ISACA®
Trust in, and value from, information systems

COBIT® 5

for Risk

COBIT® 5
AN ISACA® FRAMEWORK

With information and technology at the heart of creating value for enterprises, it is more important than ever for organizations to optimize their IT risk approach in order to effectively identify related risks, opportunities and meet enterprise objectives.

To that purpose, this publication:

- Provides guidance on how to use the COBIT 5 framework to establish the risk governance and management functions
- for the enterprise
- Provides guidance and a structured approach on how to use the COBIT 5 principles to govern and manage IT risk
- Demonstrates how COBIT 5 for Risk aligns with other relevant standards

The preceding pages provide a preview of the information contained in COBIT 5 for Risk.

To purchase COBIT 5 for Risk, or to learn more visit *www.isaca.org/cobit5*.

Not a member? Learn the value of ISACA membership. Additional information is available at *www.isaca.org/membervalue*.

ISACA®
With more than 110,000 constituents in 180 countries, ISACA (*www.isaca.org*) helps business and IT leaders maximize value and manage risk related to information and technology. Founded in 1969, the non-profit, independent ISACA is an advocate for professionals involved in information security, assurance, risk management and governance. These professionals rely on ISACA as the trusted source for information and technology knowledge, community, standards and certification. The association, which has 200 chapters worldwide, advances and validates business-critical skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) credentials. ISACA also developed and continually updates COBIT®, a business framework that helps enterprises in all industries and geographies govern and manage their information and technology.

Disclaimer
ISACA has designed and created *COBIT® 5 for Risk* (the 'Work') primarily as an educational resource for assurance 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, assurance professionals should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

Reservation of Rights

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: *info@isaca.org*
Web site: *www.isaca.org*

Provide Feedback: *www.isaca.org/cobit*
Participate in the ISACA Knowledge Center: *www.isaca.org/knowledge-center*
Follow ISACA on Twitter: *https://twitter.com/ISACANews*
Join ISACA on LinkedIn: ISACA (Official), *http://linkd.in/ISACAOfficial*
Like ISACA on Facebook: *www.facebook.com/ISACAHQ*

COBIT® 5 for Risk
ISBN: 978-1-60420-458-2
1

ACKNOWLEDGEMENTS

ISACA wishes to recognise:

COBIT for Risk Task Force
Steven A. Babb, CGEIT, CRISC, ITIL, Betfair, UK, Chairman
Evelyn Anton, CISA, CISM, CGEIT, CRISC, Uruguay
Jean-Louis Bleicher, CRISC, France
Derek Oliver, Ph.D., CISA, CISM, CRISC, FBCS, FISM, MInstISP, Ravenswood Consultants Ltd., UK
Steve Reznik, CISA, ADP Inc., USA
Gladys Rouissi, CISA, ANZ Bank, Australia
Alok Tuteja, CGEIT, CRISC, Mazrui Holdings LLC, UAE

Development Team
Floris Ampe, CISA, CGEIT, CRISC, CIA, ISO 27000, PwC, Belgium
Stefanie Grijp, PwC, Belgium
Bart Peeters, CISA, PwC, Belgium
Dirk Steuperaert, CISA, CGEIT, CRISC, ITIL, IT In Balance BVBA, Belgium
Sven Van Hoorebeeck, PwC, Belgium

Workshop Participants
Elza Adams, CISA, CISSP, PMP, IBM, USA
Yalcin Gerek, CISA, CGEIT, CRISC, TAC, Turkey
Jimmy Heschl, CISA, CISM, CGEIT, Bwin.party Digital Entertainment Plc, Austria
Mike Hughes, CISA, CGEIT, CRISC, 123 Consultants GRC Ltd., UK
Jack Jones, CISA, CISM, CRISC, CISSP, Risk Management Insight, USA
Andre Pitkowski, CGEIT, CRISC, APIT Informatica Ltd, Brazil
Eduardo Ritegno, CISA, CRISC, Banco de la Nacion Argentina, Argentina
Robert Stroud, CGEIT, CRISC, CA Technologies, USA
Nicky Tiesenga, CISA, CISM, CGEIT, CRISC, IBM, USA

Expert Reviewers
Elza Adams, CISA, CISSP, PMP, IBM, USA
Mark Adler, CISA, CISM, CGEIT, CRISC, CIA, CRP, CFE, CISSP, Wal-Mart Stores Inc., USA
Michael Berardi, CISA, CGEIT, CRISC, Bank of America, USA
Peter R. Bitterli, CISA, CISM, CGEIT, Bitterli Consulting AG, Switzerland
Sushil Chatterji, CGEIT, CMC, CEA, Edutech Enterprises, Singapore
Frank Cindrich, CGEIT, CIPP/G, CIPP/US, Deloitte and Touche, LLP, USA
Diego Patricio del Hoyo, Westpac Banking Corporation, Australia
Michael Dickson, CISA, CISM, CRISC, CPA, GBQ Partners, USA
AnnMarie DonVito, CISA, CISSP, ISSAP, ISO 27001 Lead Auditor, PRINCE2 Practitioner, ITIL Foundation V3, Deloitte AG, Switzerland
Ken Doughty, CISA, CRISC, CRMA, ANZ, Australia
Urs Fischer, CRISC, CISA, CPA (Swiss), Fischer IT GRC Consulting and Training, Switzerland
Shawna Flanders, CISA, CISM, CRISC, CSSGB, PSCU, USA
Joseph Fodor, CISA, CPA, Ernst and Young LLP, USA
Yalcin Gerek, CISA, CGEIT, CRISC, TAC, Turkey
J. Winston Hayden, CISA, CISM, CGEIT, CRISC, South Africa
Mike Hughes, CISA, CGEIT, CRISC, 123 Consultants GRC Ltd., UK
Duc Huynh, CISA, ANZ Wealth, Australia
Monica Jain, CGEIT, Southern California Edison (SCE), USA
Waleed Khalid, CISA, MetLife, UK
John W. Lainhart, IV, CISA, CISM, CGEIT, CRISC, CIPP/G, CIPP/US, IBM Global Business Services, USA
Debbie Lew, CISA, CRISC, Ernst and Young LLP, USA
Marcia Maggiore, CISA, CRISC, Consultor en TI, Argentina
Lucio Augusto Molina Focazzio, CISA, CISM, CRISC, Independent Consultant, Colombia
Anthony Noble, CISA, Viacom Inc., USA
Abdul Rafeq, CISA, CGEIT, A.Rafeq and Associates, India
Salomon Rico, CISA, CISM, CGEIT, Deloitte, Mexico
Eduardo Ritegno, CISA, CRISC, Banco de la Nacion Argentina, Argentina

ACKNOWLEDGEMENTS *(CONT.)*

Expert Reviewers *(cont.)*
Paras Kesharichand Shah, CISA, CGEIT, CRISC, Vital Interacts, Australia
Mark Stacey, CISA, FCA, BG Group plc, UK
Robert Stroud, CGEIT, CRISC, CA Technologies, USA
Greet Volders, CGEIT, Voquals N.V., Belgium
John A. Wheeler, CRISC, Gartner, USA
Tichaona Zororo, CISA, CISM, CGEIT, CRISC, CIA, CRMA, EGIT | Enterprise Governance of IT (PTY) LTD, South Africa

ISACA Board of Directors
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, International President
Allan Boardman, CISA, CISM, CGEIT, CRISC, ACA, CA (SA), CISSP, Morgan Stanley, UK, Vice President
Juan Luis Carselle, CISA, CGEIT, CRISC, RadioShack, Mexico, Vice President
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, Six Sigma Black Belt, Dell, Spain, Vice President
Theresa Grafenstine, CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA, US House of Representatives, USA, Vice President
Vittal Raj, CISA, CISM, CGEIT, CFE. CIA, CISSP, FCA, Kumar and Raj, India, Vice President
Jeff Spivey, CRISC, CPP, PSP, Security Risk Management Inc., USA, Vice President
Marc Vael, Ph.D., CISA, CISM, CGEIT, CRISC, CISSP, Valuendo, Belgium, Vice President
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Past International President
Kenneth L. Vander Wal, CISA, CPA, Ernst and Young LLP (retired), USA, Past International President
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, Director
Krysten McCabe, CISA, The Home Depot, USA, Director
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, BRM Holdich, Australia, Director

Knowledge Board
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, Chairman
Rosemary M. Amato, CISA, CMA, CPA, Deloitte Touche Tohmatsu Ltd., The Netherlands
Steven A. Babb, CGEIT, CRISC, Betfair, UK
Thomas E. Borton, CISA, CISM, CRISC, CISSP, Cost Plus, USA
Phil J. Lageschulte, CGEIT, CPA, KPMG LLP, USA
Anthony P. Noble, CISA, Viacom, USA
Jamie Pasfield, CGEIT, ITIL V3, MSP, PRINCE2, Pfizer, UK

Framework Committee
Steven A. Babb, CGEIT, CRISC, Betfair, UK, Chairman
David Cau, France
Sushil Chatterji, Edutech Enterprises, Singapore
Frank Cindrich, CGEIT, CIPP/G, CIPP/US, Deloitte and Touche, LLP, USA
Joanne T. De Vita De Palma, The Ardent Group, USA
Jimmy Heschl, CISA, CISM, CGEIT, Bwin.party Digital Entertainment Plc, Austria
Katherine McIntosh, CISA, Central Hudson Gas and Electric Corp., USA
Andre Pitkowski, CGEIT, CRISC, APIT Informatica, Brasil
Paras Kesharichand Shah, CISA, CGEIT, CRISC, Vital Interacts, Australia

Special recognition for financial support:
Los Angeles Chapter

Table of Contents

List of Figures

EXECUTIVE SUMMARY

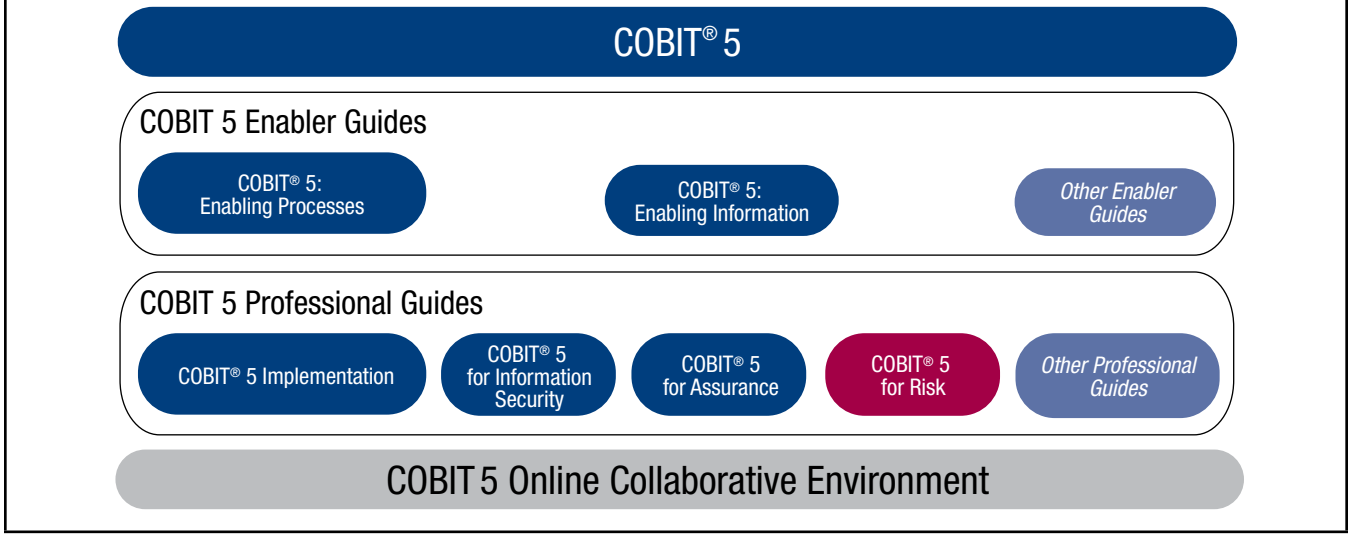
Introduction

Information is a key resource for all enterprises. From the time information is created to the moment it is destroyed, technology plays a significant role in containing, distributing and analysing information. Technology is increasingly advanced and has become pervasive in enterprises and the social, public and business environments.

COBIT 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise information technology (IT). Simply stated, COBIT 5 helps enterprises to create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use. COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking into account the full end-to-end business and IT functional areas of responsibility and considering the IT-related interests of internal and external stakeholders.

COBIT 5 for Risk, highlighted in **figure 1**, builds on the COBIT 5 framework by focusing on risk and providing more detailed and practical guidance for risk professionals and other interested parties at all levels of the enterprise.

Figure 1—COBIT 5 Product Family



Terminology

COBIT 5 for Risk discusses IT-related risk. Section 1, chapter 2 defines what is meant by IT-related risk; however, for ease of reading, the term 'risk' is used throughout the publication, which refers to IT-related risk. The guidance and principles that are explained throughout this publication are applicable to any type of enterprise, whether it operates in a commercial or non-commercial context, in the private or the public sector, as a small, medium or large enterprise.

COBIT 5 for Risk presents two perspectives on how to use COBIT 5 in a risk context: risk function and risk management. The **risk function perspective** focuses on what is needed to build and sustain the risk function within an enterprise. The **risk management perspective** focuses on the core risk governance and management processes of how to optimise risk and how to identify, analyse, respond to and report on risk on a daily basis. These perspectives are explained in detail in section 1, chapter 2. Risk; section 2A, The Risk Function Perspective; and section 2B, The Risk Management Perspective and Using COBIT 5 Enablers.

Drivers for Risk Management

The main drivers for risk management in its different forms include the need to improve business outcomes, decision making and overall strategy by providing:
- Stakeholders with substantiated and consistent opinions on the current state of risk throughout the enterprise
- Guidance on how to manage the risk to levels within the risk appetite of the enterprise

- Guidance on how to set up the appropriate risk culture for the enterprise
- Wherever possible, quantitative risk assessments that enable stakeholders to consider the cost of mitigation and the required resources against the loss exposure

To that purpose, this publication:
- Provides guidance on how to use the COBIT 5 framework to establish the risk governance and management functions for the enterprise
- Provides guidance and a structured approach on how to use the COBIT 5 principles to govern and manage IT risk
- Demonstrates how *COBIT 5 for Risk* aligns with other relevant standards

Benefits of Using This Publication

Using *COBIT 5 for Risk* increases the enterprise risk-related capabilities, which provide benefits such as:
- More accurate identification of risk and measurement of success in addressing that risk
- Better understanding of risk impact on the enterprise
- End-to-end guidance on how to manage risk, including an extensive set of measures
- Knowledge of how to capitalise on investments related to IT risk-management practices
- Understanding of how effective IT risk management optimises value, with business process effectiveness and efficiency, improved quality and reduced waste and costs
- Opportunities to integrate IT risk management with enterprise risk and compliance structures
- Improved communication and understanding amongst all internal and external stakeholders due to the common and sustainable globally accepted framework and language for assessing and responding to risk
- Promotion of risk responsibility and acceptance across the enterprise
- A complete risk profile, identifying the full enterprise risk exposure and enabling better utilisation of enterprise resources
- Improved risk awareness throughout the enterprise

Target Audience for This Publication

The intended audience for *COBIT 5 for Risk* is extensive, as are the reasons for adopting and using the framework and the benefits that each enterprise role and function can find in this publication. The roles and functions that are listed in **figure 2** are considered stakeholders for the management of risk. These stakeholders do not necessarily refer to individuals, but to roles and functions within the enterprise or its environment.

Figure 2—*COBIT 5 for Risk* Target Audience and Benefits

Role/Function	Benefit of/Reason for Adopting and Adapting *COBIT 5 for Risk*
Board and executive management	• Better understanding of their responsibilities and roles with regard to IT risk management and the implications of IT risk to enterprise strategic objectives • Better understanding of how to optimise IT use for successful strategy execution
Risk function and corporate risk managers for enterprise risk management (ERM)	Assistance with managing IT risk, according to generally accepted ERM principles, and incorporating IT risk into enterprise risk
Operational risk managers	• Linkage of their framework to *COBIT 5 for Risk* • Identification of operational losses or development of key risk indicators (KRIs)
IT management	Better understanding of how to identify and manage IT risk and how to communicate IT risk to business decision makers
IT service managers	Enhancement of their view of operational risk, which should fit into an overall IT risk management framework
Business continuity	Alignment with ERM, because assessment of risk is a key aspect of their responsibility
IT security	Positioning security risk amongst other categories of IT risk
Information security	Positioning IT risk within the enterprise information risk management structure
Chief financial officer (CFO)	Gaining a better view of IT risk and its financial implications for investment and portfolio management purposes
Enterprise governance officers	Assistance with their review and monitoring of governance responsibilities and other IT governance roles
Business	Understanding and management of IT risk—one of many business risk items, all of which should be managed consistently

Figure 2—COBIT 5 for Risk Target Audience and Benefits *(cont.)*	
Role/Function	**Benefit of/Reason for Adopting and Adapting COBIT 5 for Risk**
Internal auditors	Improved analysis of risk in support of audit plans and reports
Compliance	Support with the role as key advisors to the risk function with regards to compliance requirements and their potential impact on the enterprise
General counsel	Support with the role as key advisor for the risk function on regulation-related risk and potential impact or legal implications
Regulators	Support of their assessment of regulated enterprise IT risk management approach and the impact of risk on regulatory requirements
External auditors	Additional guidance on exposure levels when establishing an opinion on the quality of internal control
Insurers	Support with establishing adequate IT insurance coverage and seeking agreement on exposure levels
Rating agencies	In collaboration with insurers, a reference to assess and rate objectively how an enterprise is managing IT risk
IT contractors and subcontractors	• Better alignment of utility and warranty of IT services provided • Understanding of responsibilities arising from risk assessment

Note: The guidance and principles that are provided in this publication are applicable to all enterprises, irrespective of size, industry and nature.

Overview and Guidance on Use of This Publication

COBIT 5 for Risk addresses fundamental questions and issues about IT risk management. **Figure 3** shows these questions and explains how and where *COBIT 5 for Risk* addresses them, if they are within the scope of this guide.

COBIT 5 for Risk refers to the seven enablers of COBIT 5:
- Principles, Policies and Frameworks
- Processes
- Organisational Structures
- Culture, Ethics and Behaviour
- Information
- Services, Infrastructure and Applications
- People, Skills and Competencies

The unique character of each enterprise will result in these enablers being implemented and used in many different ways to manage risk in an optimal manner. This guide provides a pervasive view that explains each concept of COBIT 5 from a risk function perspective through additional guidance and examples.

To facilitate and guide the reader through the comprehensive collection of information, *COBIT 5 for Risk* is divided into three sections and six appendices. Following is a brief description of each section and how those sections are interconnected.

Section 1—Elaborates on risk and risk management and describes briefly how the COBIT 5 principles can be applied to risk management-specific needs. This section provides the reader with a conceptual baseline that is followed throughout the rest of the document.

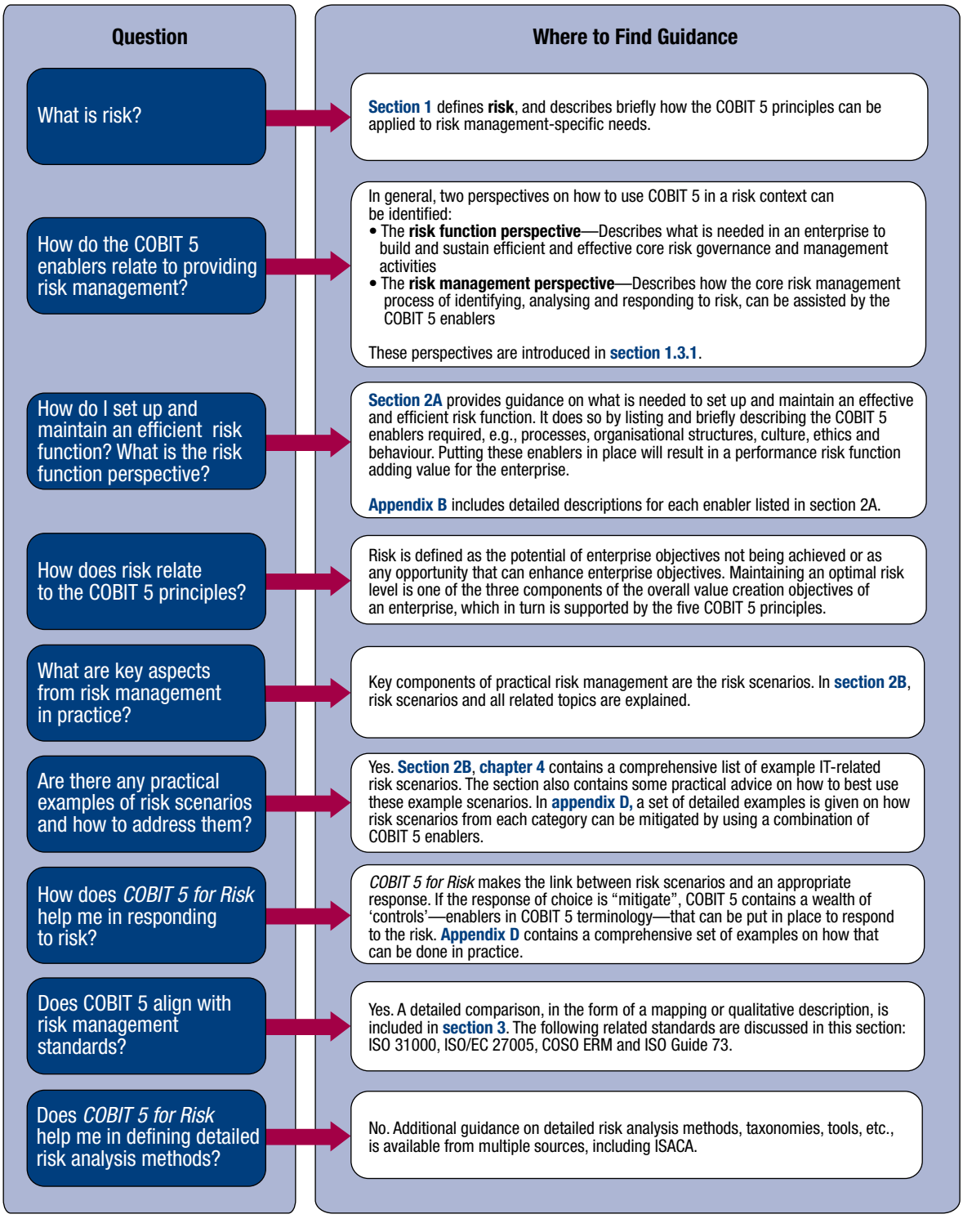
Section 2—Elaborates on using COBIT 5 enablers for risk management in practice. Governance of enterprise IT (GEIT) is systemic and supported by a set of enablers. In this section, the two perspectives on how to apply the COBIT 5 enablers are explained. Detailed guidance regarding these enablers is provided in the appendices.

Section 2A—Describes the COBIT 5 enablers that are required to build and sustain a risk function.

Section 2B—Describes how the core risk management process of identifying, analysing and responding to risk can be assisted by the COBIT 5 enablers. This section also provides some generic risk scenarios.

Section 3—Introduces the alignment of *COBIT 5 for Risk* with relevant IT or ERM standards and practices, including COSO ERM, ISO 31000, ISO/IEC 27005 and ISO Guide 73. This section also includes a comparison between *COBIT 5 for Risk* and these standards.

Figure 3—*COBIT 5 for Risk* Overview



Appendices—Contain the glossary and detailed guidance for the enablers introduced in section 2:
- **Appendix A**—Glossary
- **Appendix B**—Detailed information on enablers for risk governance and management regarding the enablers:
  - B.1—Principles, Policies and Frameworks
  - B.2—Processes
  - B.3—Organisational Structures
  - B.4—Culture, Ethics and Behaviour
  - B.5—Information
  - B.6—Services, Infrastructure Applications
  - B.7—People, Skills and Competencies

- **Appendix C**—Detailed description of core risk management processes
- **Appendix D**—Risk scenarios guidance, containing a comprehensive set of examples on how to mitigate risk scenarios using COBIT 5 enablers
- **Appendix E**—Comparison between *COBIT 5 for Risk* and the legacy *Risk IT Framework*
- **Appendix F**—Template for risk scenario description

Prerequisite Knowledge

COBIT 5 for Risk builds on COBIT 5. Most key concepts of COBIT 5 are repeated and elaborated on, making this guide a fairly standalone book—in essence, not requiring any prerequisite knowledge. However, an understanding of COBIT 5 and its enablers at the foundation level will accelerate the understanding of this guide.

If readers wish to know more about the COBIT 5 concepts beyond what is required for risk management purposes, they are referred to the COBIT 5 framework.

COBIT 5 for Risk also refers to the *COBIT Process Assessment Model (PAM): Using COBIT 5* and the COBIT 5 processes described therein. If readers want to know more about the COBIT 5 processes, e.g., to implement or improve some of them as part of a risk response, they are referred to the *COBIT 5: Enabling Processes* publication.

The COBIT 5 product set also includes a process capability model that is based on the internationally recognised ISO/IEC 15504 Software Engineering—Process Assessment standard. Even though the process assessment model is not prerequisite knowledge for *COBIT 5 for Risk*, readers can use this model as a means to assess the performance of any of the governance or management processes and to identify areas for improvement.

Page intentionally left blank

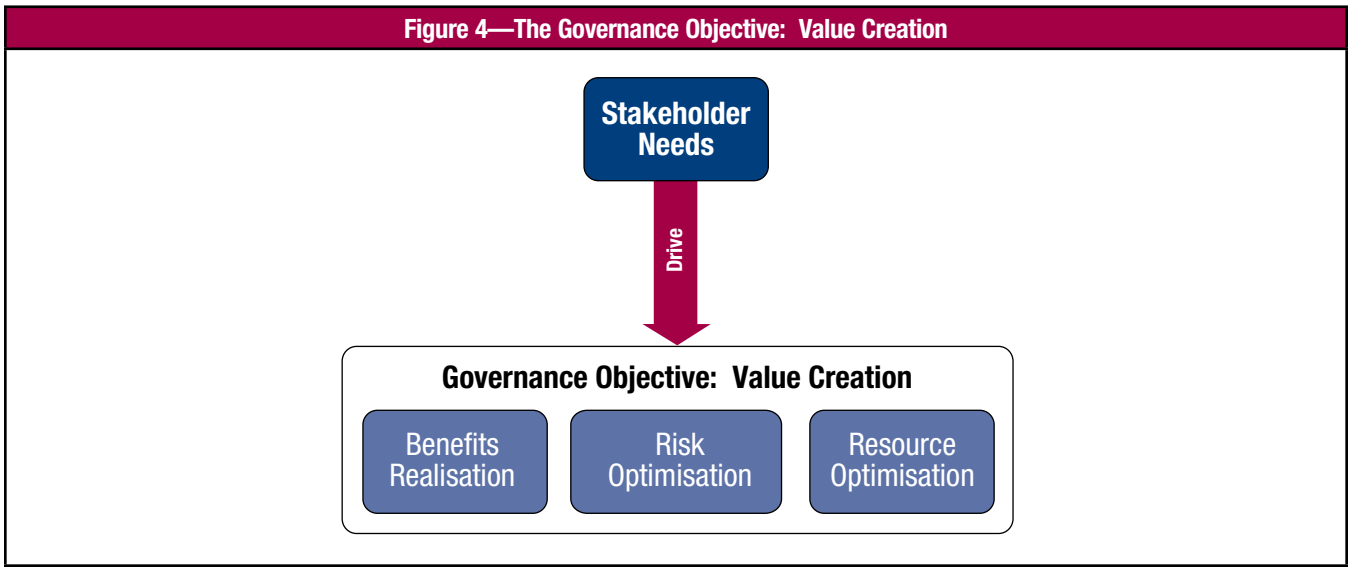
Section 1. Risk and Risk Management

Chapter 1
The Governance Objective: Value Creation

Enterprises exist to create value for their stakeholders. Consequently, any enterprise, commercial or not, has value creation as a governance objective.

Value creation means realising benefits at an optimal resource cost **while optimising risk** (**figure 4**). Benefits can take many forms, e.g., financial for commercial enterprises or public service for government entities.

Figure 4—The Governance Objective: Value Creation



Enterprises have many stakeholders, and 'creating value' means different, and sometimes conflicting, things to each stakeholder. Governance is about negotiating and deciding amongst different stakeholder value interests.

The risk optimisation component of value creation shows that:
- Risk optimisation is an essential part of any governance system.
- Risk optimisation cannot be seen in isolation, i.e., actions taken as part of risk management will influence benefits realisation and resource optimisation.

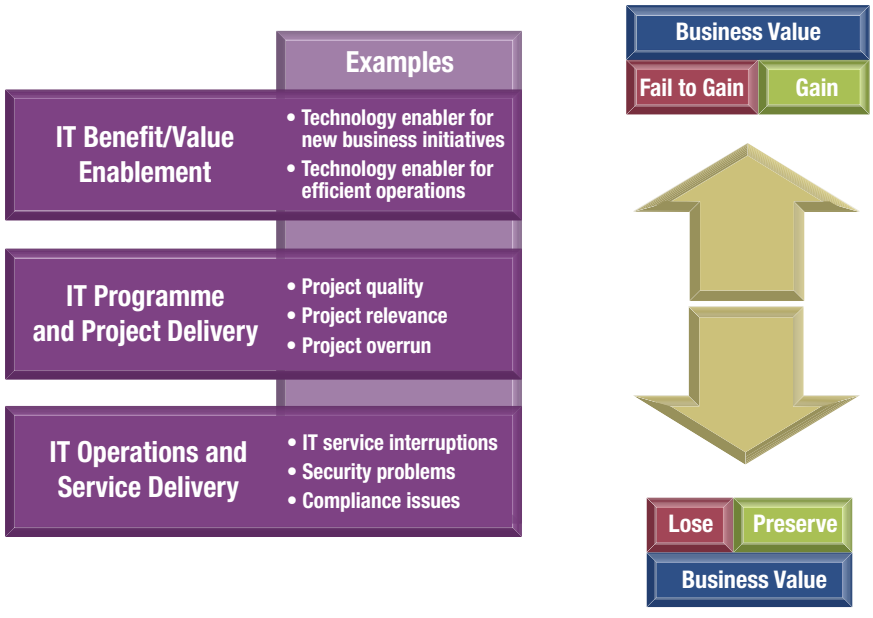
Page intentionally left blank

CHAPTER 2
RISK

Risk is generally defined as the combination of the probability of an event and its consequence (ISO Guide 73). Consequences are that enterprise objectives are not met. *COBIT 5 for Risk* defines IT risk as business risk, specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. IT risk consists of IT-related events that could potentially impact the business. IT risk can occur with both uncertain frequency and impact and creates challenges in meeting strategic goals and objectives.

IT risk always exists, whether or not it is detected or recognised by an enterprise.

Figure 5—IT Risk Categories



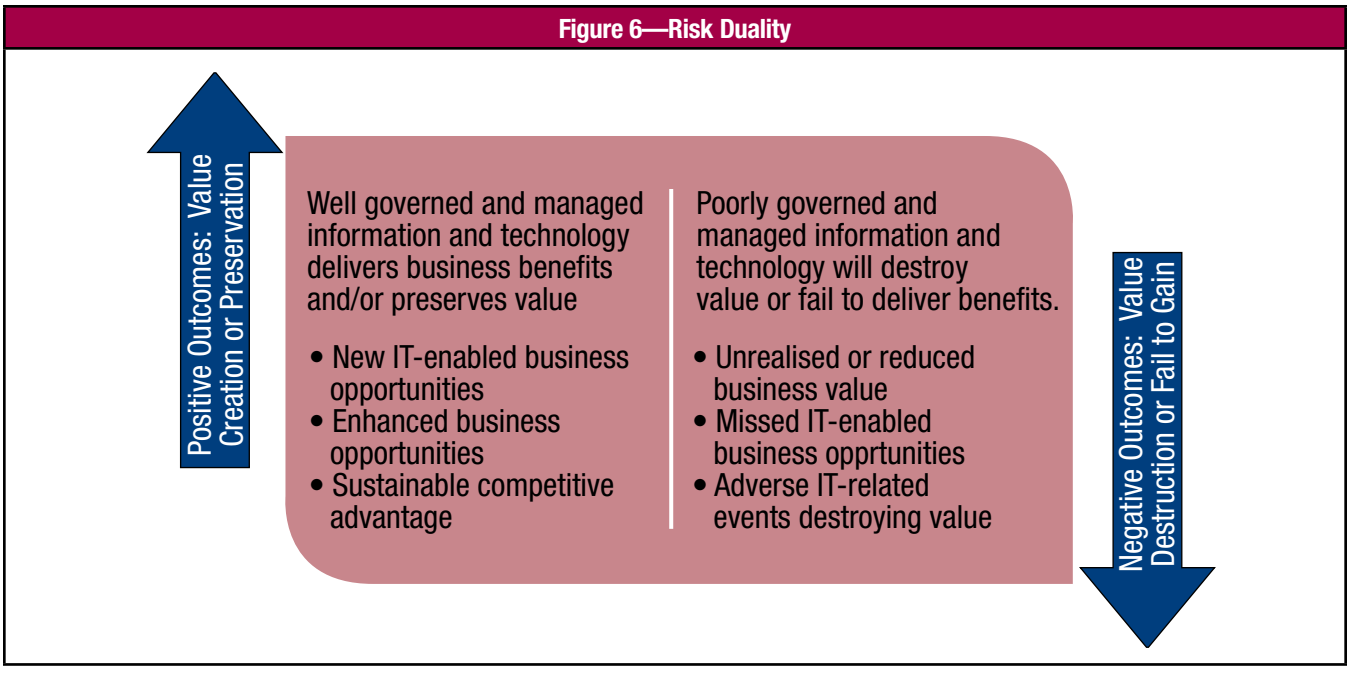
Source: ISACA, *The Risk IT Framework*, 2009, figure 2

IT risk can be categorised as follows:
- **IT benefit/value enablement risk**—Associated with missed opportunities to use technology to improve efficiency or effectiveness of business processes or as an enabler for new business initiatives
- **IT programme and project delivery risk**—Associated with the contribution of IT to new or improved business solutions, usually in the form of projects and programmes as part of investment portfolios
- **IT operations and service delivery risk**—Associated with all aspects of the business as usual performance of IT systems and services, which can bring destruction or reduction of value to the enterprise

Figure 5 shows that for all categories of downside IT risk ('Fail to Gain' and 'Lose' business value) there is an equivalent upside ('Gain' and 'Preserve' business). For example:
- **Service delivery**—If service delivery practices are strengthened, the enterprise can benefit, e.g., by being ready to absorb additional transaction volumes or market share.
- **Project delivery**—Successful project delivery brings new business functionality.

It is important to keep this upside/downside duality of risk in mind (see **figure 6**) during all risk-related decisions. For example, decisions should consider:
- The exposure that may result if a risk is not mitigated versus the benefit if the associated loss exposure is reduced to an acceptable level.
- The potential benefit that may accrue if opportunities are taken versus missed benefits if opportunities are foregone.

Figure 6—Risk Duality



Risk is not always to be avoided. Doing business is about taking risk that is consistent with the risk appetite, i.e., many business propositions require IT risk to be taken to achieve the value proposition and realise enterprise goals and objectives, and this risk should be managed but not necessarily avoided.

When risk is referenced in *COBIT 5 for Risk*, it is the **current** risk. The concept of inherent risk is rarely used in *COBIT 5 for Risk*. **Figure 7** shows how inherent, current and residual risk interrelate. Theoretically, *COBIT 5 for Risk* focuses on current risk because, in practice, that is what is used.

Figure 7—Interrelationship of Inherent, Current and Residual Risk