

COBIT[®]



for Risk

COBIT[®] 
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

© 2013 ISACA. All rights reserved. For usage guidelines, see www.isaca.org/COBITuse.

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

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, Voqualis 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	7
Executive Summary	9
Introduction	9
Terminology	9
Drivers for Risk Management.....	9
Benefits of Using This Publication.....	10
Target Audience for This Publication	10
Overview and Guidance on Use of This Publication	11
Prerequisite Knowledge	13
Section 1. Risk and Risk Management	15
Chapter 1. The Governance Objective: Value Creation	15
Chapter 2. Risk	17
Chapter 3. Scope of This Publication	19
3.1 Perspectives on Risk With COBIT 5	19
3.2 Scope of COBIT 5 for Risk	20
Chapter 4. Applying the COBIT 5 Principles to Managing Risk	23
4.1 Meeting Stakeholder Needs.....	23
4.2 Covering the Enterprise End-to-end	24
4.3 Applying a Single Integrated Framework.....	24
4.4 Enabling a Holistic Approach.....	24
4.5 Separating Governance From Management	25
Section 2A. The Risk Function Perspective	27
Chapter 1. Introduction to Enablers	27
1.1. Introduction.....	27
1.2. Dimensions of the Generic Enabler Model	27
1.3 <i>COBIT 5 for Risk</i> and Enablers.....	28
Chapter 2. Enabler: Principles, Policies and Frameworks	29
2.1 The Principles, Policies and Frameworks Model	29
2.2 Risk Function Perspective: Principles and Policies Related to Risk Governance and Management.....	30
Chapter 3. Enabler: Processes	33
3.1 The Processes Model	33
3.2 Risk Function Perspective: Processes Supporting the Risk Function.....	34
Chapter 4. Enabler: Organisational Structures	37
4.1 The Organisational Structures Model.....	37
4.2 Risk Function Perspective: Risk Governance- and Management-related Organisational Structures	38
Chapter 5. Enabler: Culture, Ethics and Behaviour	41
5.1 The Culture, Ethics and Behaviour Model	41
5.2 Risk Function Perspective: Risk Governance- and Management-related Culture and Behaviour.....	42
Chapter 6. Enabler: Information	45
6.1 The Information Model.....	45
6.2 Risk Function Perspective: Risk Governance- and Management-related Information	47
Chapter 7. Enabler: Services, Infrastructure and Applications	51
7.1 The Services, Infrastructure and Applications Model.....	51
7.2 Risk Function Perspective: Risk Governance- and Management-related Services, Infrastructure and Applications.....	52

Chapter 8. Enabler: People, Skills and Competencies	55
8.1 The People, Skills and Competencies Model	55
8.2 Risk Function Perspective: Risk Governance- and Management-related Skills and Competencies	56
Section 2B. The Risk Management Perspective and Using COBIT 5 Enablers	57
Chapter 1. Core Risk Processes	57
Chapter 2. Risk Scenarios	59
2.1 Introduction	59
2.2 Developing Risk Scenarios Workflow	60
2.3 Risk Factors	60
2.4 IT Risk Scenario Structure	62
2.5 Main Issues When Developing and Using Risk Scenarios	63
Chapter 3. Generic Risk Scenarios	67
Chapter 4. Risk Aggregation	75
4.1 Why Risk Aggregation?	75
4.2 Approach Towards Risk Aggregation	75
Chapter 5. Risk Response	79
5.1 Definitions	79
5.2 Risk Response Workflow and Risk Response Options	79
5.3 Risk Response Selection and Prioritisation	81
5.4 Guidance on Risk Response and Prioritisation	83
Section 3. How This Publication Aligns With Other Standards	85
Chapter 1. COBIT 5 for Risk and ISO 31000	85
1.1 ISO 31000:2009 Risk Management Principles and Guidelines	85
Chapter 2. COBIT 5 for Risk and ISO/IEC 27005	89
2.1 ISO/IEC 27005:2011—Information Technology—Security Techniques—Information Security Risk Management	89
Chapter 3. COBIT 5 for Risk and COSO ERM	93
3.1 COSO ERM—Integrated Framework	93
Chapter 4. Comparison With Risk Market Reference Source	97
4.1 Vocabulary Comparisons: <i>COBIT 5 for Risk</i> vs. ISO Guide 73 and COSO ERM	97
Appendices	
Appendix A. Glossary	103
Appendix B. Detailed Risk Governance and Management Enablers	105
B.1 Enabler: Principles, Policies and Frameworks	105
B.2 Enabler: Processes	109
B.3 Enabler: Organisational Structures	111
B.4 Enabler: Culture, Ethics and Behaviour	117
B.5 Enabler: Information	119
B.6 Enabler: Services, Infrastructure and Applications	159
B.7 Enabler: People, Skills and Competencies	163
Appendix C. Core COBIT 5 Risk Management Processes	165
Appendix D. Using COBIT 5 Enablers to Mitigate IT Risk Scenarios	177
Introduction	177
Appendix E. Comparison of Risk IT With COBIT 5	209
Appendix F. Comprehensive Risk Scenario Template	215

LIST OF FIGURES

Figure 1—COBIT 5 Product Family.....	9
Figure 2— <i>COBIT 5 for Risk</i> Target Audience and Benefits	10
Figure 3— <i>COBIT 5 for Risk</i> Overview	12
Figure 4—The Governance Objective: Value Creation	15
Figure 5—IT Risk Categories	17
Figure 6—Risk Duality	18
Figure 7—Interrelationship of Inherent, Current and Residual Risk.....	18
Figure 8—Two Perspectives on Risk	19
Figure 9—Illustration of Two Perspectives on Risk	20
Figure 10—Scope of <i>COBIT 5 for Risk</i>	21
Figure 11—COBIT 5 Principles	23
Figure 12—COBIT 5 Enterprise Enablers	24
Figure 13—COBIT 5 Enablers: Generic	27
Figure 14—COBIT 5 Enabler: Principles, Policies and Frameworks.....	29
Figure 15—Principles for Risk Management.....	30
Figure 16—Risk Policy Examples	31
Figure 17—COBIT 5 Enabler: Processes.....	33
Figure 18—Supporting Processes for the Risk Function.....	35
Figure 19—Key Supporting Processes for the Risk Function	35
Figure 20—Other Supporting Processes for the Risk Function.....	36
Figure 21—COBIT 5 Enabler: Organisational Structures	37
Figure 22—Key Organisational Structures.....	38
Figure 23—Lines of Defence Against Risk.....	38
Figure 24—Other Relevant Structures for Risk	39
Figure 25—COBIT 5 Enabler: Culture, Ethics and Behaviour.....	41
Figure 26—Relevant Behaviour for Risk Governance and Management.....	42
Figure 27—COBIT 5 Enabler: Information	45
Figure 28—Information Items Supporting Risk Governance and Management.....	48
Figure 29—COBIT 5 Enabler: Services, Infrastructure and Applications	51
Figure 30—Risk-Management-related Services	52
Figure 31—COBIT 5 Enabler: People, Skills and Competencies.....	55
Figure 32—Risk Management Skill Sets and Competencies.....	56
Figure 33—Core Risk Processes.....	57
Figure 34—Risk Scenario Overview	59
Figure 35—Risk Factors.....	61
Figure 36—Risk Scenario Structure	63
Figure 37—Risk Scenario Technique Main Focus Areas	64
Figure 38—Example Risk Scenarios	67
Figure 39—Aggregation of Risk Maps—Disjoint Risk.....	77
Figure 40—Aggregation of Risk Maps—Shared Risk.....	77
Figure 41—Defined Risk Terms	79
Figure 42—Risk Response Workflow.....	80
Figure 43—Risk Response Prioritisation Workflow	82
Figure 44—ISO 31000 Risk Management Principles Covered by <i>COBIT 5 for Risk</i>	85
Figure 45—ISO 31000 Risk Management Framework Covered by <i>COBIT 5 for Risk</i>	86
Figure 46—ISO 31000 Risk Management Processes Covered by <i>COBIT 5 for Risk</i>	87

Figure 47—Information Security Risk Management Process 89

Figure 48—ISO/IEC 27005 Process Steps Covered by *COBIT 5 for Risk*..... 90

Figure 49—COSO ERM Components Covered by *COBIT 5 for Risk* 93

Figure 50—Comparison of ISO Guide 73 With *COBIT 5 for Risk* Definitions..... 97

Figure 51—Comparison of COSO ERM and *COBIT 5 for Risk* Definitions..... 100

Figure 52—Risk Principles 105

Figure 53—Risk Policy Table of Contents Example 105

Figure 54—Validity Aspects to be Identified in a Risk Policy..... 106

Figure 55—Risk Function Key Supporting Processes 109

Figure 56—Enterprise Risk Management (ERM) Committee 111

Figure 57—Enterprise Risk Group 113

Figure 58—Risk Function..... 114

Figure 59—Audit Department 115

Figure 60—Compliance Department..... 116

Figure 61—Risk Profile 119

Figure 62—Template Risk Register Entry 123

Figure 63—Risk Communication Plan..... 124

Figure 64—Risk Report 127

Figure 65—Risk Awareness Programme 129

Figure 66—Risk Map..... 131

Figure 67—Risk Universe, Appetite and Tolerance 133

Figure 68—Risk Capacity, Risk Appetite and Actual Risk..... 135

Figure 69—What Is a Key Risk Indicator?..... 137

Figure 70—Example KRIs..... 141

Figure 71—Emerging Risk Issues and Factors..... 142

Figure 72—Risk Taxonomy 145

Figure 73—Business Impact Analysis 147

Figure 74—Risk Event..... 150

Figure 75—Risk and Control Activity Matrix (RCAM) 153

Figure 76—Risk Assessment 155

Figure 77—Programme/Project Risk Advisory Services..... 159

Figure 78—Incident Management Services 159

Figure 79—Architecture Advisory Services..... 160

Figure 80—Risk Intelligence Services 160

Figure 81—Risk Management Services 160

Figure 82—Crisis Management Services 161

Figure 83—Risk Manager..... 163

Figure 84—Risk Analyst..... 164

Figure 85—Core Risk Management Processes 165

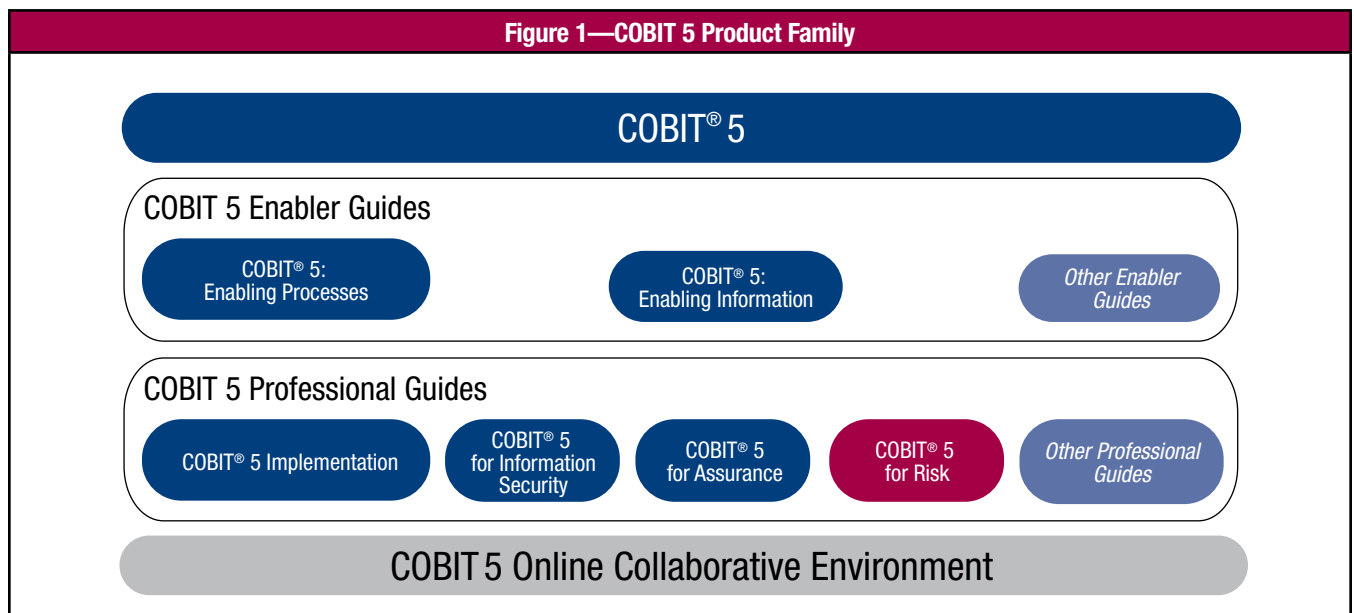
EXECUTIVE SUMMARY

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.



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 <i>COBIT 5 for Risk</i>
Board and executive management	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Linkage of their framework to <i>COBIT 5 for Risk</i> • 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	<ul style="list-style-type: none"> • 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.

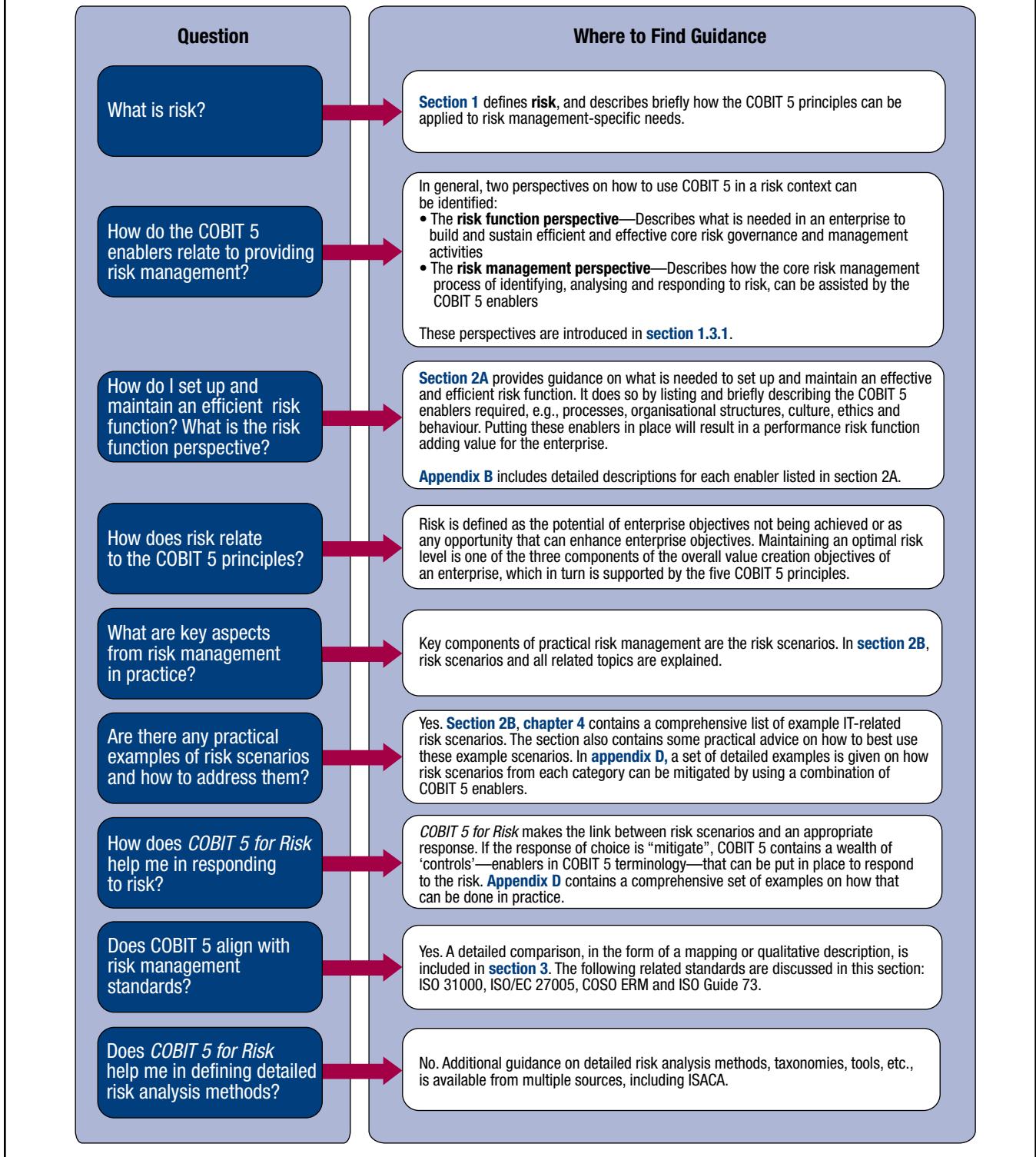
Section 2—Elaborates on using COBIT 5 enablers for risk management in practice. Governance of enterprise IT (GEIT) is systemic and supported by a set of enablers. In this section, the two perspectives on how to apply the COBIT 5 enablers are explained. Detailed guidance regarding these enablers is provided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

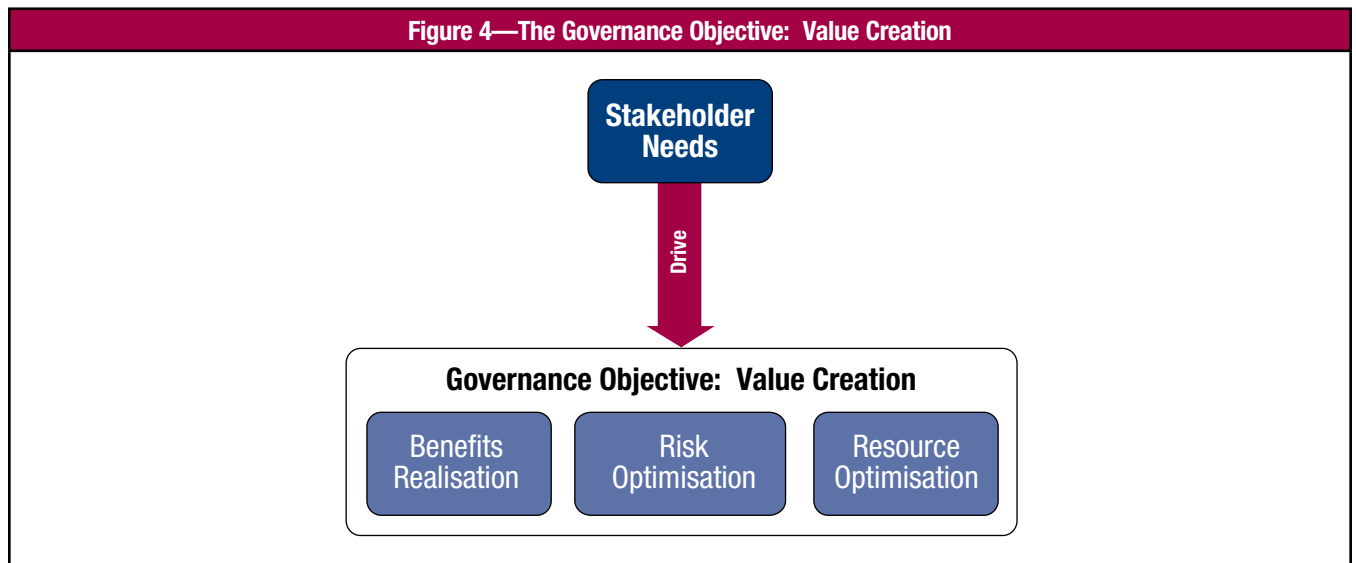
SECTION 1. RISK AND RISK MANAGEMENT

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.



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:

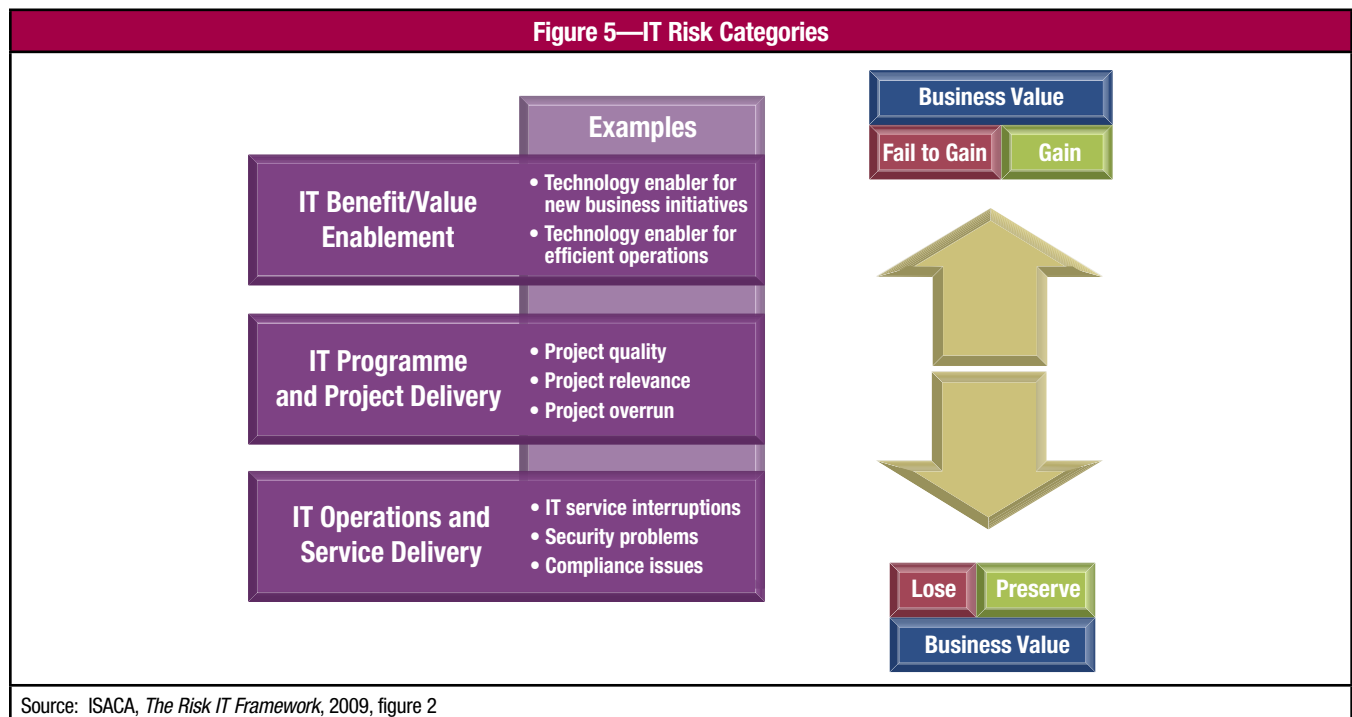
- Risk optimisation is an essential part of any governance system.
- Risk optimisation cannot be seen in isolation, i.e., actions taken as part of risk management will influence benefits realisation and resource optimisation.

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.



IT risk can be categorised as follows:

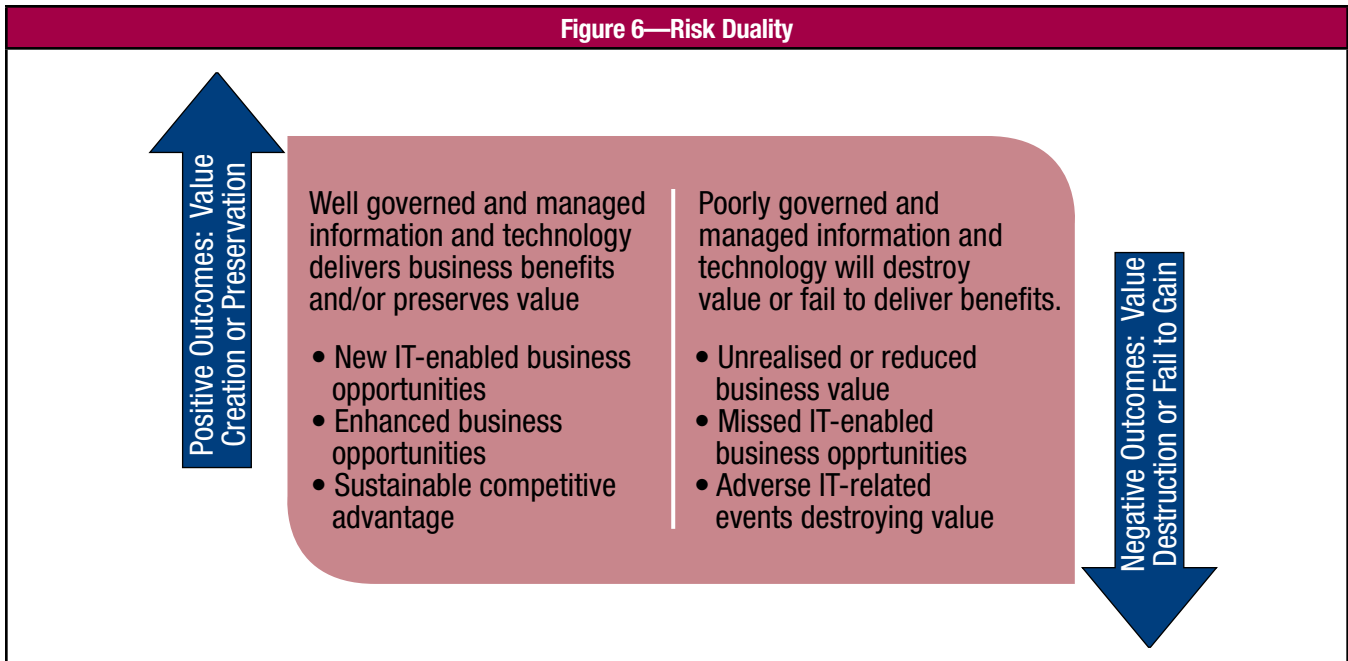
- **IT benefit/value enablement risk**—Associated with missed opportunities to use technology to improve efficiency or effectiveness of business processes or as an enabler for new business initiatives
- **IT programme and project delivery risk**—Associated with the contribution of IT to new or improved 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.



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.

