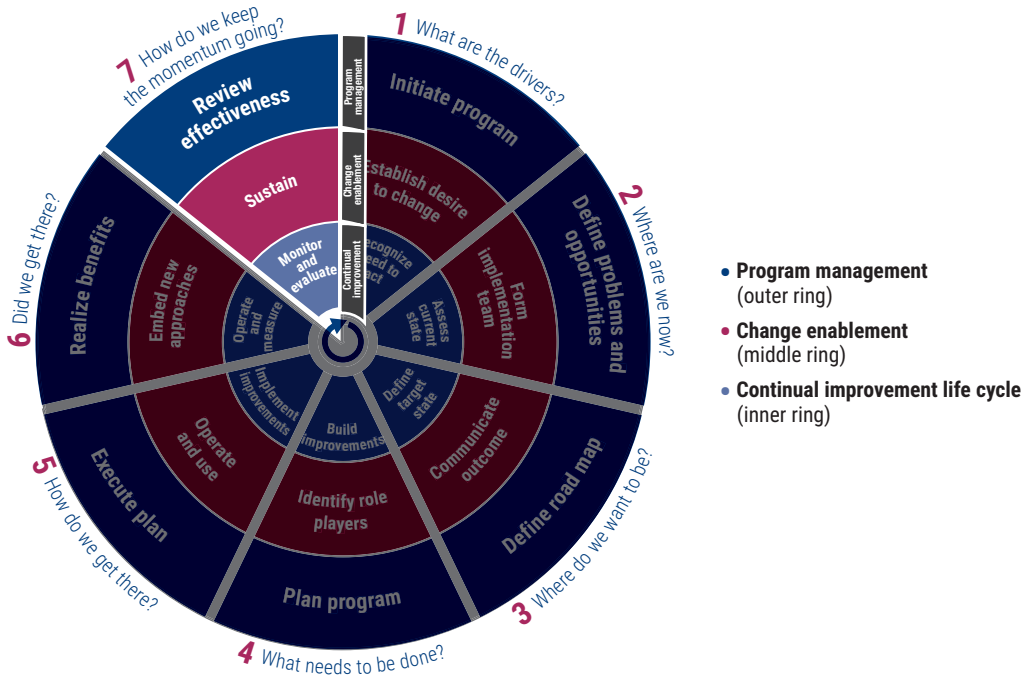


Figure 6.26—Phase 7 Roles

When you are...	Your role in this phase is to...
Board and executive	Provide direction, set objectives, and allocate roles and responsibilities for the enterprise's ongoing approach to, and improvement of, EGIT. Continue to set the tone at the top, develop organizational structures, and encourage a culture of good governance and accountability for I&T among business and IT executives. Ensure that IT is aware of and, as appropriate, involved in, new business objectives and requirements in as timely a manner as possible.
Business management	Provide support and commitment by continuing to work positively with IT to improve EGIT and make it business as usual. Verify that new EGIT objectives are aligned with current enterprise objectives.
IT management	Drive and provide strong leadership to sustain the momentum of the improvement program. Engage in governance activities as part of normal business practice. Create policies, standards and processes to ensure that governance becomes business as usual.
Internal audit	Provide objective and constructive input, encourage self-assessment, and provide assurance to management that governance is working effectively, thus building confidence in I&T. Provide ongoing audits based on an integrated governance approach, using criteria shared with IT and the business based on the COBIT® 2019 framework.
Risk, compliance and legal	Work with IT and the business to anticipate legal and regulatory requirements. Identify and respond to I&T-related risk as a normal activity in EGIT.

Figure 6.27—Phase 7 Objectives, Descriptions, Tasks, Inputs, Resources and Outputs	
Description of Phase 7—How Do We Keep the Momentum Going?	
Phase objective	Assess the results and experience gained from the program. Record and share any lessons learned. Improve organizational structures, processes, roles and responsibilities to change the enterprise's behavior so that EGIT becomes business as usual and is continually optimized. Ensure that new, required actions drive further iterations of the life cycle. Continually monitor performance and ensure that results are regularly reported. Drive commitment and ownership of all accountabilities and responsibilities.
Phase description	This phase enables the team to determine whether the program delivered against expectations. This can be done by comparing the results to the original success criteria and gathering feedback from the implementation team and stakeholders via interviews, workshops and satisfaction surveys. The lessons learned can contain valuable information for team members and project stakeholders for use in ongoing initiatives and improvement projects. It involves continual monitoring, regular and transparent reporting, and confirmation of accountabilities. Further improvements are identified and used as input to the next iteration of the life cycle. In this phase, the enterprise should build on the successes and lessons learned from the governance implementation project(s) to build and reinforce commitment among all IT and business stakeholders for continually improved governance of I&T. Policies, organizational structures, roles and responsibilities, and governance processes should be developed and optimized so that EGIT operates effectively as part of normal business practice and the culture, demonstrated by top management, supports this.
Continual improvement (CI) tasks	Monitor and evaluate: **1.** Identify new governance objectives and requirements based on experiences gained, current business objectives for I&T or other trigger events. **2.** Gather feedback and perform a stakeholder satisfaction survey. **3.** Measure and report actual results against originally established project measures of success. Embed continual monitoring and reporting. **4.** Perform a facilitated project review process with project team members and project stakeholders to record and pass on lessons learned. **5.** Look for additional high-impact, low-cost opportunities to further improve EGIT. **6.** Identify lessons learned. **7.** Communicate requirements for further improvements to the stakeholders and document them for use as input to the next iteration of the life cycle.
Change enablement (CE) tasks	Sustain: **1.** Provide conscious reinforcement and an ongoing communication campaign, as well as demonstrated continual top management commitment. **2.** Confirm conformance to objectives and requirements. **3.** Continually monitor the effectiveness of the change itself, change enablement activities and buy-in of stakeholders. **4.** Implement corrective action plans where required. **5.** Provide feedback on performance, reward achievers and publicize successes. **6.** Build on lessons learned. **7.** Share knowledge from the initiative to the broader enterprise.
Program management (PM) tasks	Review program effectiveness: **1.** At program closure, ensure that a program review takes place and approve conclusions. **2.** Review program effectiveness.
Input	• Updated project and program scorecards • Change effectiveness measures (both business and perception measures) • Report explaining scorecard results • Postimplementation review report • Performance reports • Business and IT strategy • New triggers such as new regulatory requirements

Figure 6.27—Phase 7 Objectives, Descriptions, Tasks, Inputs, Resources and Outputs *(cont.)*	
Description of Phase 7—How Do We Keep the Momentum Going?	
Output	• Recommendations for further EGIT activities after a period of normalization • Stakeholder satisfaction survey • Documented success stories and lessons learned • Ongoing communication plan • Performance reward scheme
ISACA resources	• *COBIT® 2019 Framework: Governance and Management Objectives* (EDM01, APO01, BAI08, MEA01), *www.isaca.org/cobit* • ISACA supporting products as currently listed at *www.isaca.org*

Figure 6.28—Phase 7 RACI Chart

Key Activities	Board	I&T Governance Board	CIO	Business Executive	IT Managers	IT Process Owners	IT Audit	Risk and Compliance	Program Steering
	Responsibilities of Implementation Role Players								
Identify new governance objectives (CI1).	C	A	R	R	C	C	C	C	I
Identify lessons learned (CI2).		I	A	C	R	R	C	C	I
Sustain and reinforce changes (CE1).		A	R	R	R	R	C	C	I
Confirm conformance to objectives and requirements (CE2).	I	A	R	C	R	R	R	I	R
Close program with formal review of effectiveness (PM1).	I	A	C	C	C	C	C	C	R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or Informed.

APPENDIX A
Example Decision Matrix

This appendix shows an example of how to identify key topic areas requiring clear decision-making roles and responsibilities. It is provided as a guide and can be modified and adapted to suit an enterprise's specific organization and requirements.[14]

Figure A.1—Example Decision Matrix

Decision Topic	Scope	Responsible, Accountable, Consulted, Informed (RACI)							
		Executive Committee	I&T Governance Board	Enterprise Risk Committee	Portfolio Manager	Steering (Programs/Projects) Committee	IT Management[15]	Business Process Owners	Employees
Governance	• Integrating with enterprise governance • Establishing principles, structures, objectives	A/R	R	C			C	R	I
Enterprise strategy	• Defining enterprise goals and objectives • Deciding where and how I&T can enable and support enterprise objectives	A/R	R	C			C	R	I
I&T policies	• Providing accurate, understandable and approved policies, procedures, guidelines and other documentation to stakeholders • Developing and rolling out I&T policies • Ensuring that policies result in beneficial outcomes in accordance with guiding principles • Enforcing I&T policies	I	A	C			R	C	C
I&T strategy	• Incorporating IT and business management in the translation of business requirements into service offerings and developing strategies to deliver these services in a transparent and effective manner • Engaging with business and senior management in aligning I&T strategic planning with current and future business needs • Understanding current I&T capabilities • Providing a prioritization scheme for business objectives that quantifies business requirements	I	A	C	I		R	C	C

[14] This example is based on the EGIT matrix developed by IT Winners. It is used with their permission.
[15] IT management includes all roles within the IT function at a management level.

Figure A.1—Example Decision Matrix *(cont.)*

Decision Topic	Scope	Responsible, Accountable, Consulted, Informed (RACI)							
		Executive Committee	I&T Governance Board	Enterprise Risk Committee	Portfolio Manager	Steering (Programs/Projects) Committee	IT Management[15]	Business Process Owners	Employees
I&T direction	• Providing appropriate platforms for the business applications and services in line with the defined I&T architecture and information & technology standards • Producing an information and technology provisioning plan	I	C	C			A/R	C	C
I&T methods and frameworks	• Establishing transparent, flexible and responsive IT organizational structures and defining and implementing I&T processes that integrate owners, roles and responsibilities into business and decision processes • Defining a practical I&T process framework • Establishing appropriate organizational bodies and structure • Defining roles and responsibilities	I	C	C	I	I	A/R	I	I
Enterprise architecture	• Defining and implementing architecture and standards that recognize and leverage technology opportunities • Establishing a forum to guide architecture and verify compliance • Establishing the architecture plan balanced against cost, risk and requirements • Defining the information architecture, including the establishment of an enterprise data model that incorporates a data classification scheme • Ensuring the accuracy of the information architecture and data model • Assigning data ownership • Classifying information using an agreed classification scheme	A	C	C	I	I	R	R	C
I&T-enabled investment and portfolio prioritization	• Making effective and efficient I&T-enabled investment and portfolio decisions • Forecasting and allocating budgets • Defining formal investment criteria • Measuring and assessing business value against forecast	I	A		C	C	R		

[15] IT management includes all roles within the IT function at a management level.

Figure A.1—Example Decision Matrix *(cont.)*

Decision Topic	Scope	Responsible, Accountable, Consulted, Informed (RACI)							
		Executive Committee	I&T Governance Board	Enterprise Risk Committee	Portfolio Manager	Steering (Programs/Projects) Committee	IT Management[15]	Business Process Owners	Employees
I&T-enabled investment and program prioritization	• Setting and tracking I&T budgets in line with I&T strategy and investment decisions • Measuring and assessing business value against forecast • Defining a program and project management approach that is applied to I&T-enabled business projects and enables stakeholder participation in, and monitoring of, project risk and progress • Defining and enforcing program and project frameworks and approach • Issuing project management guidelines • Performing project planning for each project detailed in the project portfolio	I	A		R	C	C/I	C/I	C/I
Managing, monitoring and evaluating SLAs	• Identifying service requirements, agreeing on service levels and monitoring the achievement of service levels • Formalizing internal and external agreements in line with requirements and delivery capabilities • Reporting on service level achievements (reports and meetings) • Identifying and communicating new and updated service requirements to strategic planning • Meeting operational service levels for scheduled data processing, protecting sensitive output, and monitoring and maintaining infrastructure	I	A	R			R	R	I

[15] IT management includes all roles within the IT function at a management level.

Figure A.1—Example Decision Matrix *(cont.)*									
		Responsible, Accountable, Consulted, Informed (RACI)							
Decision Topic	Scope	Executive Committee	I&T Governance Board	Enterprise Risk Committee	Portfolio Manager	Steering (Programs/Projects) Committee	IT Management[15]	Business Process Owners	Employees
IT application management	• Identifying technically feasible and cost-effective solutions • Defining business and technical requirements • Undertaking feasibility studies as defined in the development standards • Approving (or rejecting) requirements and feasibility study results • Ensuring that there is a timely and cost-effective development or acquisition process • Translating business requirements into design specifications • Selecting appropriate development and maintenance standards (waterfall, Agile, DevOps, etc.) and adhering to the standards for all modifications • Separating development, testing and operational activities	I	I	C			A/R	C	C
IT infrastructure	• Operating the IT environment in line with agreed service levels and defined instructions • Maintaining the IT infrastructure	I	I	C			A/R	C	C
I&T security	• Defining I&T security policies, plans and procedures and monitoring, detecting, reporting and resolving security vulnerabilities and incidents • Understanding security requirements, including privacy and cybersecurity, vulnerabilities and threats, in line with business requirements and impact • Managing user identities and authorizations in a standardized manner • Testing security regularly	I	A	R			R	R	C/I
Procurement and contracts	• Acquiring and maintaining I&T resources that respond to the delivery strategy, establishing an integrated and standardized IT infrastructure, and reducing IT procurement risk • Obtaining professional legal and contractual advice • Defining procurement procedures and standards • Procuring requested hardware, software and services in line with defined procedures	I	I	C			A/R	C	C

[15] IT management includes all roles within the IT function at a management level.

Figure A.1—Example Decision Matrix *(cont.)*

Decision Topic	Scope	Responsible, Accountable, Consulted, Informed (RACI)							
		Executive Committee	I&T Governance Board	Enterprise Risk Committee	Portfolio Manager	Steering (Programs/Projects) Committee	IT Management[15]	Business Process Owners	Employees
I&T compliance	• Identifying all applicable laws, regulations and contracts; defining the corresponding level of I&T compliance; and optimizing IT processes to reduce the risk of noncompliance • Identifying legal, regulatory and contractual requirements related to I&T • Assessing the impact of compliance requirements • Monitoring and reporting on compliance with these requirements	C/I	A	C			A/R	C	C/I

[15] IT management includes all roles within the IT function at a management level.

Page intentionally left blank