Chapter 1
Introduction

1.1 Enterprise Governance of Information and Technology

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

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

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

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

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

1.2 Benefits of Information and Technology Governance

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

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

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

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

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

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

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

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

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

1.3 COBIT as an I&T Governance Framework

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

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

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

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

1.3.1 What Is COBIT and What Is It Not?

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

COBIT is a framework for the governance and management of enterprise information and technology,[4] aimed at the whole enterprise. Enterprise I&T means all the technology and information processing the enterprise puts in place to achieve its goals, regardless of where this happens in the enterprise. In other words, enterprise I&T is not limited to the IT department of an organization, but certainly includes it.

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

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

In most enterprises, overall governance is the responsibility of the board of directors, under the leadership of the chairperson. Specific governance responsibilities may be delegated to special organizational structures at an appropriate level, particularly in larger, complex enterprises.

- **Management** plans, builds, runs and monitors activities, in alignment with the direction set by the governance body, to achieve the enterprise objectives.

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

COBIT defines the components to build and sustain a governance system: processes, organizational structures, policies and procedures, information flows, culture and behaviors, skills, and infrastructure.[5]

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

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

Several misconceptions about COBIT should be dispelled:

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

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

1.4 Structure of This Publication

The remainder of this publication contains the following chapters:

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