

THE RISK IT PRACTITIONER GUIDE

Risk Universe, Appetite and Tolerance

Risk Awareness, Communication and Reporting

Expressing and Describing Risk, Risk Scenarios

Risk Responses and Prioritisation
Using COBIT® and Val IT™

***Risk* IT**
BASED ON COBIT®

ISACA®
Serving IT Governance Professionals

ISACA®

With more than 86,000 constituents in more than 160 countries, ISACA (www.isaca.org) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems assurance and security, enterprise governance of IT, and IT-related risk and compliance. Founded in 1969, ISACA sponsors international conferences, publishes the *ISACA® Journal*, and develops international information systems auditing and control standards. It also administers the globally respected Certified Information Systems Auditor™ (CISA®), Certified Information Security Manager® (CISM®), and Certified in the Governance of Enterprise IT® (CGEIT®) designations.

ISACA developed and continually updates the COBIT®, Val IT™ and Risk IT frameworks, which help IT professionals and enterprise leaders fulfil their IT governance responsibilities and deliver value to the business.

Disclaimer

ISACA has designed and created *The Risk IT Practitioner Guide* (the 'Work') primarily as an educational resource for chief information officers (CIOs), senior management and IT management. 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, officers and managers should apply their own professional judgement to the specific control circumstances presented by the particular systems or information technology environment.

Reservation of Rights

© 2009 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorization of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and non-commercial use and for consulting/advisory engagements, and must include full attribution of the material's source. No other right or permission is granted with respect to this work.

ISACA

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

ISBN 978-1-60420-116-1

The Risk IT Practitioner Guide

Printed in the United States of America

CGEIT is a trademark/service mark of ISACA. The mark has been applied for or registered in countries throughout the world.

ACKNOWLEDGEMENTS

ISACA wishes to recognise:**Development Team**

Dirk Steuperaert, CISA, CGEIT, IT In Balance BVBA, Belgium, Chair
 Steven De Haes, Ph.D., University of Antwerp Management School, Belgium
 Gert du Preez, CGEIT, PricewaterhouseCoopers, Belgium
 Rachel Massa, CISSP, PricewaterhouseCoopers LLP, USA
 Bart Peeters, PricewaterhouseCoopers, Belgium
 Steve Reznik, CISA, PricewaterhouseCoopers LLP, USA

IT Risk Task Force (2008-2009)

Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
 Steven Babb, CGEIT, KPMG, UK
 Brian Barnier, CGEIT, ValueBridge Advisors, USA
 Jack Jones, CISA, CISM, CISSP, Risk Management Insight LLC, USA
 John W. Lainhart IV, CISA, CISM, CGEIT, IBM Business Consulting Services, USA
 Gladys Rouissi, CISA, MComp, Commonwealth Bank of Australia, Australia
 Lisa R. Young, CISA, CISSP, Carnegie Mellon University, USA

Expert Reviewers

Mark Adler, CISA, CISM, CGEIT, CFE, CFSA, CIA, CISSP, Commercial Metals, USA
 Steven Babb, CGEIT, KPMG, UK
 Gary Baker, CGEIT, CA, Deloitte & Touche LLP, Canada
 Dave H. Barnett, CISM, CISSP, CSDP, CSSLP, Applied Biosystems, USA
 Brian Barnier, CGEIT, ValueBridge Advisors, USA
 Laurence J. Best, PricewaterhouseCoopers LLP, USA
 Peter R. Bitterli, CISA, CISM, Bitterli Consulting AG, Switzerland
 Luis Blanco, CISA, Citibank, UK
 Adrian Bowles, Ph.D., Sustainability Insights Group (SIG411), USA
 Dirk Bruyndonckx, CISA, CISM, CGEIT, MCA, KPMG Advisory, Belgium
 Olivia Xardel-Burtin, Grand Duchy of Luxembourg
 M. Christophe Burtin, Grand Duchy of Luxembourg
 Rahul Chaurasia, Student, Indian Institute of Information Technology, Allahabad U.P, India
 Richard H. Chew, CISA, CISM, CGEIT, Emerald Management Group, USA
 Philip De Picker, CISA, MCA, Nationale Bank van België, Belgium
 Roger Debreceny, Ph.D., FCPA, University of Hawaii-Manoa, USA
 Heidi L. Erchinger, CISA, CISSP, System Security Solutions Inc., USA
 Robert Fabian, Ph.D., I.S.P., Independent Consultant, Canada
 Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
 Shawna Flanders, CISA, CISM, ACS, PSCU Financial Services, USA
 John Garms, CISM, CISSP, ISSEP, Electric-Tronics Inc., USA
 Dennis Gaughan, AMR Research, USA
 Yalcin Gerek, CISA, CGEIT, TAC, Turkey
 Edson Gin, CISA, CFE, CIPP, SSCP, USA
 Pete Goodhart, PricewaterhouseCoopers LLP, USA
 Gary Hardy, CGEIT, IT Winners, South Africa
 Winston Hayden, ITGS Consultants, South Africa
 Jimmy Heschl, CISA, CISM, CGEIT, KPMG, Austria
 Francisco Igual, CISA, CGEIT, CISSP, SOAPProjects Inc., USA
 Monica Jain, CGEIT, CSQA, CSSBB, USA
 John E. Jasinski, ITIL Service Manager, Six Sigma Black Belt, USA
 Jack Jones, CISA, CISM, CISSP, Risk Management Insight LLC, USA
 Dharmesh Joshi, CISA, CGEIT, CA, CIA, CIBC, CISSP, Canada
 Catherine I. Jourdan, PricewaterhouseCoopers LLP, USA
 Kamal Khan, CISA, CISSP, MBCS, Saudi Aramco, Saudi Arabia
 Marty King, CISA, CGEIT, CPA, BCBSNC, USA
 Terry Kowalyk, Credit Union Deposit Guarantee Corporation, Canada
 Denis Labhart, Swiss Life, Switzerland
 John W. Lainhart IV, CISA, CISM, CGEIT, IBM Business Consulting Services, USA
 Philip Le Grand, Datum International Ltd., UK
 Brian Lind, CISA, CISM, Topdanmark A/S, Denmark
 Bjarne Lonberg, CISSP, A.P. Moller—Maersk, Denmark
 Jo Lusk, CISA, Federal Government, USA
 Charles Mansour, CISA, Charles Mansour Audit & Risk Service, UK
 Mario Micallef, CGEIT, CPAA, FIA, Ganado & Associates, Malta
 John Mitchell, Ph.D., CISA, CGEIT, CFE, FBSC, LHS Business Control, UK
 Jack Musgrove, CGEIT, CMC, BI International, USA

ACKNOWLEDGEMENTS (*cont.*)

Expert Reviewers (*cont.*)

Paul Phillips, Barclays Bank Plc, UK
Andre Pitkowski, CGEIT, OCTAVE, APIT Informatica, Brazil
Felix Ramirez, CISA, CGEIT, Riebeeck Associates, USA
Martin Rosenberg, Ph.D., IT Business Management, UK
Claus Rosenquist, CISA, PBS, Denmark
Gladys Rouissi, CISA, MComp, Commonwealth Bank of Australia, Australia
Daniel L. Ruggles, CISM, CGEIT, CISSP, CMC, PMP, PM Kinetics LLC, USA
Stephen J. Russell, PricewaterhouseCoopers LLP, USA
Deena Lavina Saldanha, CISA, CISM, Obegi Chemicals LLC, UAE
Mark Scherling, Canada
William D. Sewall, CISSP, ISRMC LLC, USA
Gustavo Adolfo Solis Montes, Grupo Cynthus SA de CV, Mexico
John Spangenberg, SeaQuation, The Netherlands
Robert E. Stroud, CGEIT, CA Inc., USA
Jason B. Taule CISM, CGEIT, CDPS, CHSIII, CMC, CPCM, NSA-IAM, General Dynamics Information Technology-Health IT Solutions; USA
John Thorp, CMC, I.S.P., The Thorp Network, Canada
Lance M. Turcato, CISA, CISM, CGEIT, CPA, CITP, City of Phoenix, USA
Kenneth Tyminski, Retired, USA
E.P. van Heijningen, Ph.D., RA, ING Group, The Netherlands
Sylvain Viau, CISA, CGEIT, ISO Lead Auditor, 712iem Escadron de Communication, Canada
Greet Volders, CGEIT, Voquals NV, Belgium
Thomas M. Wagner, Marsh Risk Consulting, Canada
Owen Watkins, ACA, MBCS, Siemens, UK
Clive E. Waugh, CISSP, CEH, Intuit, USA
Amanda Xu, CISA, CISM, Indymac Bank, USA
Lisa R. Young, CISA, CISSP, Carnegie Mellon University, USA

ISACA Board of Directors

Emil D'Angelo, CISA, CISM, Bank of Tokyo Mitsubishi UFJ, USA, International President
George Ataya, CISA, CISM, CGEIT, CISSP, ICT Control SA-NV, Belgium, Vice President
Yonosuke Harada, CISA, CISM, CGEIT, CAIS, InfoCom Research Inc., Japan, Vice President
Ria Lucas, CISA, CGEIT, Telstra Corp. Ltd., Australia, Vice President
Jose Angel Pena Ibarra, CGEIT, Alintec, Mexico, Vice President
Robert E. Stroud, CGEIT, CA Inc., USA, Vice President
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Vice President
Rolf von Roessing, CISA, CISM, CGEIT, KPMG Germany, Germany, Vice President
Lynn Lawton, CISA, FBCS CITP, FCA, FIIA, KPMG LLP, UK, Past International President
Everett C. Johnson Jr., CPA, Deloitte & Touche LLP (retired), USA, Past International President
Gregory T. Grocholski, CISA, The Dow Chemical Company, USA, Director
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Director
Howard Nicholson, CISA, CGEIT, City of Salisbury, Australia, Director
Jeff Spivey, CPP, PSP, Security Risk Management, USA, Trustee

Framework Committee

Patrick Stachtchenko, CISA, CGEIT, CA, Stachtchenko & Associates SAS, France, Chair
George Ataya, CISA, CISM, CGEIT, CISSP, ICT Control SA-NV, Belgium, Vice President
Steven A. Babb, CGEIT, United Kingdom
Sergio Fleginsky, CISA, Akzonobel, Uruguay
John W. Lainhart, IV, CISA, CISM, CGEIT, IBM Global Business Services, USA
Mario C. Micallef, CGEIT, CPAA, FIA, Malta
Derek J. Oliver, CISA, CISM, CFE, FBCS, United Kingdom
Robert G. Parker, CISA, CA, CMC, FCA, Canada
Jo Stewart-Rattray, CISA, CISM, CGEIT, RSM Bird Cameron, Australia
Robert E. Stroud, CGEIT, CA Inc., USA
Rolf M. von Roessing, CISA, CISM, CGEIT, KPMG Germany, Germany

Special Recognition

To the following members of the 2008-2009 IT Governance Committee who initiated the project and steered it to a successful conclusion:

Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Chair
Sushil Chatterji, Edutech Enterprises, Singapore
Kyung-Tae Hwang, CISA, Dongguk University, Korea
John W. Lainhart IV, CISA, CISM, CGEIT, IBM Business Consulting Services, USA
Hugh Penri-Williams, CISA, CISM, CCSA, CIA, Glaniad 1865 Eur, France
Gustavo Adolfo Solis Montes, CISA, CISM, Grupo Cynthus SA de CV, Mexico
Robert E. Stroud, CGEIT, CA Inc., USA
John Thorp, CMC, I.S.P., The Thorp Network Inc., Canada
Wim Van Grembergen, Ph.D., University of Antwerp Management School and IT Alignment and Governance Research Institute, Belgium

TABLE OF CONTENTS

Introduction to the Practitioner Guide 7

 Structure of the Document 7

 The Risk IT Process Model 7

 Risk IT Positioning With Respect to COBIT and Val IT 8

 Overview of the Guide—Mapping Against the Process Model 8

1. Defining a Risk Universe and Scoping Risk Management 11

 Risk Universe 11

 Enterprise IT Risk Assessment 12

 Scoping IT Risk Management 14

2. Risk Appetite and Risk Tolerance 15

 Risk Appetite and Risk Tolerance Defined 15

 Risk Appetite 15

 Risk Tolerance 17

3. Risk Awareness, Communication and Reporting 19

 Introduction 19

 Risk Awareness and Communication 19

 Key Risk Indicators and Risk Reporting 22

 Risk Profile 24

 Risk Aggregation 25

 Risk Culture 29

4. Expressing and Describing Risk 31

 Introduction 31

 Expressing Impact in Business Terms 34

 Describing Risk—Expressing Frequency 37

 Describing Risk—Expressing Impact 38

 COBIT Business Goals Mapping With Other Impact Criteria 42

 Risk Map 46

 Risk Register 47

5. Risk Scenarios 51

 Risk Scenarios Explained 51

 Risk Factors 53

 Example Risk Scenarios 57

 Capability Risk Factors in the Risk Analysis Process 69

 Environmental Risk Factors in the Risk Analysis Process 71

6. Risk Response and Prioritisation 75

 Risk Response Options 75

 Risk Response Selection and Prioritisation 77

7. A Risk Analysis Workflow 81

8. Mitigation of IT Risk Using COBIT and Val IT 83

Appendix 1. Risk Concepts in Risk IT vs. Other Standards and Frameworks 111

 Comparison of Major Features 111

Appendix 2. Risk IT and ISO 31000 113

 ISO 31000 Risk Management—Guidelines on Principles and Implementation of Risk Management 113

Appendix 3. Risk IT and ISO 27005 117

 ISO/IEC 27005:2008, IT—Security Techniques—Information Security Risk Management 117

Appendix 4. Risk IT and COSO ERM 119

 COSO Enterprise Risk Management—Integrated Framework 119

Appendix 5. Vocabulary Comparisons: Risk IT vs. ISO Guide 73 and COSO ERM 123

 Risk IT and ISO Guide 73 on Risk Management Vocabulary 123

 Risk IT and COSO ERM on Risk Management Vocabulary 125

Appendix 6. Risk IT Glossary 129

List of Figures 131

Other ISACA Publications 133

Page intentionally left blank

INTRODUCTION TO THE PRACTITIONER GUIDE

The Risk IT Framework describes a detailed process model for the management of IT-related risk. In this model, multiple references are made to risk analysis, risk profile, responsibilities, key risk indicators (KRIs) and many other risk-related terms.

The Risk IT Practitioner Guide contains practical and more detailed guidance on how to accomplish some of the activities described in the process model.

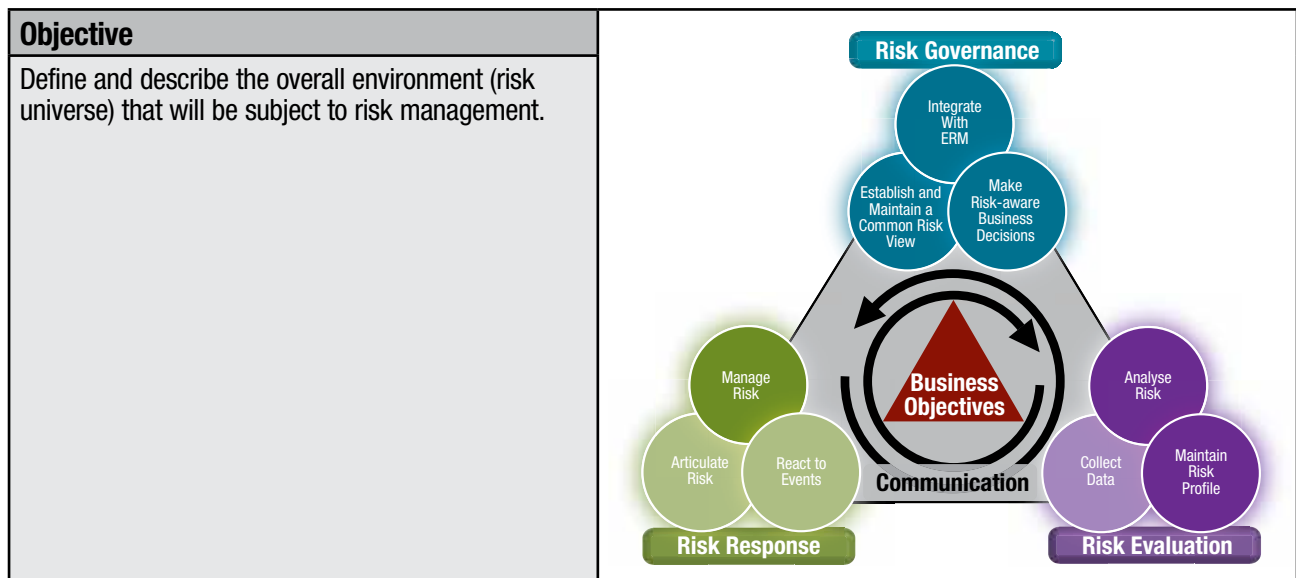
In enterprises wishing to enhance maturity of risk management practices, *The Risk IT Practitioner Guide* can provide a solution accelerator, not in a prescriptive manner but as a solid platform upon which an improved practice can be built. *The Risk IT Practitioner Guide* can be used to assist with setting up an IT risk management framework in the enterprise, as well as to enhance existing IT risk management practices.

This guide does not claim completeness or comprehensiveness, meaning that besides the techniques and practices described here, other viable solutions and techniques exist and may be applied for managing IT risk.

Structure of the Document

This document contains:

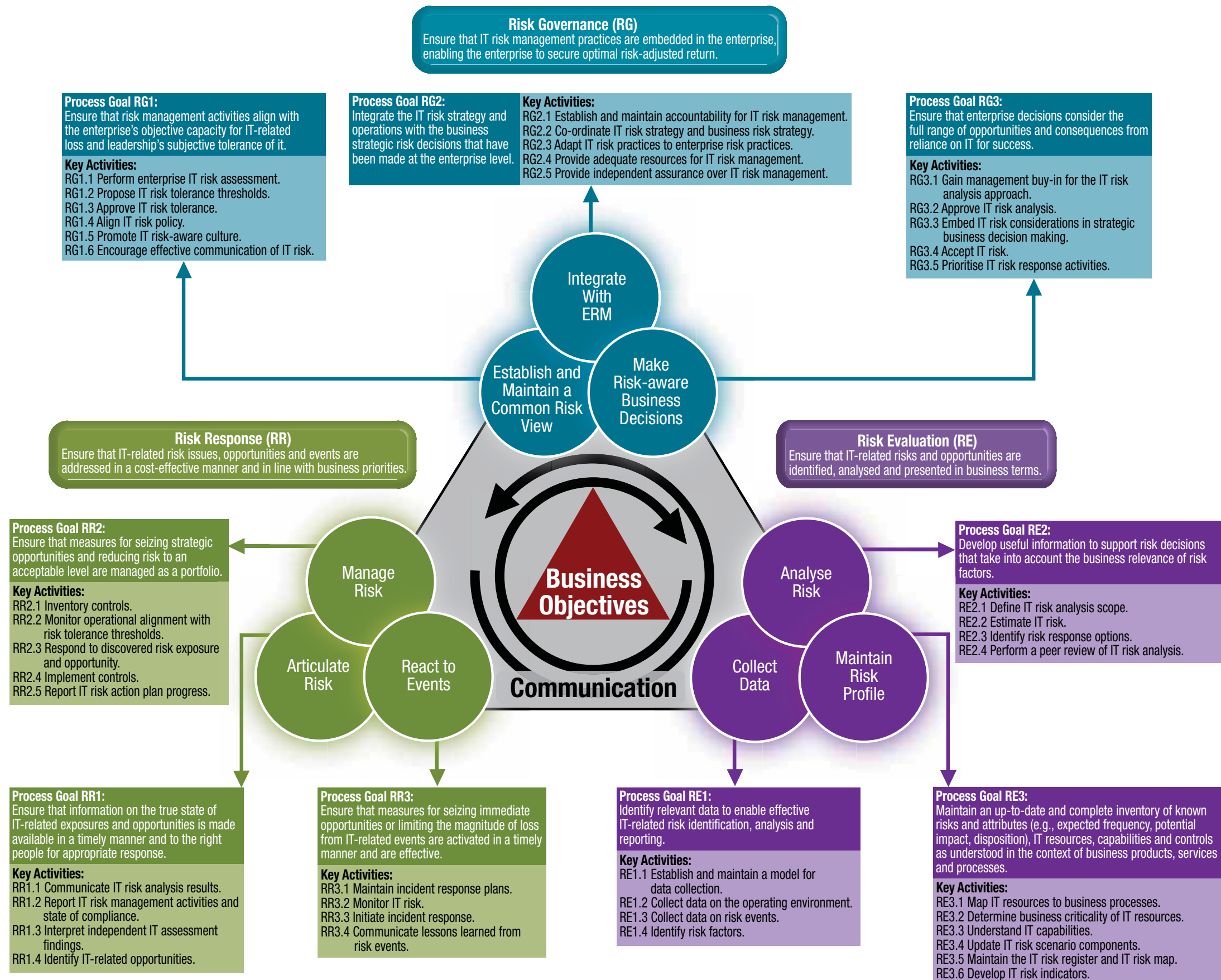
1. An introduction containing a general positioning of the practitioner guide and navigation tools to allow the reader to identify relevant guidance. The positioning with respect to COBIT and Val IT is also briefly discussed.
2. Eight chapters, each of which provides guidance on a particular topic or group of topics. Each chapter has illustrations like the one shown below, where the highlighted sections indicate where in the risk IT process framework the described technique can be applied or where it is relevant.
3. Five appendices, in which the relation between Risk IT and other major (IT) risk management standards and frameworks is discussed.



The Risk IT Process Model

The Risk IT framework is described in full detail in *The Risk IT Framework* publication. For easy reference purposes, **figure 1** contains a graphic overview of the Risk IT process model and its components.

Figure 1—Risk IT Process Model Overview



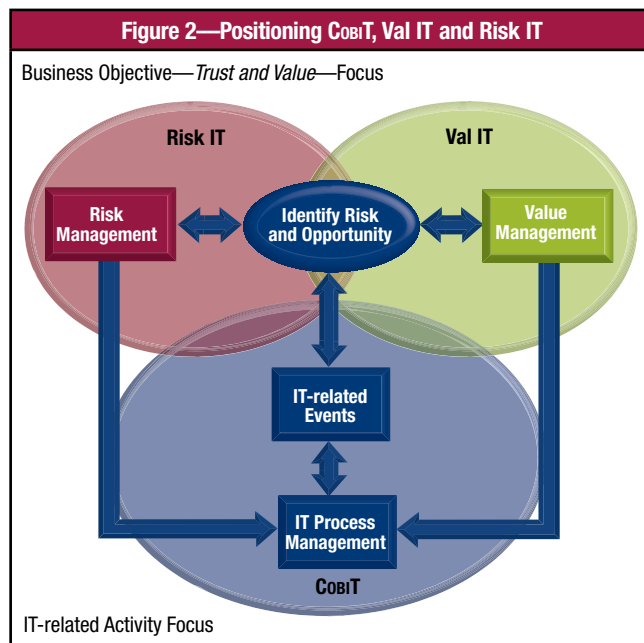
Risk IT Positioning With Respect to CoBIT and Val IT

The *Risk IT Framework* document explains that although Risk IT is a stand-alone risk management framework, it can be used in conjunction with CoBIT and Val IT.

Figure 2 depicts how these three frameworks relate to each other in the context of good IT governance.

The CoBIT processes manage all IT-related activities within the enterprise. These processes deal with events internal or external to the enterprise. Internal events can include operational IT incidents, project failures, full (IT) strategy switches and mergers. External events can include changes in market conditions, new competitors, new technology becoming available and new regulations affecting IT.

These events all pose a risk and/or opportunity and need to be assessed and responses developed. The risk dimension, and how to manage it, is the main subject of the Risk IT framework. When opportunities for IT-enabled business change are identified, the Val IT framework best describes how to progress and maximise the return on investment. The outcome of the assessment will probably have an impact on some of the IT processes and/or on the input to the IT processes; hence, the arrows from 'Risk Management' and 'Value Management' link to the 'IT Process Management' area.



Overview of the Guide—Mapping Against the Process Model

Figure 3 contains an overview of the eight main chapters and select sub-sections of this guide, mapped against the processes of the Risk IT framework. The table identifies the processes to which each section in *The Risk IT Practitioner Guide* applies.

Section	Subsection	Risk IT Framework Domain and Process Reference									
		RG1	RG2	RG3	RE1	RE2	RE3	RR1	RR2	RR3	
1. Defining a Risk Universe and Scoping Risk Management		RG1	RG2	RG3		RE2	RE3		RR2		
2. Risk Appetite and Risk Tolerance		RG1									
3. Risk Awareness, Communication and Reporting	Risk Awareness and Communication	RG1	RG2	RG3	RE1	RE2	RE3	RR1	RR2	RR3	
	Key Risk Indicators and Risk Reporting						RE3	RR1	RR2		
	Risk Profiles						RE3				
	Risk Aggregation	RG1	RG2	RG3				RR1			
	Risk Culture	RG1	RG2								
4. Expressing and Describing Risk	Introduction	RG1	RG2			RE2		RR1			
	Expressing Impact in Business Terms	RG1	RG2			RE2		RR1			
	Describing Risk—Expressing Frequency	RG1				RE2		RR1			
	Describing Risk—Expressing Impact	RG1				RE2		RR1			
	CoBIT Business Goal Mapping With Other Impact Criteria	RG1	RG2								
	Risk Map	RG1					RE3	RR1			
	Risk Register						RE3				
5. Risk Scenarios	Risk Scenarios Explained	RG1				RE2	RE3				
	Example Risk Scenarios					RE2					
	Capability Risk Factors in the Risk Analysis Process	RG1			RE1	RE2	RE3				
	Environmental Risk Factors in the Risk Analysis Process	RG1			RE1	RE2					
6. Risk Response and Prioritisation			RG3					RR2	RR3		
7. A Risk Analysis Workflow				RE1	RE2	RE3	RR1				
8. Mitigation of IT Risk Using CoBIT and Val IT					RE2		RR1	RR2	RR3		

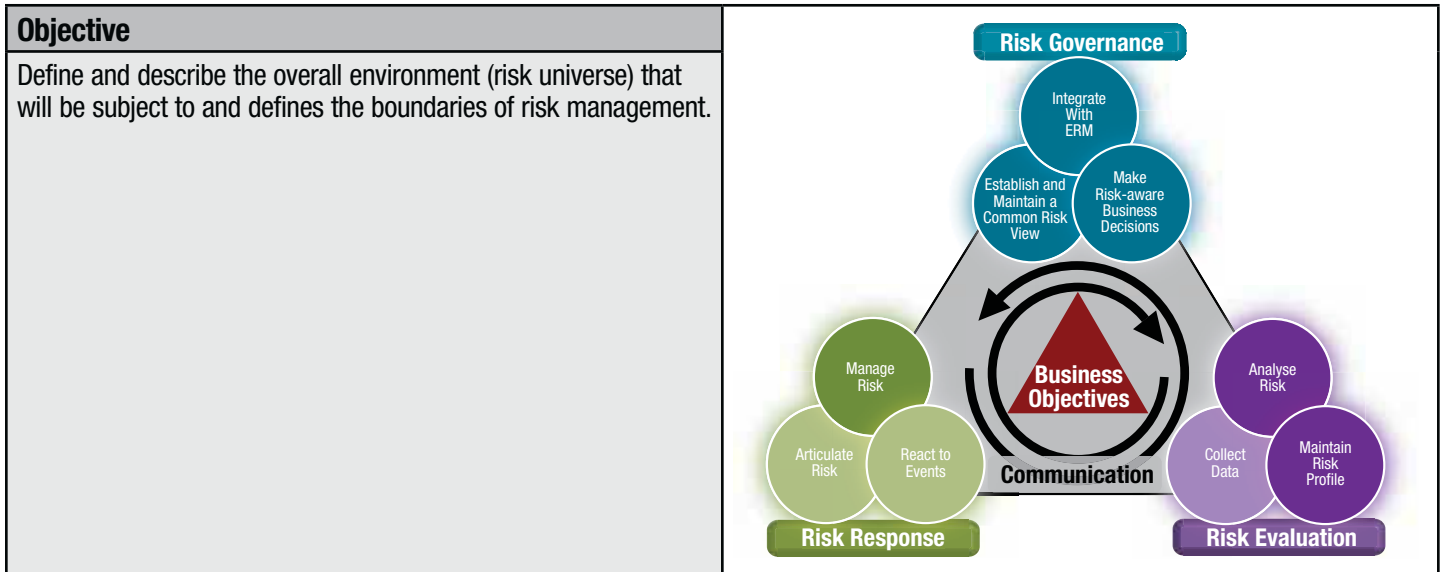
Figure 4 provides a navigation aid between *The Risk IT Framework* and *The Risk IT Practitioner Guide*, but in a different direction—it shows which techniques are applicable to assist which risk management process. Chapters (**bold**) and sub-sections are listed.

Figure 4—Mapping Risk IT Processes With Risk IT Practitioner Guide Chapters																							
Risk IT Framework Domain and Process Reference	1. Defining a Risk Universe and Scoping Risk Management	2. Risk Appetite and Risk Tolerance	3. Risk Awareness, Communication and Reporting—Risk Awareness and Communication	Key Risk Indicators and Risk Reporting	Risk Profile	Risk Aggregation	Risk Culture	4. Expressing and Describing Risk—Introduction	Expressing Impact in Business Terms	Describing Risk—Expressing Frequency	Describing Risk—Expressing Impact	CoaT Business Goals Mapping With Other Impact Criteria	Risk Map	Risk Register	5. Risk Scenarios—Explained	Example Risk Scenarios	Capability Risk Factors in the Risk Analysis Process	Environmental Risk Factors in the Risk Analysis Process	6. Risk Response and Prioritisation	7. A Risk Analysis Workflow	8. Mitigation of IT Risk Using CoaT and Val IT		
RG1 Establish and maintain common risk view																							
RG2 Integrate with ERM																							
RG3 Make risk-aware business decisions																							
RE1 Collect data																							
RE2 Analyse risk																							
RE3 Maintain risk profile																							
RR1 Articulate risk																							
RR2 Manage risk																							
RR3 React to events																							

Page intentionally left blank

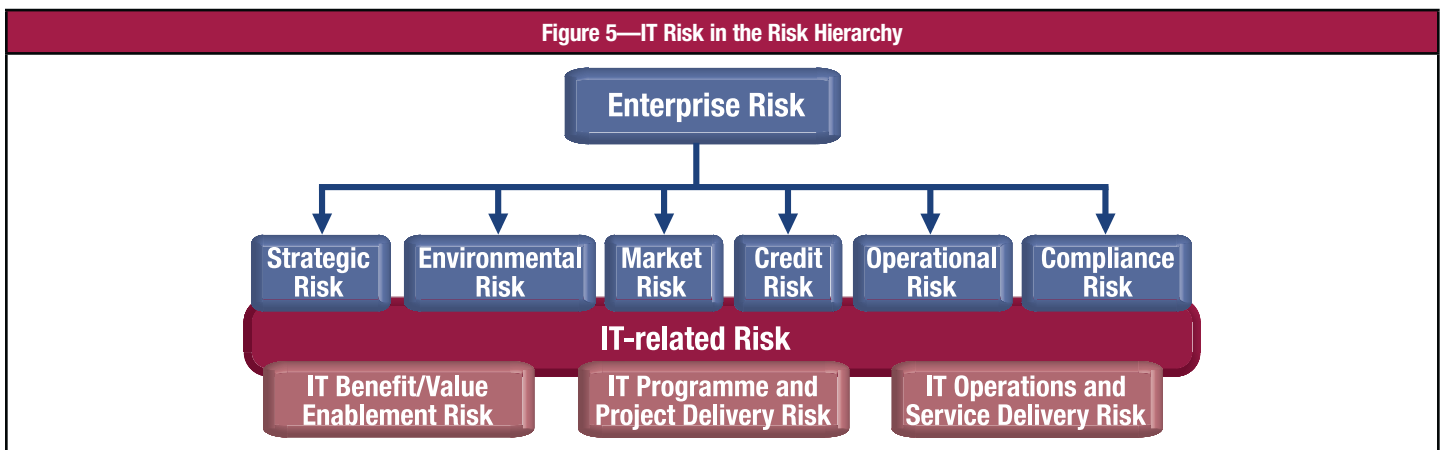
1. DEFINING A RISK UNIVERSE AND SCOPING RISK MANAGEMENT

1. DEFINING A RISK UNIVERSE AND SCOPING RISK MANAGEMENT



Risk Universe

In the definition of IT risk (see *The Risk IT Framework*), IT risk is highlighted as a business risk. IT risk is a component of the overall risk universe of the enterprise, as shown in **figure 5**. Other risks that an enterprise faces include strategic risk, environmental risk, market risk, credit risk, operational risk and compliance risk. In many enterprises, IT-related risk is considered to be a component of operational risk, e.g., in the financial industry in the Basel II framework. However, even strategic risk can have an IT component to it, especially where IT is the key enabler of new business initiatives. The same applies for credit risk, where poor IT (security) can lead to lower credit ratings. For that reason it is better not to depict IT risk with a hierarchic dependency on one of the other risk categories, but perhaps as shown in the (financial industry-oriented) example given in **figure 5**.



IT risk is depicted in its three main categories, as explained in *The Risk IT Framework*, and as shown in **figure 6**.

Managing the IT risk of the enterprise starts with defining the risk universe; a risk universe describes the overall (risk) environment (i.e., defines the boundaries of risk management activities) and provides a structure for managing IT risk. The risk universe:

- Considers the overall business objectives, business processes and their dependencies throughout the enterprise. It describes which IT applications and infrastructure support the business objectives through the provision of IT services. It is worth highlighting that IT risk needs to be seen from an end-to-end business activity perspective, crossing IT function silos (IT operations, project management, application development, disaster recovery, security, etc.).
- Considers the full value chain of the enterprise. This can include not only the enterprise and its subsidiaries/business units, but also clients, suppliers and service providers (the ‘extended’ enterprise).

- Considers a full life-cycle view of IT-related business activities, including transformation programmes, investments, projects and operations
- Includes a logical and workable segmentation of the overall risk environment (e.g., across organisational entities, geographic locations, technologies, applications). This sounds relatively easy but often it is not—the hierarchical organisation of the enterprise, business processes, and supporting IT infrastructure and services often are not aligned, and it is highly probable that different views along different dimensions exist for the overall environment. It is up to the enterprise to determine which view will be the most meaningful to support the business objectives of the enterprise while considering the potential overlaps or omissions.
- Needs to be reviewed and updated on a regular basis due to the constantly changing internal and external environment

Enterprise IT Risk Assessment

Purpose

In the Risk IT process model, a high-level risk assessment is included as part of the Risk Governance (RG) domain. The purpose of this assessment is to obtain an initial view on the overall IT risk with which the enterprise is confronted. In practice, this can be achieved by a high-level assessment of components of the risk universe, e.g., organisational entities.

The enterprise IT risk assessment provides a perspective on the inherent risk of the entity, i.e., an assessment of the IT-related risk without taking into account any detailed risk analysis results and, thus, without fully taking into account existing controls or other risk responses.

The outcome of the risk assessment is used to scope and prioritise more detailed risk management activities. The assessment:

- Allows the identification of the (potential) high-risk areas throughout the enterprise
- Provides an overview of major risk factors to which the enterprise is subject, whether it can influence them or not. These risk factors are important for more detailed risk analyses that follow.
- Provides first indications of major risk scenarios, which is important input to the scenario-building phase of the more detailed risk analysis exercises to be performed at a later stage

The enterprise IT risk assessment needs to be repeated on a regular basis; this can be a simple annual confirmation of earlier results if no major changes occurred in any of the risk factors. If major changes (e.g., mergers, new markets) occur to the enterprise, the assessment needs to be redone. In stable environments, a yearly update or confirmation of the assessment is recommended.

An enterprise IT risk assessment involves all major stakeholders of the enterprise. Stakeholders for risk management are identified in *The Risk IT Framework*, chapter 2. The assessment should be facilitated by an experienced risk management professional to guarantee impartiality and consistency throughout the enterprise.

Sample Enterprise IT Risk Assessment

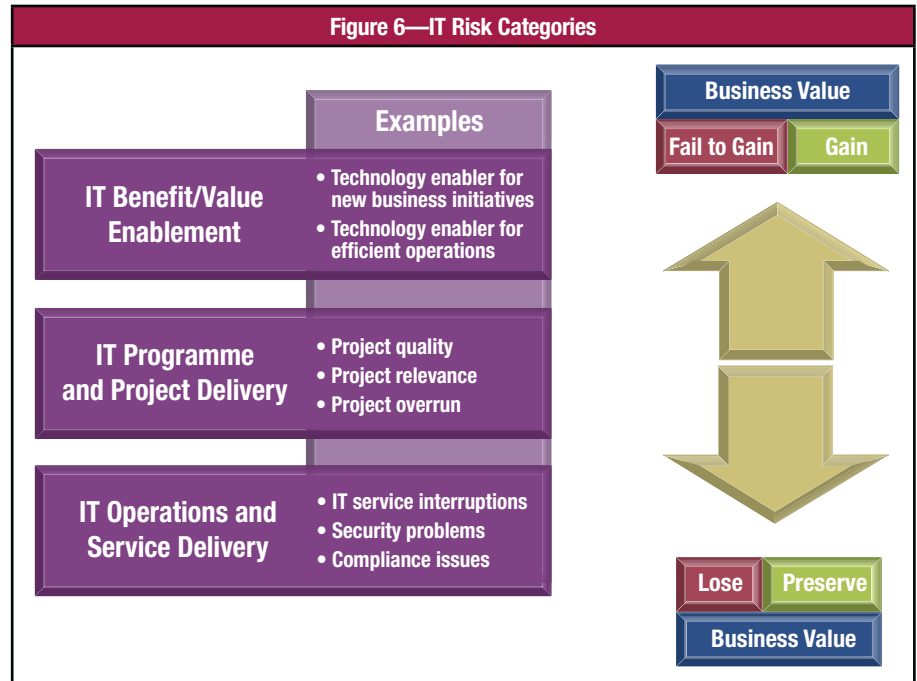
Figure 7 shows a sample high-level risk assessment form, using the risk factors defined in chapter 5, in the Risk Scenarios Explained section. Risk factors co-determine the overall criticality of the entity (or function or process) risk without going into too much detail. They serve as examples and may need to be adapted to be suitable for the enterprise. The high-level analysis provides an initial view of the overall criticality of the enterprise risk, allowing it to prioritise risk management efforts, e.g., to decide where to perform the first thorough risk analysis.

Outcome of Enterprise IT Risk Assessment

Figures 8 and 9 depict a possible outcome of an enterprise IT risk assessment, using a colour code for the overall IT risk ratings obtained. The drawing represents the risk universe as defined by the enterprise, and for each entity, the colour code represents the IT risk rating obtained through the risk assessment.

The same four-rating scale is used in the sample form in figure 7:

- Black—Very High
- Red—High
- Orange—Medium
- Green—Low



1. DEFINING A RISK UNIVERSE AND SCOPING RISK MANAGEMENT

Figure 7—Enterprise IT Risk Assessment Form

Part I—Description				
Entity				
Entity strategic role and objectives				
Assessment date				
Assessor(s)				
Major business processes				
IT infrastructure and applications supporting major business processes				
Important dependencies				
Part II—Risk Factor Assessment				
Risk Factor (Reference)	Assessment	Rating	Comment	
External Environment				
Market				
Rate of change				
Industry/competition				
Geopolitical situation				
Regulatory environment				
Technology status and evolution				
Internal Environment				
Strategic importance of IT for the entity				
Operational importance of IT for the entity				
Complexity of IT				
Complexity of organisation				
Degree of change				
Change management capability				
Risk management philosophy and values				
Risk appetite of the entity				
Operating model				
Risk Management Capability (Risk IT)				
Risk Governance (RG)				
Risk Evaluation (RE)				
Risk Response (RR)				
IT Management Capability (CobIT)				
Plan and Organise (PO)				
Acquire and Implement (AI)				
Deliver and Support (DS)				
Monitor and Evaluate (ME)				
Value Management Capability (Val IT)				
Value Governance (VG)				
Programme Management (PM)				
Investment Management (IM)				
Part III—Conclusion				
Overall high-level IT risk rating (based on results of the assessment of all risk factors below) ¹	Low Entity is marginally dependent on IT and/or IT risk is well controlled	Medium Entity is dependent on IT and/or some IT risks are not well controlled	High Entity is very dependent on IT and/or significant IT risk management deficiencies exist	Very High Entity is critically dependent on IT and/or very significant IT risk management issues exist
Top five risk factors				
Top five IT risk scenarios				

¹ The scales mentioned in the table are examples only; each enterprise should define its own risk ratings.

Scoping IT Risk Management

When the risk universe is constructed, and after an initial enterprise IT risk assessment is completed, scoping of risk management activities can take place. Scoping includes the activities to decide:

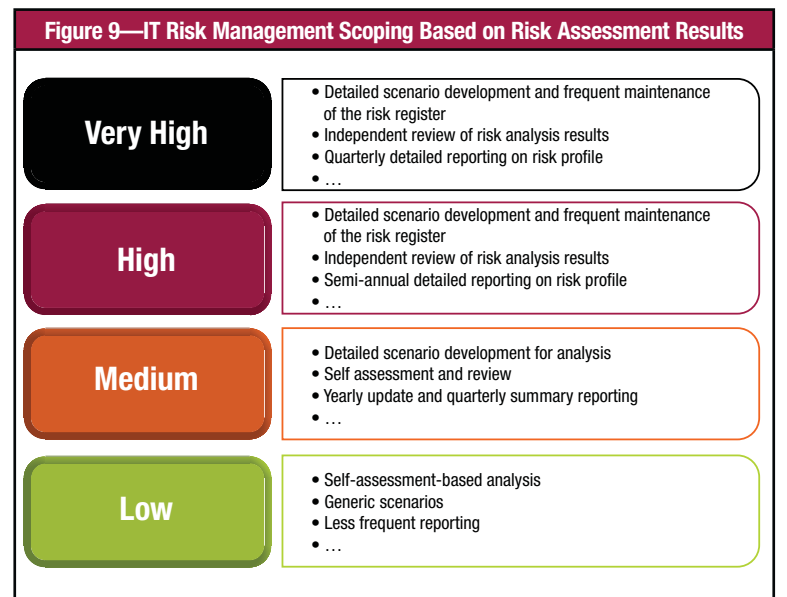
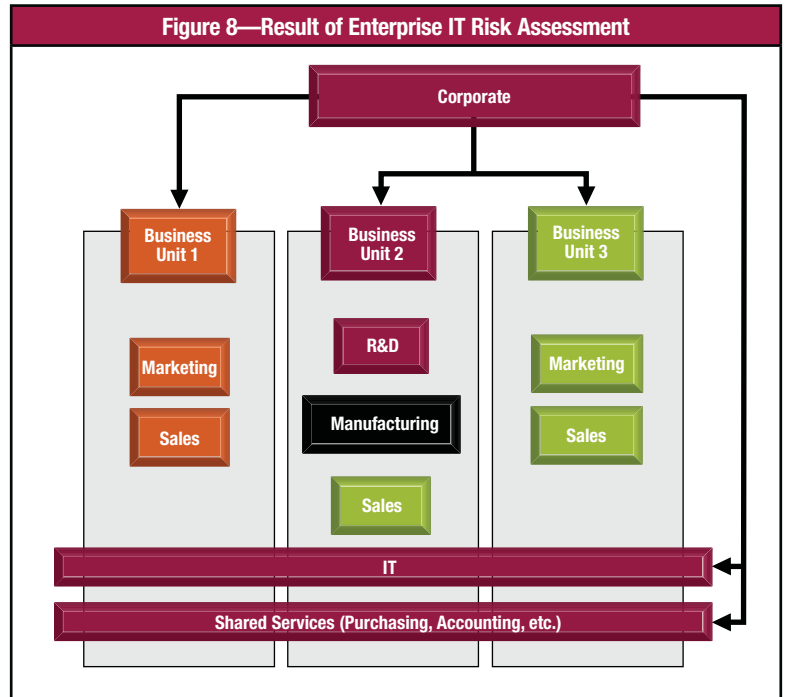
- Which entities in the risk universe will be subject to risk management activities
- The expected breadth and depth of risk management activities, including risk analysis and reporting

Using the four-scale risk assessment categories from the previous section, an enterprise could decide that the following would apply for each of the risk categories:

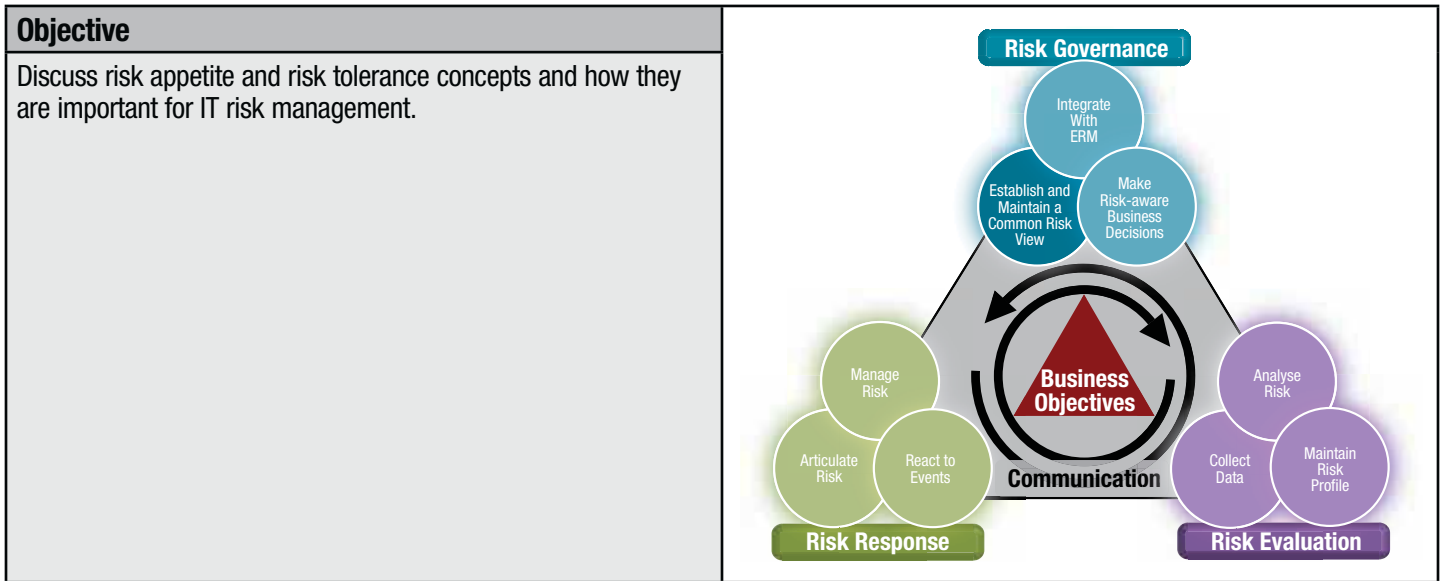
- Self-assessment-based analysis
- Generic scenarios
- Less frequent reporting

An entity in the category of 'high' risk would be required to report every six months on its risk profile, would require some form of independent review of its risk analysis results, and would be required to perform a thorough and detailed risk scenario development and analysis.

This chart is one convenient way to bring together business lines, functional areas and risk importance. This is especially helpful for enterprises struggling to view both business-line and functional perspectives. Yet, enterprises struggle to identify, prioritise and take action for a variety of reasons. Thus, there are a variety of other tools to help visualise risks and take action.



2. RISK APPETITE AND RISK TOLERANCE



Risk Appetite and Risk Tolerance Defined

COSO Definition

Risk appetite and tolerance are concepts that are frequently used, but the potential for misunderstanding is high. Some people use the concepts interchangeably, others see a clear difference. The Risk IT framework definitions are compatible with the COSO ERM definitions² (which are equivalent to the ISO 31000 definition in Guide 73):

- Risk appetite—The broad-based amount of risk a company or other entity is willing to accept in pursuit of its mission (or vision)
- Risk tolerance—The acceptable variation relative to the achievement of an objective (and often is best measured in the same units as those used to measure the related objective)

Risk Appetite and Risk Tolerance in the Risk IT Process Model

Both concepts are introduced in the Risk IT process model, in the key management practices RG1.2, RG1.3 and RG1.4 of process RG1 *Establish and maintain a common risk view*:

- RG1.2 Propose IT risk tolerance thresholds—Establish the amount of IT-related risk a line of business, product, service, process, etc., is willing to take to meet its objectives (risk appetite). Express limits in measures similar to the underlying business objectives and against acceptable and unacceptable business impacts. Consider any trade-offs that may be required to achieve key objectives in context of risk-return balance. Propose limits and measures in the context of IT benefit/value enablement, IT programme and project delivery, and over multiple time horizons (e.g., immediate, short-term, long term).
- RG1.3 Approve IT risk tolerance—Evaluate proposed IT risk tolerance thresholds against the enterprise’s acceptable risk and opportunity levels. Take into account the results of enterprise IT risk assessment and trade-offs required to achieve key objections in the context of risk-return balance). Consider the potential effects of IT risk concentration and correlation across lines of business, product, service and process. Determine whether any unit-specific tolerance thresholds should be applied to all business lines. Define the types of events (internal or external) and changes to business environments or technologies that may necessitate a modification to the IT risk tolerance. Approve IT risk tolerance thresholds.
- RG1.4 Align IT risk policy—Codify IT risk appetite and tolerance into policy at all levels across the enterprise. Recognise that IT risk is inherent to enterprise objectives and document how much IT risk is desired and allowed in pursuit of those objectives. Document risk management principles, risk focus areas and key measurements. Adjust IT risk policy based on changing risk conditions and emerging threats. Align operational policy and standards statements with risk tolerance. Perform periodic or triggered reviews of operational policy and standards against IT risk policy and tolerance. Where there are gaps, set target dates based on acceptable risk exposure time limits and required resources. Where appropriate, propose adjustments to risk tolerance instead of modifying established and effective operational policy and standards.

Risk Appetite

Risk appetite is the amount of risk an enterprise is prepared to accept. When considering the risk appetite levels for the enterprise, two major factors are important:

- The enterprise’s objective capacity to absorb loss, e.g., financial loss, reputation damage
- The (management) culture or predisposition towards risk taking—cautious or aggressive. What is the amount of loss the enterprise wants to accept to pursue a return?

² Committee of Sponsoring Organizations (COSO) of the Treadway Commission, *Enterprise Risk Management —Integrated Framework*, USA, 2004, www.coso.org

Risk appetite can in practice be defined in terms of combinations of frequency and magnitude of a risk. Risk appetite can and will be different amongst enterprises—there is no absolute norm or standard of what constitutes acceptable and unacceptable risk. **Figure 10** illustrates the risk appetite of two distinct enterprises.

Figure 10—Sample Risk Scenarios and Risk Appetite			
	Event	Enterprise A	Enterprise B
A	Event (project delay) with average impact (financial loss > US \$100,000) occurring once in a year	Acceptable	Acceptable
B	Event (project delay) with average impact (financial loss > US \$100,000) occurring 10 times in a year	Unacceptable	Acceptable
C	Event (security incident) with impact on regulatory compliance (small fines) and public embarrassment (press coverage) occurring once in five years	Acceptable	Unacceptable
D	Event (security incident) with impact on regulatory compliance (large fines) and public embarrassment (extended press coverage) occurring 10 times in a year	Unacceptable	Really Unacceptable
E	Condition (IT architecture obsolescence) preventing future rapid growth through new applications	Really Unacceptable	Unacceptable
F	Event (new application [representing significant investment] development failure) delaying new business initiatives for six months and hence failing to gain additional monthly revenue of US \$10 million	Really Unacceptable	Unacceptable
G	Event (new application development failure) delaying new business initiatives for two months and hence failing to gain additional revenue of US \$250,000	Acceptable	Acceptable

Risk maps provide a graphic means to depict risk on a two-dimensional graph, using the dimensions of frequency and magnitude (see chapter 4, for a more detailed discussion). Risk appetite can be defined using the same risk maps—different bands of risk significance can be defined, indicated by coloured bands on the risk map, as shown in **figure 11**.

In the example in **figure 11**, four bands of significance are defined:

- Red—Indicates really unacceptable risk. The enterprise estimates that this level of risk is far beyond its normal risk appetite. Any risk found to be in this band might trigger immediate risk response.
- Yellow—Indicates unacceptable risk, i.e., also above the acceptable risk appetite. The enterprise might, as a matter of policy, require mitigation or another adequate response to be defined within certain time boundaries.
- Green—Indicates normal acceptable level of risk, usually with no special action required, except for maintaining the current controls or other responses
- Blue—Indicates very low risk, where cost-saving opportunities may be found by decreasing the degree of control or where opportunities for assuming more risk might arise

This risk appetite scheme is an example. Every enterprise should define its own risk appetite levels and review them on a regular basis. This definition should be in line with the overall risk culture that the enterprise wants to express, i.e., ranging from very risk averse to risk taking/opportunity seeking. There is no universal right or wrong, but it needs to be defined, well understood and communicated.

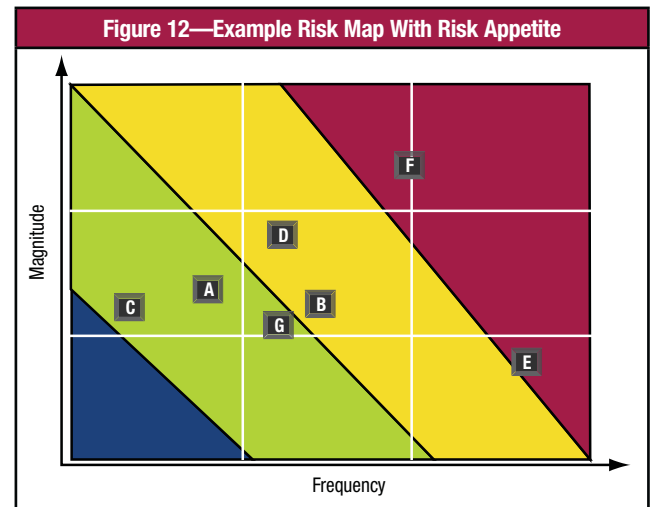
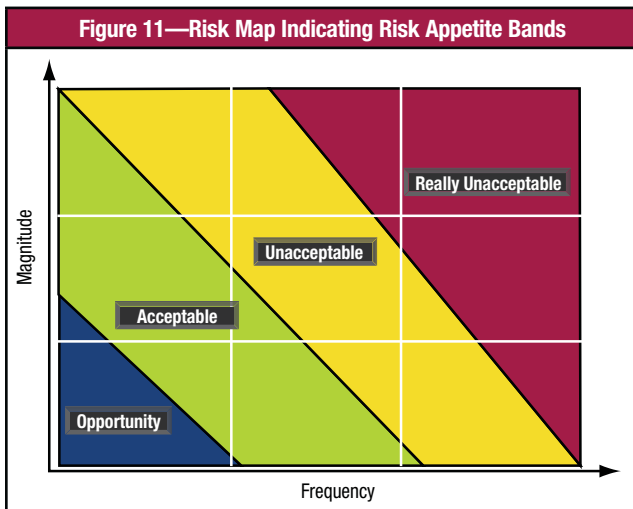
When the example in **figure 10** is plotted on a risk map, as shown in **figure 11**, the result is shown in **figure 12** (the example depicts enterprise A), clearly indicating the major areas of attention for this enterprise.

During a risk analysis, risk scenarios will be assessed (see chapter 5) and plotted on a risk map, such as the one in **figure 12**. Depending on this assessment, an adequate risk response can then be defined (see chapter 6).

Risk appetite is defined by senior management at the enterprise level (process RG1 of the Risk IT process model). There are several benefits associated with defining risk appetite at the enterprise level:

- Supporting and providing evidence of the risk-based decision-making processes, because all risk decisions are based on where the risk resides on the risk map and, hence, all risk response actions can be tracked back and justified
- Supporting the understanding of how each component of the enterprise contributes to the overall risk profile
- Showing how different resource allocation strategies can add to or lessen the burden of risk by simulating different risk response options

2. RISK APPETITE AND RISK TOLERANCE



- Supporting the prioritisation and approval process of risk response actions through risk budgets. A risk budget allows enterprises to trade off: types of risk (time to market vs. reliability) and risk acceptance vs. investment to reduce risk. For example, it is helpful to understand how to use a risk budget to spend on reducing 'known' risks (e.g., operational stability and availability of an ordering infrastructure) to allow acceptance of 'unknown' risks (e.g., new product take-on rates).
- Identifying specific areas where risks should receive a response

Risk appetite is translated into a number of standards and policies, to contain the risk level within the boundaries set by the risk appetite. For example, an enterprise relatively mature in risk management might set the following boundaries for its risk appetite:

- Management of a financial service firm has determined that the main processing platform and applications cannot be unavailable for any period longer than two hours and the system should be able to process yearly transaction growth of 15 percent without performance impact. IT management needs to translate this into specific availability and redundancy requirements for the servers and other infrastructure on which the applications are running. In turn, this leads to:
 - Detailed technical capacity requirements and forecast requirements
 - Specific IT procedures for performance monitoring and capacity planning
- Management has determined that new business initiatives' time-to-market is crucial and IT applications supporting these initiatives cannot be delivered with delays exceeding one month, no exceptions allowed. IT management has to translate this into resource requirements and development process requirements for all development initiatives.

As with the risk universe description and enterprise IT risk assessment (see chapter 1), the risk appetite and the boundaries between bands of significance need to be regularly adjusted or confirmed.

Risk Tolerance

Risk tolerance is the tolerable deviation from the level set by the risk appetite definition. Examples include:

- Standards require projects to be completed within the estimated budgets and time, but overruns of 10 percent of budget or 20 percent of time are tolerated.
- Service levels for system uptime require 99.5 percent availability on a monthly basis; however, isolated cases of 99.4 percent will be tolerated.
- The enterprise is very security risk-averse and does not want to accept any external intrusions; however, single isolated intrusions with limited damage can be tolerated.
- A user profile approval procedure exists, but in some instances, less than full compliance with the procedure can be tolerated.

In the previous examples, risk tolerance is defined using IT process metrics or adherence to defined IT procedures and policies, which in turn are a translation of the IT goals that need to be achieved to support business objectives.

Risk tolerance can also be expressed using the example risk map (see **figure 12**). The enterprise would tolerate a certain risk to be in the red zone for a certain period, provided some justification or approval is given.

Risk appetite and risk tolerance go hand in hand. Risk tolerance is defined at the enterprise level and is reflected in policies set by the executives. At lower (tactical) levels of the enterprise, exceptions can be tolerated (or different thresholds defined) as long as at the enterprise level the overall exposure does not exceed the set risk appetite. Any business initiative includes a risk component, so management should have the discretion to pursue new opportunities up to the level of risk appetite. Enterprises where policies are 'cast in stone' rather than 'lines in the sand' could lack the agility and innovation to exploit new business opportunities. Conversely, there are situations where policies are based on specific legal, regulatory or industry requirements where it is appropriate to have no risk tolerance for failure to comply.

Risk appetite and tolerance should be defined and approved by the board and clearly communicated to all stakeholders. Risk appetite is generally the more static translation on how much risk is acceptable; risk tolerance allows individual and justified exceptions. A process should be in place to review and approve any exceptions.

An enterprise's risk appetite and tolerance change over time; indeed, new technology, new organisational structures, new market conditions, new business strategy and many other factors require the enterprise to reassess its risk portfolio at regular intervals, and also require the enterprise to reconfirm its risk appetite at regular intervals, triggering risk policy reviews. In this respect, an enterprise also needs to understand that the quality of the risk management is directly proportional to the amount of risk that can be taken in pursuit of returns.

The cost of mitigation options can affect risk tolerance. There may be circumstances where the cost/business impact of risk mitigation options exceeds an enterprise's capabilities/resources, thus forcing higher tolerance for one or more risk conditions. For example, if a regulation says that 'sensitive data at rest must be encrypted', yet there is no feasible encryption solution or the cost of implementing a solution would have large negative impact, the enterprise may choose to accept the risk associated with regulatory non-compliance. This would be a risk trade-off.

3. RISK AWARENESS, COMMUNICATION AND REPORTING

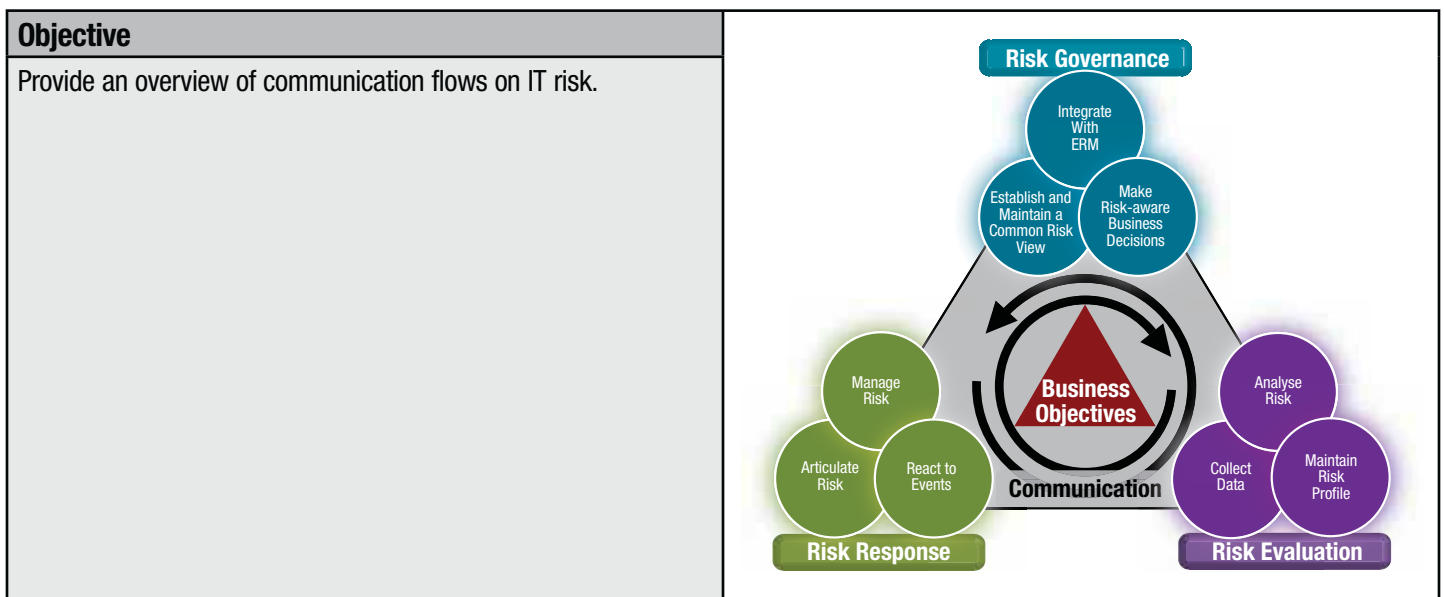
Introduction

This chapter deals with a number of topics related to communication of IT risk. They apply to all processes in the Risk IT framework, because they are related and interlinked.

The chapter discusses the following topics:

- Risk awareness and communication—Describes major types of communication on risk and lists the major information streams on IT risk amongst all stakeholders. To a large extent this section is also included in *The Risk IT Framework* publication because it is a very important aspect of IT risk management.
- Key risk indicators and risk reporting—Discusses the concept of key risk indicators and how they can and should be used for reporting risk
- Risk profiles—Discusses another risk reporting technique, i.e., the risk profile
- Risk aggregation—Discusses reporting of risk throughout the enterprise, from the unit level up to the corporate level
- Risk culture—How behaviour influences risk management

Risk Awareness and Communication



Risk awareness is about acknowledging that risk is an integral part of the business. This does not imply that all risks are to be avoided or eliminated, but rather that they are well understood and known, IT risk issues are identifiable, and the enterprise recognises and uses the means to manage them.

Communication is a key part in this process. Risk communication refers to the idea that people are naturally uncomfortable talking about risk. People tend to put off admitting that risk is involved, and communicating about issues, incidents and eventually even crises.

Awareness and Communication Benefits

The benefits of open communication on IT risk include:

- Contributing to executive management’s understanding of the actual exposure to IT risk, enabling definition of appropriate and informed risk responses
- Awareness amongst all internal stakeholders of the importance of integrating risk and opportunity in their daily duties
- Transparency to external stakeholders regarding the actual level of risk and risk management processes in use

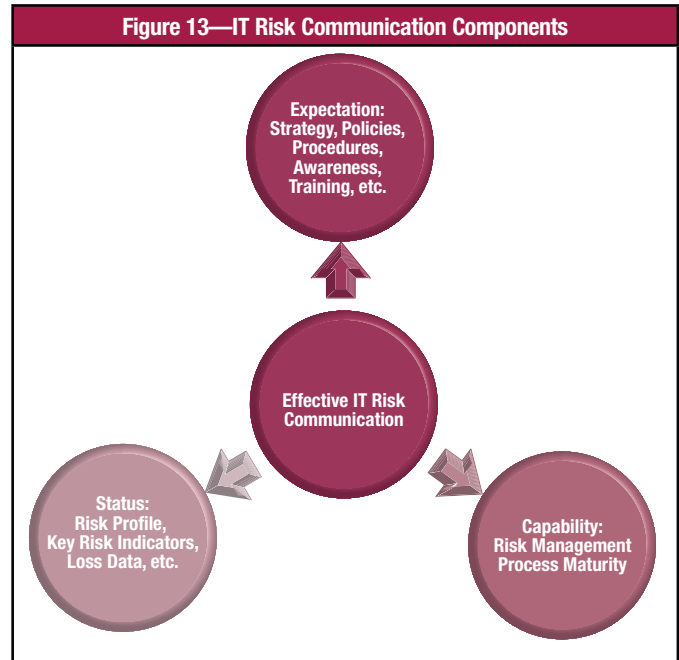
The consequences of poor communication include:

- A false sense of confidence at the top on the degree of actual exposure related to IT, and lack of a well-understood direction for risk management from the top down
- Unbalanced communication to the external world on risk, especially in cases of high but managed risk, may lead to an incorrect perception on actual risks by third parties such as clients, investors, or regulators
- The perception that the enterprise is trying to cover up known risks from stakeholders

Risk Communication—What to Communicate?

IT risk communication covers a broad array of information flows. As shown in **figure 13**, Risk IT distinguishes amongst the following major types of IT risk communication:

- Information on expectations from risk management—This includes risk strategy, policies, procedures, awareness training and continuous reinforcement of principles. This is essential communication on the enterprise overall strategy towards IT risk, and it drives all subsequent efforts on risk management. It sets the overall expectations from risk management.
- Information on current risk management capability—This information allows monitoring of the state of the ‘risk management engine’ in the enterprise, and is a key indicator for good risk management. It has predictive value for how well the enterprise is managing risk and reducing exposure.
- Information on the actual status with regard to IT risk—This includes information such as:
 - Risk profile of the enterprise, i.e., the overall portfolio of (identified) risks to which the enterprise is exposed
 - Event/loss data
 - KRIs to support management reporting on risk
 - Root cause of loss events
 - Options to mitigate (cost and benefits) risks



To be effective, all information exchanged, regardless of its type, should be:

- Clear—Known and understood by all stakeholders
- Concise—Information or communication should not inundate the recipients. All ground rules of good communication apply to communication on risk. This includes the avoidance of jargon and technical terms regarding risk since the intended audiences are generally not deeply technologically skilled.
- Useful—Any communication on risk must be relevant. Technical information that is too detailed and/or is sent to inappropriate parties will hinder, rather than enable, a clear view of risk.
- Timely—For each risk, critical moments exist between its origination and its potential business consequence. For example, a risk may originate when an inadequate IT organisation is set up, and the business consequence is inefficient IT operations and service delivery. In another example, the origination point may be project failure, and the business consequence is delayed business initiatives. Communication is timely when it allows action to be taken at the appropriate moments to identify and treat the risk. It serves no useful purpose to communicate project delay a week before the deadline.
- Aimed at the correct target audience—Information must be communicated at the right level of aggregation, adapted for the audience and enabling informed decisions. In this process, aggregation must not hide root causes of risk. For example, a security officer needs technical IT data on intrusions and viruses to deploy solutions. An IT steering committee may not need this level of detail, but it does need aggregated information to decide on policy changes or additional budgets to treat the same risk.
- Available on a need-to-know basis—IT-risk-related information should be known and communicated to all parties with a genuine need; a risk register with all documented risks is not public information and should be properly protected against internal and external parties with no need for it.

Communication does not always need to be formal, through written reports or messages. Timely face-to-face meetings amongst stakeholders are an important communication means for IT-risk-related information.

Risk Communication—Stakeholders

Figure 14 provides an overview of important communication flows for effective and efficient risk management. It is a summary only and does not represent all communication flows amongst all risk management processes (additional flows are included in the detailed process descriptions of the process framework). The table’s intent is to provide a one-page overview of the main communication flows on IT risk that should exist in one form or another in any enterprise.

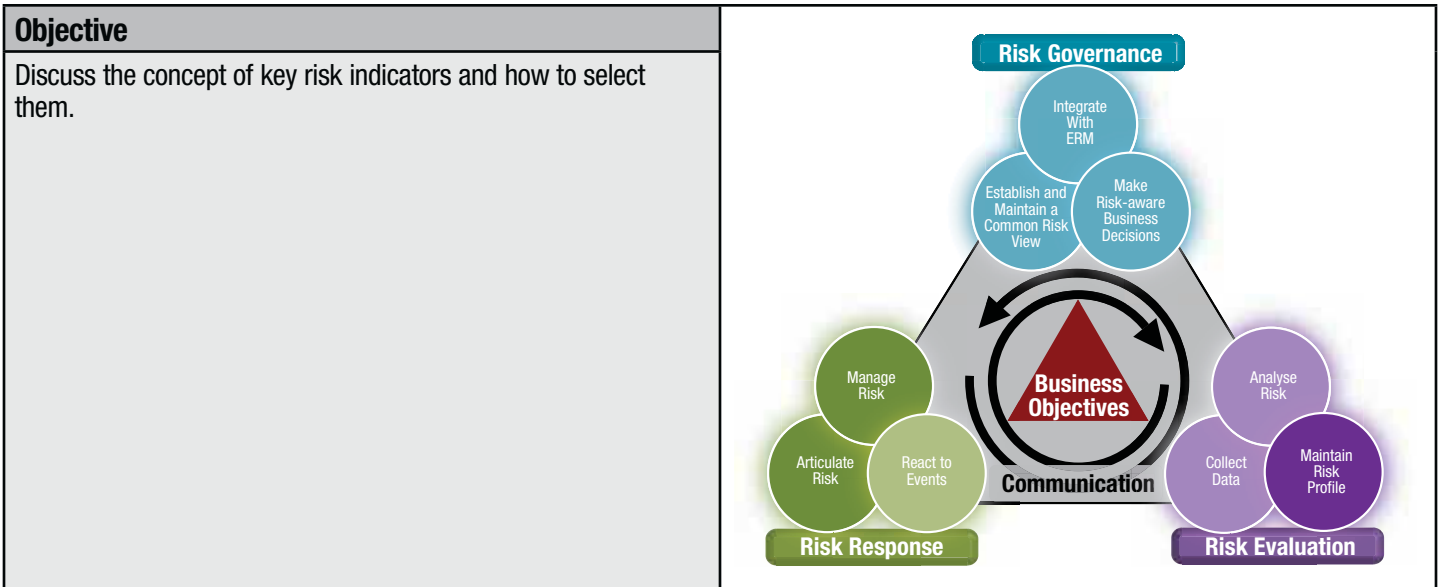
Figure 14 does not include the source and destination of the information nor the actions that should be taken on them; these can be found in the detailed process model.

3. RISK AWARENESS, COMMUNICATION AND REPORTING

Figure 14—Risk Communication Flows

Input	Stakeholders	Output
<ul style="list-style-type: none"> Executive summary IT risk reports Current IT risk exposure/profile KRIs 	Executive management and board	<ul style="list-style-type: none"> Enterprise appetite for IT risk Key performance objectives IT risk RACI charts IT-related policies, expressing management's IT risk tolerance Risk awareness expectations Risk culture Risk analysis request
<ul style="list-style-type: none"> IT risk management scope and plan IT risk register IT risk analysis results Executive summary IT risk reports Integrated/aggregated IT risk report KRIs Risk analysis request 	Chief risk officer (CRO) and enterprise risk committee	<ul style="list-style-type: none"> Enterprise appetite for IT risk Residual IT risk exposures IT risk action plan
<ul style="list-style-type: none"> Enterprise appetite for IT risk IT risk management scope and plan Key performance objectives IT risk RACI charts IT risk assessment methodology IT risk register 	Chief information officer (CIO)	<ul style="list-style-type: none"> Residual IT risk exposures Operational IT risk information Business impact of the IT risk and impacted business units Ongoing changes to risk factors
<ul style="list-style-type: none"> Key performance objectives 	Chief financial officer (CFO)	<ul style="list-style-type: none"> Financial information with regard to IT and IT programmes/projects (budget, actual, trends, etc.)
<ul style="list-style-type: none"> IT risk management scope Plans for ongoing business and IT risk communication Risk culture Business impact of the IT risk and impacted business units Ongoing changes to IT risk factors 	Business management and business process owners	<ul style="list-style-type: none"> Control and compliance monitoring Risk analysis request
<ul style="list-style-type: none"> Key performance objectives IT risk action plan IT risk assessment methodology IT risk register Risk culture 	IT management (including security and service management)	<ul style="list-style-type: none"> IT risk mitigation strategy and plan, including assignment of responsibility and development of metrics
<ul style="list-style-type: none"> Key performance objectives IT risk RACI charts IT risk action plan Control and compliance monitoring 	Compliance and audit	<ul style="list-style-type: none"> Audit findings
<ul style="list-style-type: none"> Key performance objectives IT risk action plan IT risk assessment methodology IT risk register Audit findings 	Risk control functions	<ul style="list-style-type: none"> Residual IT risk exposures IT risk reports
<ul style="list-style-type: none"> Risk awareness expectations Risk culture 	Human resources (HR)	<ul style="list-style-type: none"> Potential IT risk Support on risk awareness initiatives
<ul style="list-style-type: none"> Control and compliance monitoring 	External auditors	<ul style="list-style-type: none"> Audit findings
<ul style="list-style-type: none"> Public opinion, legislation IT risk executive summary report In general, all communications intended for the board and executive management 	Regulators	<ul style="list-style-type: none"> Requirements for controls and reporting Summary findings on risk
<ul style="list-style-type: none"> Executive summary risk reports 	Investors	<ul style="list-style-type: none"> Risk tolerance levels for their portfolio of investments
<ul style="list-style-type: none"> Summary IT risk reports, including residual risk, controls maturity levels and audit findings 	Insurers	<ul style="list-style-type: none"> Insurance coverage (property, business interruption, directors and officers)
<ul style="list-style-type: none"> Risk awareness expectations Risk culture 	All employees	<ul style="list-style-type: none"> Potential IT risk issues

Key Risk Indicators and Risk Reporting



Key Risk Indicators

Risk indicators are metrics capable of showing that the enterprise is subject to, or has a high probability of being subject to, a risk that exceeds the defined risk appetite. They are specific to each enterprise, and their selection depends on a number of parameters in the internal and external environment, such as the size and complexity of the enterprise, whether it is operating in a highly regulated market, and its strategy focus. Identifying risk indicators should take into account the following aspects (amongst others):

- Consider the different stakeholders in the enterprise. Risk indicators should not focus solely on the more operational or the strategic side of risk. They can and should be identified for all stakeholders. Involving the right stakeholders in the selection of risk indicators will also ensure greater buy-in and ownership.
- Make a balanced selection of risk indicators, covering performance indicators (indicating risk after events have occurred), lead indicators (indicating what capabilities are in place to prevent events from occurring) and trends (analysing indicators over time or correlating indicators to gain insights).
- Ensure that the selected indicators drill down to the root cause of the events (indicative of root cause and not just symptoms).

An enterprise may develop an extensive set of metrics to serve as risk indicators; however, it is not possible or feasible to maintain that full set of metrics as key risk indicators (KRIs). KRIs are differentiated as being highly relevant and possessing a high probability of predicting or indicating important risk. Criteria to select KRIs include:

- Impact—Indicators for risks with high business impact are more likely to be KRIs.
- Effort to implement, measure and report—For different indicators that are equivalent in sensitivity, the one that is easier to measure is preferred.
- Reliability—The indicator must possess a high correlation with the risk and be a good predictor or outcome measure.
- Sensitivity—The indicator must be representative for risk and capable of accurately indicating variances in the risk.

To illustrate the difference between reliability and sensitivity in the previous list, an example of a smoke detector can be used. Reliability means that the smoke detector will sound an alarm every time that there is smoke. Sensitivity means that the smoke detector will sound when a certain threshold of smoke density is reached.

The complete set of KRIs should also balance indicators for risks and root causes, as well as business impact.

The selection of the right set of KRIs will have the following benefits to the enterprise:

- Provide an early warning (forward-looking) signal that a high risk is emerging to enable management to take proactive action (before the risk actually becomes a loss)
- Provide a backward-looking view on risk events that have occurred, enabling risk responses and management to be improved
- Enable the documentation and analysis of trends
- Provide an indication of the enterprise's risk appetite and tolerance through metric setting (i.e., KRI thresholds)
- Increase the likelihood of achieving the enterprise's strategic objectives
- Assist in continually optimising the risk governance and management environment

Some of the common challenges encountered in successfully implementing KRIs include:

- KRIs are not linked to specific risks.
- KRIs are often incomplete or inaccurate in specification, i.e., too generic.
- There is a lack of alignment amongst risk, the KRI description and the KRI metric.

3. RISK AWARENESS, COMMUNICATION AND REPORTING

- There are too many KRIs.
- KRIs are difficult to measure.
- It is difficult to aggregate, compare and interpret KRIs in a systematic fashion at an enterprise level.

Since the enterprise’s internal and external environment is constantly changing, the risk environment is also highly dynamic and the set of KRIs needs to be changed over time. Each KRI is related to the risk appetite and tolerance so trigger levels can be defined that will enable stakeholders to take appropriate action in a timely manner.

In addition to indicating risk, KRIs are particularly important during the communication on risk (see previous Risk Awareness and Communication section in this chapter and *The Risk IT Framework*, chapter 5). They facilitate a dialogue on risk within the enterprise, based on clear and measurable facts. This results in a less emotion-based or overly intuitive discussion on where to place priorities for risk management. At the same time, KRIs can be used to improve risk awareness throughout the enterprise, due to the factual nature of these indicators.

The following Risk IT components can serve as KRIs:

- The metrics of the three domains and their processes in the Risk IT process model. They are a combination of:
 - Process indicators and, as such, predictors for risk management capabilities, indicating the successful establishment and operation of the risk management process and environment
 - Outcome measures, indicating risk exposure, measuring actual incidents and related losses
- The process goals and related process metrics defined in the processes of the Risk IT framework
- The maturity model, which gives an indication of the process maturity of the various risk management processes
- Aggregated risk analysis/status results (See the Risk Aggregation section later in this chapter for more details.)

In addition, the COBIT and Val IT frameworks provide a number of very similar metrics (the goal/metrics cascade) on the maturity of IT processes and the different levels of metrics (business process, IT process, activity) designed to measure successful operations and outcome of IT process in support of the business. From these metrics, a selection can be made to indicate the quality of the controls (key management practices) put in place to mitigate risk.

Figure 15 contains an example of some possible KRIs for different stakeholders. Both types of indicators are used (lead and lag indicators). This table is not complete (nor is it intended to be), but it provides readers with some suggestions and inspiration for their own set of key risk indicators.

The stakeholders that are considered here are:

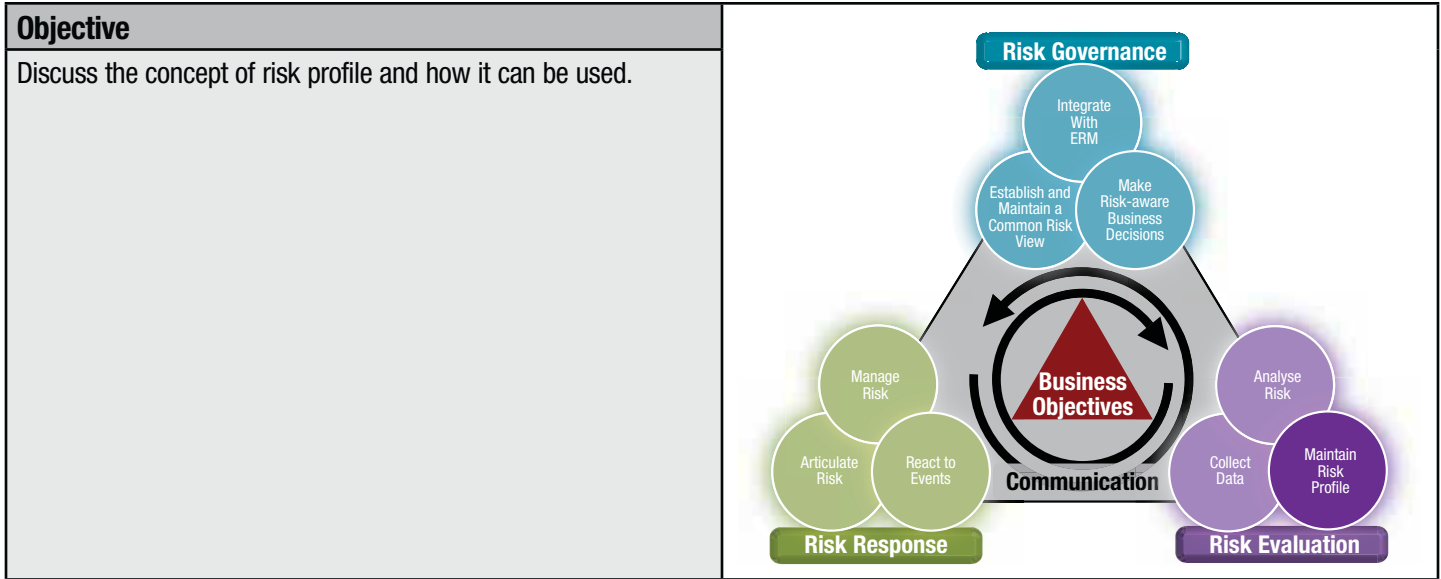
- CIO—This function requires a view on IT risk for the enterprise.
- CRO—The CRO requires a broad view on IT risk from across the business, but can be considered to have a more operational focus.
- Chief Executive Officer (CEO)/Board—These entities require a high-level, aggregated view on risk.

Figure 15—Example Key Risk Indicators

Source ³	Event Category	CIO	CRO	CEO/Board
P03, P05, P010, VG5	Investments/project decision-related events	<ul style="list-style-type: none"> • Percent of projects on time, on budget • Number and type of deviations from technology infrastructure plan 	<ul style="list-style-type: none"> • Percent of IT projects reviewed and signed off on by quality assurance (QA) that meet target quality goals and objectives • Percent of projects with benefit defined up front 	<ul style="list-style-type: none"> • Percent of IT investments exceeding or meeting the predefined business benefit • Percentage of IT expenditures that have direct traceability to the business strategy
P01, VG1	Business-involvement-related events	<ul style="list-style-type: none"> • Degree of approval of business owners of the IT strategic/tactical plans 	<ul style="list-style-type: none"> • Frequency of meetings with enterprise leadership involvement where IT’s contribution to value is discussed 	<ul style="list-style-type: none"> • Frequency of CIO reporting to or attending executive board meetings at which IT’s contribution to enterprise goals is discussed
DS5	Security	<ul style="list-style-type: none"> • Percent of users who do not comply with password standards 	<ul style="list-style-type: none"> • Number and type of suspected and actual access violations 	<ul style="list-style-type: none"> • Number of (security) incidents with business impact
P07, AI4, DS13, ME3	Involuntary staff act (e.g., destruction)	<ul style="list-style-type: none"> • Number of service levels impacted by operational incidents • Percent of IT staff who complete annual IT training plan 	<ul style="list-style-type: none"> • Number of incidents caused by deficient user and operational documentation and training • Number of business-critical processes relying on IT, not covered by IT continuity plan 	<ul style="list-style-type: none"> • Cost of IT non-compliance, including settlements and fines • Number of non-compliance issues reported to the board or causing public comment or embarrassment

³ The source refers to the COBIT and Val IT process references.

Risk Profile



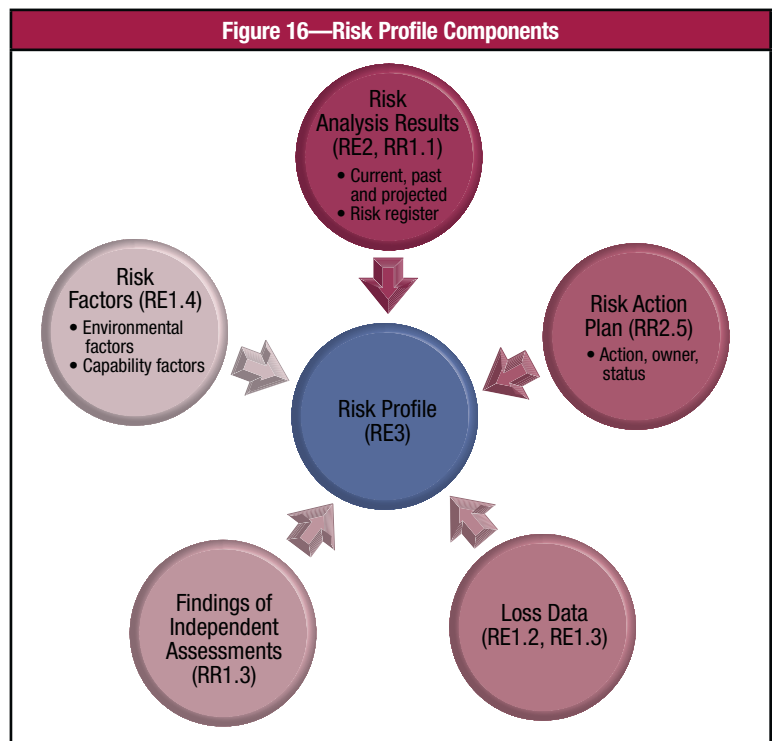
A risk profile is a description of the overall (identified) risks to which the enterprise is exposed. A risk profile is a quick description of the actual risk status of an entity and is useful for reporting purposes, e.g., as part of a risk dashboard at the entity or enterprise level. The risk profile draws upon underlying data, such as risk register, risk analysis results and performance indicators. By consequence, the risk profile also relies on the quality of these underlying data and the processes used to obtain them.

Some important aspects to consider in relation to the risk profile:

- A risk profile is very similar to the aggregated IT risk for the enterprise: both provide a complete and coherent view on all IT risk for the enterprise. The risk profile is created and maintained through ongoing risk analysis.
- A risk profile needs to be defined and maintained, using the already described techniques for expressing risk in business terms and using consistent and similar processes for risk analysis throughout the enterprise. It needs to be updated (very) regularly. The update frequency depends on the overall environment but should be at least on an annual basis and with any significant external or internal environment change.
- A risk profile contains, in addition to the risk map, information on historic loss data and KRIs.

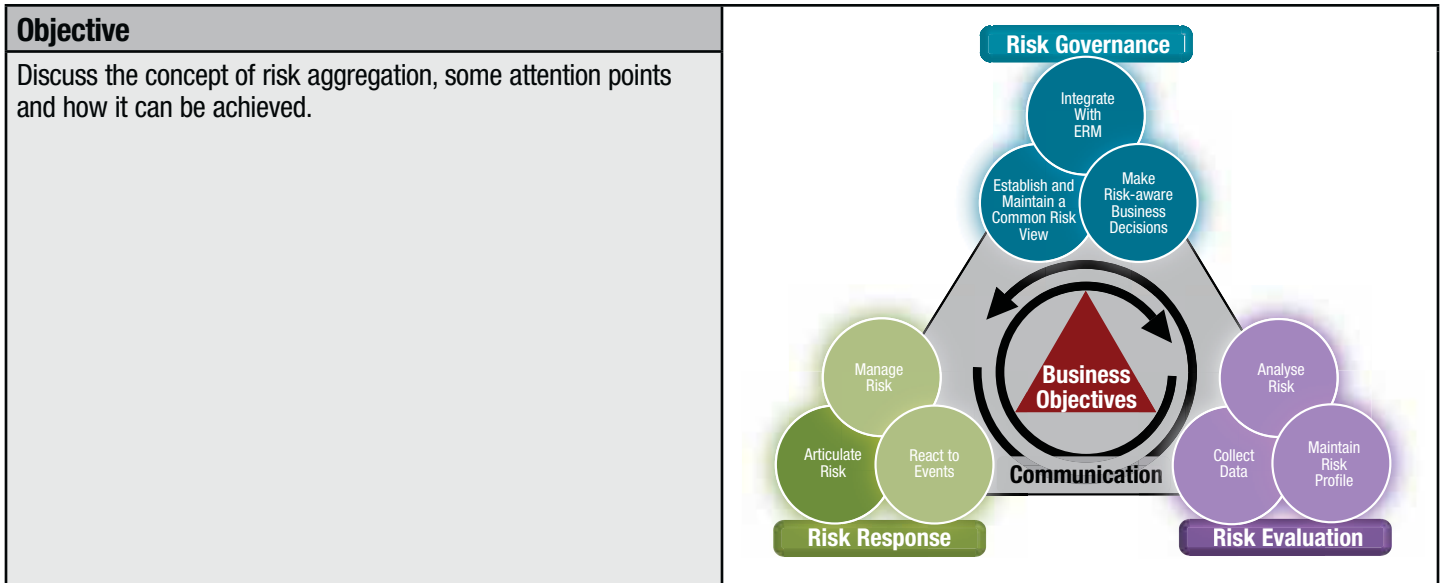
Suggested contents for a risk profile would include at least the following components, based on its definition and as shown in **figure 16**:

- Overview of risk factors, including both environmental risk factors and capability-related risk factors (vulnerabilities), as explained in detail in chapter 5, in the Risk Scenarios Explained section
- Results of the latest enterprise risk assessment and risk analysis, as reflected in the most current risk map (or equivalent representation or description) and in the risk register
- Recent (historical) loss data, providing insight on past risk and allowing the current risk map of assessed risk to be put into perspective
- KRIs, providing insight and overview on the actual level of exposure to risk and the frequency that risk will materialise
- Recent audit findings related to IT risk, providing additional information (and potentially duplicate information) on current risk management capability and IT management capability



3. RISK AWARENESS, COMMUNICATION AND REPORTING

Risk Aggregation



Why Risk Aggregation?

IT risk management can reach its full potential only if IT risk is managed throughout the entire enterprise. It is less valuable when only a partial view of IT risk is obtained. A partial view has two aspects in this context:

- Only part of potential IT risks are considered during risk analysis and risk management.
- Only part of the enterprise is within scope of risk management, i.e., the entire enterprise is not considered.

Every enterprise needs an end-to-end (business activity) view of IT risk, beyond the technical issues, to prevent a false sense of security or a false sense of urgency. This end-to-end business activity view is also what is seen in the real world of producing and selling various goods and services. For that reason an **aggregated** or summarised view of IT risk is required. An aggregated IT risk view allows proper review of risk tolerance, instead of having only silo views of individual or partial risks. For example, a change management problem on an enterprise risk planning (ERP) system could have far-reaching consequences across multiple business lines, countries, partners and customers. Executive management needs to see the aggregated impact of this risk to the entire enterprise, not view it as just a risk on one server in one data centre in one location.

In practice, some obstacles prevent effectively obtaining a consistent and realistic view of actual risk exposure at the enterprise level:

- Lack of consistent and clear terminology across the enterprise
- Existence of complex enterprises with different (sub-)cultures, making it difficult to contain and define the different entities where risk needs to be described, and making it difficult to obtain coherent, reliable and consistent data on risk, even the absolute minimum requirement of a high-level risk assessment
- Presence of qualitative data (and absence of quantitative data) in most cases, with limited reliance on the reliability of the reported risk levels, or with different and/or incompatible scales used for assessing frequency and impact
- Existence of unknown dependencies between reported risks, which can hide bigger risks, e.g., different entities all reporting the same, medium-level risk, which could turn out to be a major risk for the entire enterprise if it occurs
- The use of ordinal scales for expressing risk in different categories, and the mathematical difficulties or dangers of using these numbers to do any sort of calculation
- In complex enterprises, a particular risk at the entity level being important for the entity itself, but for various reasons (e.g., size, enterprise strategy) less important at the enterprise level. This scaling of risk needs to be well understood when aggregating risk information.
- Use by different stakeholders (such as operational risk groups, internal audit, technology risk management, governance, business process improvement [BPI], project management office [PMO], enterprise architecture [EA], quality control [QC]) in large and complex enterprises of different methodologies/frameworks to understand, measure and respond to risk. This prevents an effective aggregation of risk.
- Immaturity of the enterprise in terms of process management, leading to failure to measure process performance and process outcomes, hence an inability to have an accurate view of risk factors
- Failure to understand gaps in ability to detect an event and respond to it

Approach Towards Risk Aggregation

There are different ways to perform risk aggregation. Some guidance in this respect:

- Ensure that there is a uniform, consistent, agreed-upon and communicated method for assessing frequency and magnitude of risk scenarios (see chapter 4). The same method should be used to present aggregated risk; using the same taxonomy for describing risk allows one to aggregate and report on varying types of IT risk, such as, value-creation-related risks, project delivery risks, operational IT risks, because they are all expressed in terms of business impact using the same metrics.

- Be cautious with the mathematics, and aggregate only data and numbers that are meaningful. Do not aggregate data of different natures, e.g., on status of controls or operational IT metrics. Although these are good risk indicators (see chapter 3, Key Risk Indicators and Risk Reporting section), they are meaningless as long as they are not associated with an ultimate business impact. For example, if certain controls are not fully effective or are badly designed, this constitutes no risk in itself. Only when the risk scenarios that rely on these controls are unacceptable because of the failing controls is there an issue. Hence, the information on failing controls is not a reliable metric on its own.
- Focus on real risk for business activities and their most important indicators, and avoid a focus on calculating things that are easily measurable but less relevant. Refer to chapter 3, Key Risk Indicators and Risk Reporting section, to select good risk indicators. Reporting firewall attacks may be easy to measure, but if up-to-date security measures are in place, these attacks, although probably very frequent, carry little business impact.
- Do not aggregate risk information in such a way that hides actionable detail. Of course, this depends on the 'level of responsibility' of the reporting. Issues that must be addressed by a certain organisational layer must be visible, but may be aggregated (hidden) for the next level of authority because there is no immediate action required at that level. The root cause of risks must be visible to those responsible for managing them. This also requires some attention to the aggregation algorithm that will be used.
- Note that risk aggregation is possible in multiple dimensions, e.g., organisational units, types of risks, business processes. The benefit of risk aggregation in a business process is that it allows understanding of weak links in achieving successful business outcomes. Sometimes multiple views (using a combination of several dimensions) may be needed to satisfy risk management and business needs.
- Aggregate risk at the enterprise level, where it can be considered in combination with all other risks that the enterprise needs to manage (integration with ERM; see process RG2 of the Risk IT process model). Take into account the enterprise structure (geographic split, business units, etc.) to set up a meaningful cascade of risk aggregation without losing sight of important specific risks.
- Take into account dependencies at different levels:
 - First, the dependency between event and ultimate business impact needs to be understood. For example, when a server goes down, which business process might suffer, and how does this translate into financial impact, impact for the customer, etc.? This is part of the initial risk analysis process.
 - Next, there might be dependencies between events that make aggregation more than a mathematical addition. Events can amplify each other, for example:
 - One data centre down could be acceptable; a second data centre down at the same time might be a catastrophe.
 - A security incident followed by an error during security software emergency upgrade because of inadequate change management and configuration management procedures leads to extended recovery times for (critical) services affected.
 - A project developing a new IT architecture, including data models and infrastructure, is significantly delayed, thus delaying several new application development projects that would normally rely on the timely completion of the architecture project.

Figure 17 shows one possible and simple approach for aggregating risk. This approach is valid only when risks are disjointed (independent) between entities. When risks are shared or connected, this approach is not valid and may lead to underestimation of actual risk. In

figure 17:

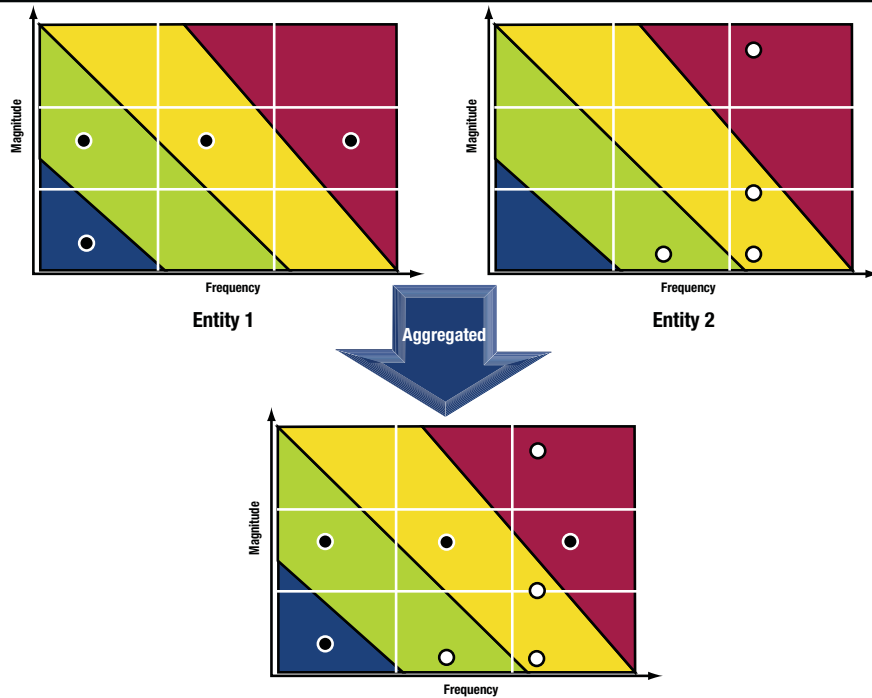
- Two entities create, after due risk analysis, their own risk maps. Note that the Entity 2 has some more severe risk compared to Entity 1.
- The risks on the maps are brought together on one aggregated map; this approach is valid only when all entities use the same metrics and scales in their risk maps.
- The aggregated picture shows a quite even spread of risks throughout the enterprise, allowing proper management response to be defined.

The method to aggregate risks shown in **figure 17** was simply adding them together. Other methods may exist, e.g., each entity shows only its top 10 risks. As mentioned previously, the aggregation method shown must allow sufficient sensitivity, i.e., no major risks or root causes should remain hidden from the appropriate decision makers.

The aggregation approach described previously is valid only when risks in different entities are independent, i.e., when they are not shared and when they do not influence each other. Therefore, a key activity in risk aggregation is to analyse risk analysis results from different entities, verify whether such dependencies exist and, in case they do, adapt the aggregated risk map accordingly.

3. RISK AWARENESS, COMMUNICATION AND REPORTING

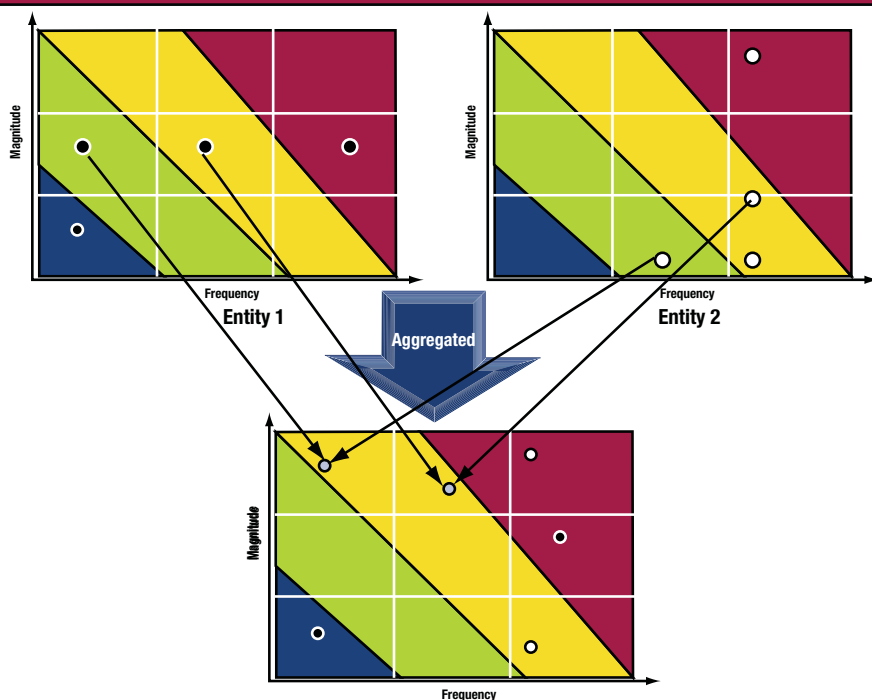
Figure 17—Aggregation of Risk Maps: Disjoint Risks



If, for example, all units were using the same data centre or power grid when this data centre or power grid became unavailable, the entire enterprise would be affected at once. This may be assessed differently (i.e., more seriously) compared to one entity going down for a brief time.

When discussing cascading risk, the magnitude of a joint failure might be increased, but generally, there is less frequency of joint failures. In other words, the probability of two or more elements failing at the same time is usually less than the probability of either one failing. The aggregated risk map may then look as shown in **figure 18**.

Figure 18—Aggregation of Risk Maps: Shared Risks



One benefit of aggregation, certainly in case of dependencies, is that the risk for the overall enterprise becomes highly visible and funds may become available to define an enterprise response to the risk whereas, at the entity level, such a response would not have been feasible or justifiable. Thus, aggregation has allowed the definition and implementation of a cost-efficient response to current risk and residual risk to be reduced within the defined risk appetite levels.

As explained in the previous Risk Profiles section, aggregated risk maps can be part of the risk profile of the enterprise, which itself is part of risk reporting.

3. RISK AWARENESS, COMMUNICATION AND REPORTING

Risk Culture

Objective

Discuss aspects of risk culture and how they affect risk management.



Risk management is about helping enterprises take more risk in pursuit of return. A risk-aware culture characteristically offers a setting in which components of risk are discussed openly, and acceptable levels of risk are understood and maintained. A risk-aware culture begins at the top, with board members who set direction, communicate risk-aware decision making and reward effective risk management behaviours. Risk awareness also implies that all levels within an enterprise are aware of how and why to respond to adverse IT events.

Risk culture is a concept that is not easy to describe. It consists of a series of behaviours, as shown in **figure 19**.

Risk culture includes:

- Behaviour towards taking risk—How much risk does the enterprise feel it can absorb and which risks is it willing to take? This is the risk appetite question, as discussed in chapter 2. As mentioned, there is no absolute good or bad in this respect, but the real risk appetite needs to be clear and communicated.
- Behaviour towards following policy—Once risk appetite is defined (and regularly updated), it has to be translated into policy for the entire enterprise. An element of risk culture is the extent to which people will, or will not, embrace and/or comply with policy.
- Behaviour towards negative outcomes—A third component of risk culture is how the enterprise will deal with negative outcomes, i.e., loss events or missed opportunities. Will it learn from them and try to adjust, or will blame be assigned without treating the root cause?



Some symptoms of an inadequate or problematic risk culture include:

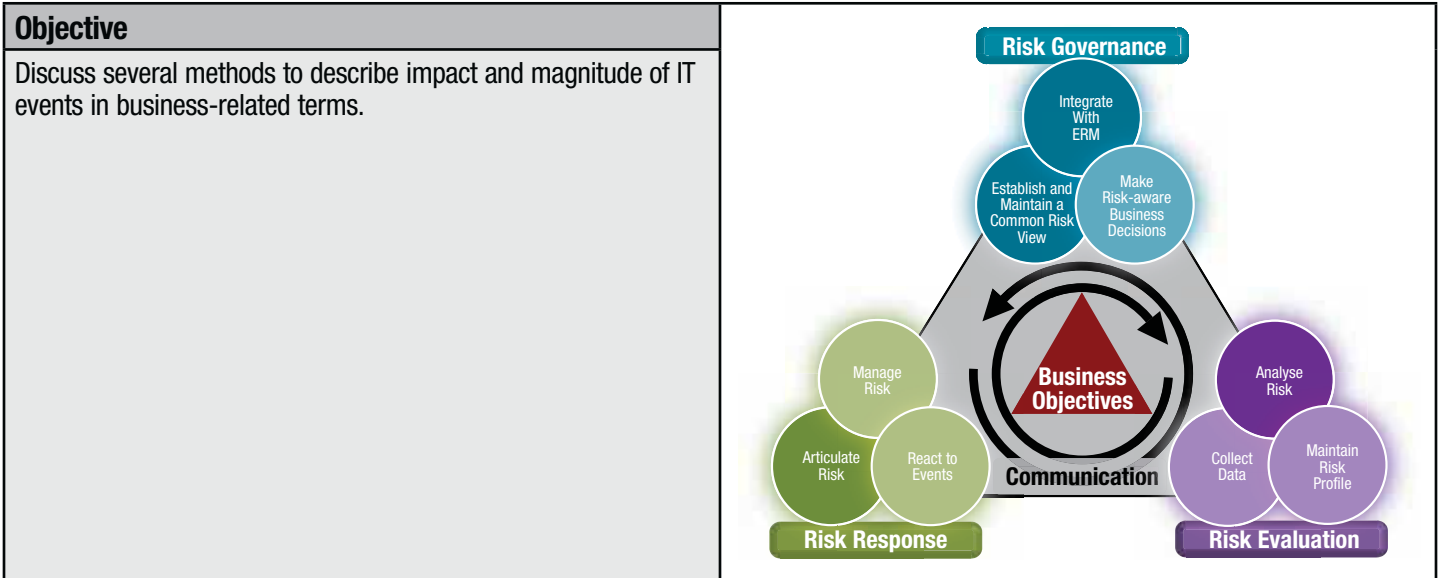
- Misalignment between real risk appetite and translation into policies. Management’s real position towards risk can be reasonably aggressive and risk taking, whereas the policies that are created reflect a much more strict attitude. The resulting behaviour will be mostly non-compliance with policies because management and staff will act in line with the relative high-risk appetite vs. the more strict policies.
- The existence of a ‘blame culture’. This type of culture should by all means be avoided; it is the most effective inhibitor of relevant and efficient communication. In a blame culture, business units tend to point the finger at IT when projects are not delivered on time or do not meet expectations. In doing so, they fail to realise how the business unit’s involvement up front affects project success. In extreme cases, the business unit may assign blame for a failure to meet the expectations that the unit never clearly communicated. The ‘blame game’ only detracts from effective communication across units, further fuelling delays. Executive leadership must identify and quickly control a blame culture if collaboration is to be fostered throughout the enterprise.

Some guidance to diagnose and improve risk culture problems includes those components listed in **figure 20**.

Figure 20—Guidance to Improve Risk Culture Problems	
Guidance Component	Example
Try to derive the real risk appetite from the behaviours and opinions of senior management.	An enterprise adopts an aggressive growth business strategy. As a result, large sums are invested in new IT projects supporting new business models and tapping into new sales channels. The enterprise wants to push for fast delivery and fast time-to-market, and quickly satisfy customer demands. The enterprise also decides to rely on non-redundant technology infrastructure until sufficient funds are generated to make infrastructure more resilient and to strengthen overall IT processes to deal with expected volumes. The flipside of these strategies is the risk that quality and stability may suffer, infrastructure may not be able to withstand any sort of major incident, and security may not be the first priority.
Verify that policies are aligned with the real risk appetite, i.e., they are too strict and, therefore, never will be complied with because management simply does not intend to achieve this level of risk management.	Using the example above, setting policies requiring very strict security procedures, change management procedures, a heavy development process and full business continuity planning (BCP)/disaster recovery planning (DRP) capability would be out of line with the real risk position the enterprise wants to take. Even if, for 'political correctness', such policies would be defined, the only result will be extensive non-compliance (and lots of resulting frustration).
Check for signs of blame culture and, if such a culture exists, initiate actions to change it; these actions start with senior management's reaction to adverse events and with setting the right examples at the highest level of responsibility.	Continuing with the example above, one could imagine that some failures will occur, e.g., projects somewhat late and operational incidents. If management reaction would then be to assign blame, this would not only be in contradiction with its own <i>de facto</i> risk appetite position, but it would also lead to incidents and failures being covered up, resulting in a distorted view of the actual situation with regard to IT risk.

4. EXPRESSING AND DESCRIBING RISK

Introduction



Introduction and Chapter Contents

This chapter addresses a number of issues discussing risk; the presence of a common language throughout the enterprise is key to the success of risk management, and this chapter provides a number of techniques to help develop such a language for IT risk management.

The following are discussed:

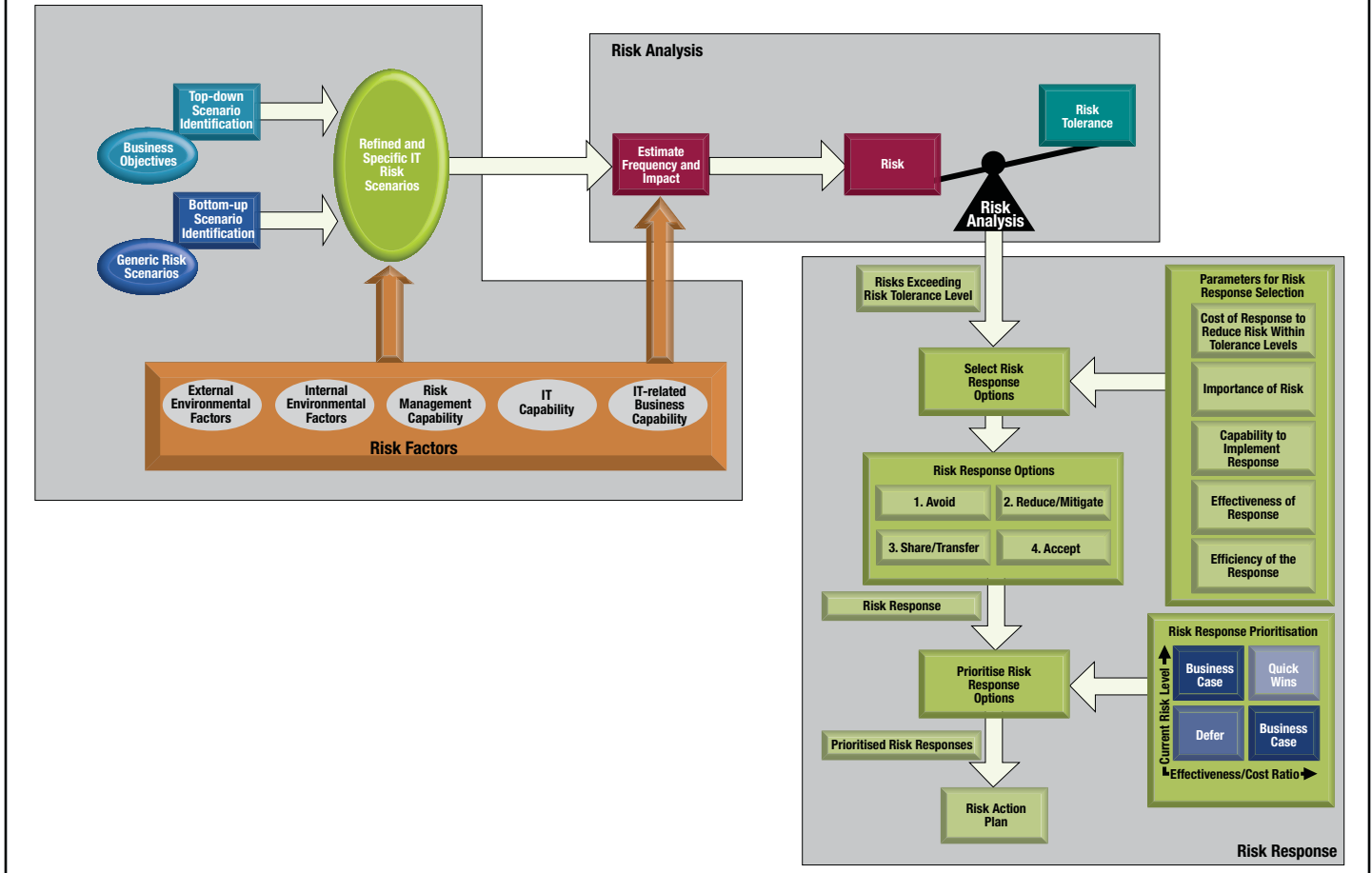
- General introduction to risk analysis, general overview of the risk assessment flow and a brief discussion of risk analysis methods
- Methods to describe the impact of IT risk scenarios in business-relevant terms
- Expressing the frequency of events
- Expressing the impact or magnitude of risk scenarios
- Mapping of COBIT business goals with other impact criteria schemes
- Risk maps as risk analysis reporting tools, discussion of some attention points when using them
- Risk register, using a template for risk register entry

The contents of this chapter are closely related to the contents of chapter 5. Whereas this chapter describes the mechanisms and metrics to conduct risk analyses, chapter 5 describes how to develop risk scenarios to which the risk analyses are applied.

Risk Analysis Overview

The contents of this chapter and chapters 5 and 6 can be summarised by **figure 21**, all components of which are further explained and elaborated on in these chapters.

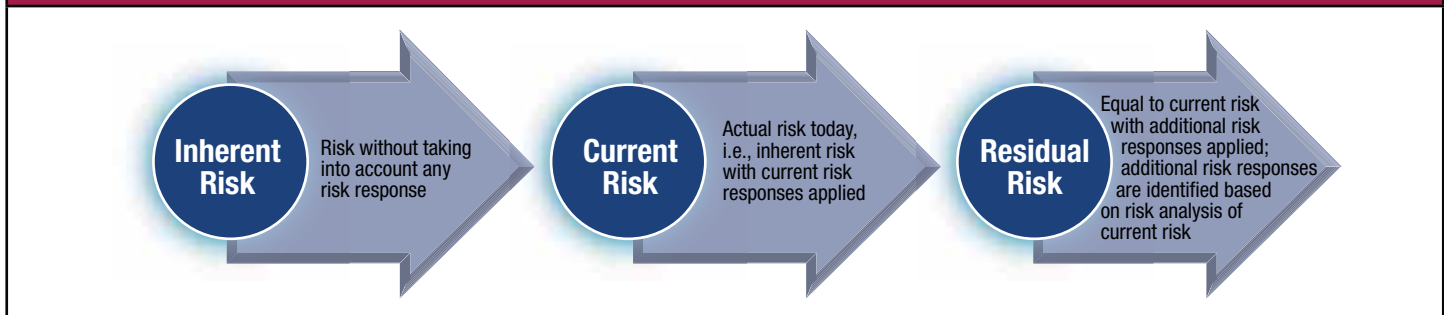
Figure 21—Risk Analysis and Risk Response Overview



In this chapter, well-known terminology about risk management is used. Because not all risk management standards and frameworks use the terminology identically, the following bullets provide a brief overview of some of the terms used in this publication:

- Risk analysis and risk assessment—Risk analysis is the actual estimation of frequency and magnitude/impact of a risk scenario. Risk assessment is a slightly broader term, including the preliminary and ancillary activities around risk analysis, i.e., identification of detailed risk scenarios and definition of risk responses.
- Risk, inherent and residual—When risk is referenced in Risk IT, it is the current risk. The concept of inherent risk is rarely used in Risk IT. **Figure 22** shows how inherent, current and residual risk interrelate.

Figure 22—Inherent Risk, Current Risk and Residual Risk



Risk Analysis Methods—Quantitative vs. Qualitative

As mentioned previously, risk analysis is the process of estimating the two essential properties of each risk scenario:

- Frequency—The number of times in a given period (usually in a year) that an event is likely to occur
- Impact—The business consequence of the scenario

Several methods for risk analysis exist, ranging between high-level and mostly qualitative to very detailed and/or quantitative, with hybrid methods in between. Both forms may be needed at different stages of the risk management process. For example, qualitative tends to be better at the initial risk assessment stage to establish priorities, and quantitative can then provide the required rigour and accuracy for the selected high-risk areas.

The enterprise's culture, resources, skills and knowledge of IT risk management, environment, risk appetite, and its existing approach to ERM will determine which methodology should be used.

The different methods—quantitative and qualitative—have some common limitations:

- No method is fully objective, and results of risk assessments are always dependent on the person performing them and his/her skills and views.
- IT-risk-related data (such as loss data and IT risk factors) are very often of poor quality or quite subjective (e.g., process maturity, control weaknesses). Using structures or models can help to achieve more objectivity and can provide at least a basis for discussion in the risk analysis.
- Quantitative approaches run the risk of creating over-confidence in complex models based on insufficient data. However, over-simplified qualitative or quantitative models can also result in unreliable results.

Qualitative Risk Analysis

A qualitative risk assessment approach uses expert opinions to estimate the frequency and business impact of adverse events. The frequency and the magnitude of impact are estimated using qualitative labels. These labels can vary depending on the circumstances and different environments.

When to Use, Strengths, Limitations, Weaknesses

- In situations where there is only limited or low-quality information available, qualitative risk analysis methods are usually applied.
- The major disadvantages of using the qualitative approach are a high level of subjectivity, great variance in human judgements and lack of standardised approach during the assessment.
- However, qualitative risk assessment is usually less complex than quantitative analysis, and consequently is also less expensive.

Quantitative Risk Analysis

As soon as quantitative values are used (e.g., ranges) to define qualitative values, or when only quantitative values are used, it is a quantitative analysis. The essence of quantitative risk assessment is to derive the frequency and consequences of risk scenarios, based on statistical methods and data.

When to Use, Strengths, Limitations, Weaknesses

- Quantitative risk analysis is more objective because it is based on formal empirical data.
- Using purely quantitative methods requires sufficient, complete and reliable data on past and comparable events. Obtaining these data is in many cases very difficult unless the enterprise has already embraced process improvement and follows an approach such as Six Sigma for IT monitoring and productivity improvement.
- Some things are very hard or impossible to quantify—value of human life, cost of terrorist attacks or similar events, loss of reputation.

Combining Qualitative and Quantitative, Moving Towards Probabilistic Risk Assessment

Both techniques have some advantages and disadvantages. Furthermore, neither of the approaches described previously seems to meet all the requirements for management of IT risk to extensively support the overall ERM processes.

Analysis based on subjective opinions or estimated data⁴ may be insufficient. There is still the question of uncertainty. How certain can one be about the results of risk assessment? Some advanced methods exist to increase reliability of risk assessments, but these require deep statistical skills. They include:

- Probabilistic risk assessment—Using a mathematical model to construct the qualitative risk assessment approach while using the quantitative risk assessment techniques and principles. In a simple way, the statistical models are used and missing data to populate these models are collected using qualitative risk assessment methods (interviews, Delphi method, etc.).
- Monte Carlo simulation—A powerful method for combining qualitative and quantitative approaches, which is based on a normal deterministic simulation model described previously, but iteratively evaluates the model using sets of random numbers as inputs. While deterministic models will provide the expected value, Monte Carlo simulation will give the value as a probability distribution based on the quality of the information provided.

Practical Guidance on Analysing Risk

The selection for qualitative or quantitative risk analysis depends upon many factors:

- User needs—Is there a need for highly accurate data or is a qualitative approach adequate?
- Availability and quality of the data related to IT risk
- Time available for risk analysis
- Level of comfort and expertise of those experts who are giving input

⁴ There is a difference and potential confusion between 'subjective opinions' and 'estimated data'. An opinion is how someone feels about something, e.g., bad, good, acceptable, unacceptable. Those statements are impossible to substantiate or dispute because they are in the eye of the beholder. An estimate is what a person believes is true given the information he/she has. Estimates can be substantiated or invalidated. The problem is, too often people use qualitative terms such as 'high' or 'low', without defining them by using ranges or other objective scales. In those instances, the statements tend to be much more subjective, harder to substantiate or dispute, and essentially meaningless for real decision making.

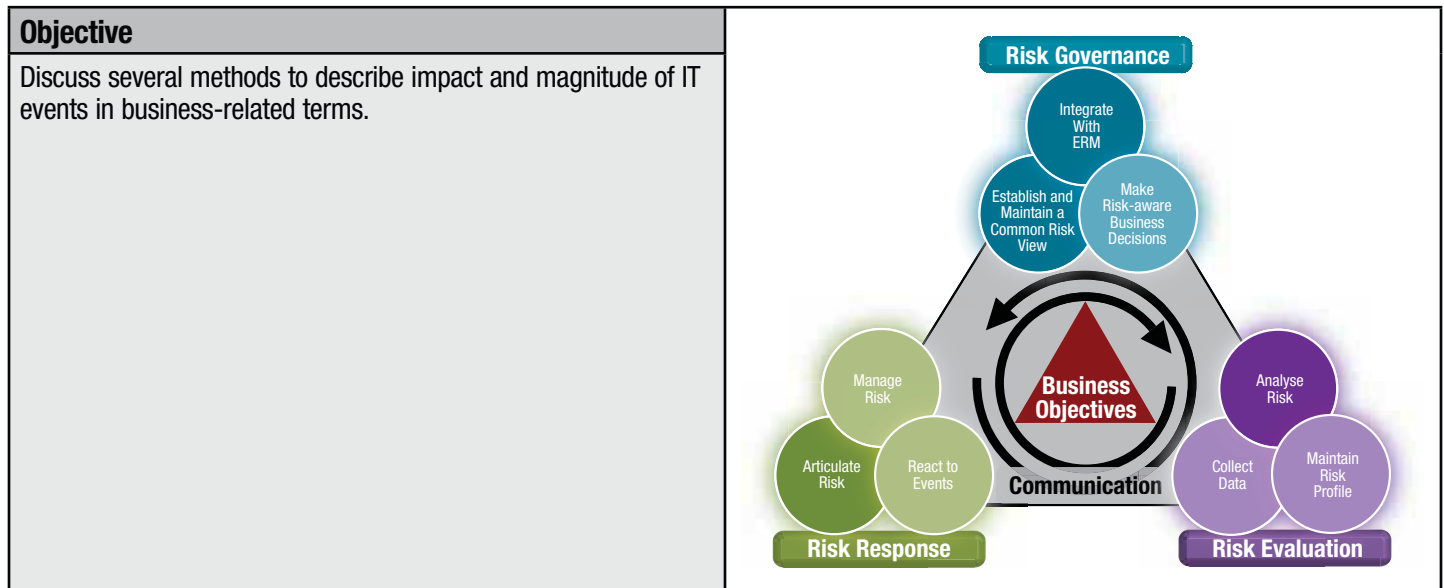
Statistical data may be available in varying quantities and quality, ranging on a continuous scale from almost non-existent to widely available. At the higher end of the scale, i.e., when a wide choice of statistical data are available, a quantitative assessment might be the preferred risk assessment method; at the other end of the scale, with very little, incomplete or poor data, a qualitative assessment may be the only available solution. Hybrid risk assessment methods may be applied to situations in between both extremes described here.

There are many good sources of data to support risk analysis, and there are a number of sources where these data can be obtained internally, including colleagues from BPI, the PMO, EA, QC and other disciplines that may be collecting similar data.

The following section of this chapter describes some suggested techniques that are mostly qualitative techniques and will be most commonly used. Despite their inherently lower precision, they can provide very insightful and relevant data because they provide a model by which all risks can be measured and described using the same language and reference base, eliminating the most notorious cases of subjectivity and ambiguity. For example:

- If a time frame is not specified in a scenario, then a conclusion that the likelihood of an event is ‘high’ may be interpreted differently by different people. One person might assume that it is highly likely to occur this year, while another person might assume that it means it is highly likely to happen eventually.
- If scales are not defined for loss magnitude, then one person’s subjective interpretation of ‘severe loss’ can be significantly different from someone else’s interpretation.

Expressing Impact in Business Terms

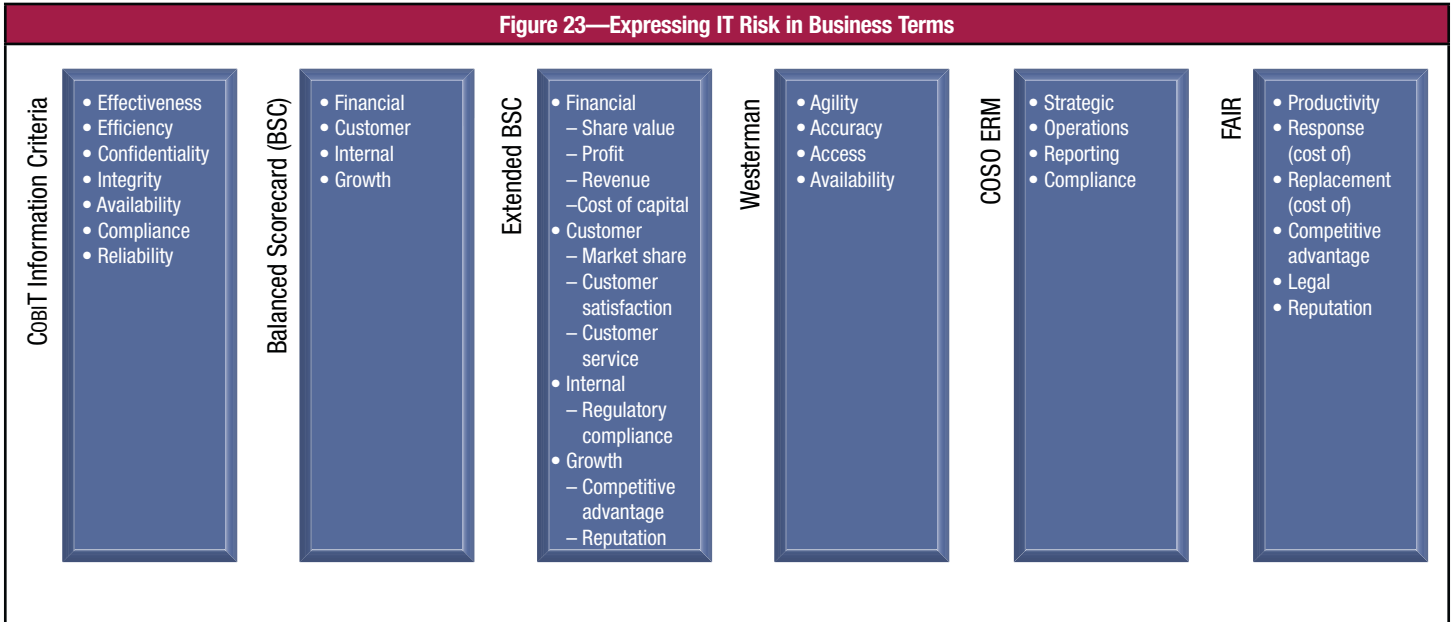


Meaningful IT risk assessments and risk-based decisions require that IT risk be expressed in unambiguous and clear business-relevant terms. Effective risk management requires mutual understanding between IT and the business over which risks need to be managed and why. All stakeholders must have the ability to understand and express how adverse events may affect business objectives. This means that:

- An IT person should understand how IT-related failures or events can impact enterprise objectives and cause direct or indirect loss to the enterprise.
- A business person should understand how IT-related failures or events can affect key services and processes.

The link between IT risk scenarios and ultimate business impact needs to be established to understand the effects of adverse events. Several techniques and options exist that can help the enterprise to describe IT risk in business terms. The Risk IT framework requires that IT risks be translated/expressed into business relevant terms, but does not prescribe any single method. Some available methods are shown in **figure 23** and they are briefly discussed in the remainder of this section.

Figure 23—Expressing IT Risk in Business Terms



COBIT Information Criteria (Business Requirements for Information)

The COBIT information criteria allow for the expression of business aspects related to the use of IT. They express a condition to which information (in the widest sense), as provided through IT, must conform for it to be beneficial to the enterprise.

The seven information criteria are:

- Efficiency
- Effectiveness
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

The business impact of any IT-related event lies in the consequence of not achieving the information criteria. By describing impact in these terms, this remains a sort of intermediate technique, not fully describing the business impact, e.g., impact on customers or in financial terms.

COBIT Business Goals and Balanced Scorecard

A further technique is based on the ‘business goals’ concept introduced in COBIT. Indeed, business risk lies in any combination of those business goals not being achieved. The COBIT business goals are structured in line with the four classic balanced scorecard (BSC) perspectives: financial, customer, internal and growth.

For practical purposes, one can imagine that for each business goal, a translation is possible to express the non-achievement of the goal in terms of its impact on the overall business, illustrated by the example in **figure 24**⁵:

Figure 24—COBIT (BSC) Risk Description in Business Terms

Business Goal	Risk Expressed as Business Consequence
Provide a good return on investment of IT-enabled business investments.	There is inadequate return on investment of IT-enabled business investments.
Improve corporate governance and transparency.	Inadequate financial transparency for markets reflects on share value and compliance risk.
Improve customer orientation and service.	Bad or insufficient customer service results in client loss.
Offer competitive products and services.	Ineffective products and services do not address customer needs, resulting in revenue loss.

⁵ This table contains a sample of the business goals as they are defined in COBIT 4.1. The full table is included in appendix I of the COBIT 4.1 framework.

Extended BSC Criteria

A variant of the approach described in the example in **figure 24** goes one step further, linking the BSC dimensions to a limited set of more tangible criteria. The following criteria are often observed to be used for this purpose:

- Financial
 - Share value
 - Profit
 - Revenue
 - Cost of capital
- Customer
 - Market share
 - Customer satisfaction
 - Customer service
- Internal
 - Regulatory compliance
- Growth
 - Competitive advantage
 - Reputation

This set of criteria can be used selectively, and the user should be aware that there are still cause-effect relationships included in this table (e.g., customer [dis]satisfaction can impact competitive advantage and/or market share). Usually a subset of these criteria is used to express risk in business terms.

Westerman 4 'A's—An Alternative Approach to Express Business Impact

Another means of expressing IT risk into business terms is based on the 4A framework⁶. This defines IT risk as the potential for an unplanned event involving IT to threaten any of four interrelated enterprise objectives:

- Agility—Possess the capability to change with managed cost and speed.
- Accuracy—Provide correct, timely and complete information that meets the requirements of management, staff, customers, suppliers and regulators.
- Access—Ensure appropriate access to data and systems, so that the right people have the access they need and the wrong people do not.
- Availability—Keep the systems (and their business processes) running, and recover from interruptions.

COSO ERM

The *COSO ERM—Integrated Framework* lists the following criteria:

- Strategic—High-level goals, aligned with and supporting the enterprise mission. Strategic objectives reflect management's choice as to how the enterprise will seek to create value for its stakeholders.
- Operations—These pertain to the effectiveness and efficiency of the enterprise's operations, including performance and profitability goals and safeguarding resources against loss.
- Reporting—These pertain to the reliability of reporting. They include internal and external reporting and may involve financial and non-financial information.
- Compliance—These pertain to adherence to relevant laws and regulations.

FAIR

The FAIR method is security-oriented in origin, but the impact criteria apply to all IT-related risks. The criteria used here are:

- Productivity—The reduction in an enterprise's ability to generate its primary value proposition (e.g., income, goods, services)
- Responses—Expenses associated with managing a loss event (e.g., internal or external person-hours, logistical expenses)
- Replacement—The intrinsic value of an asset, typically represented as the capital expense associated with replacing lost or damaged assets
- Competitive advantage—Losses associated with diminished competitive advantage
- Legal—Legal or regulatory actions levied against an enterprise
- Reputation—Losses associated with an external perception that an enterprise's value proposition is reduced or leadership is incompetent, criminal or unethical

Summary

There are multiple options for expressing IT risk in business terms, and there is no right or wrong option. One has to choose the option that fits best with the enterprise, and complement this scheme with a range of scales to quantify the risk during risk analysis. For those enterprises utilising COSO guidance for financial reporting purposes, more information can be found in the ISACA publication *IT Control Objectives for Sarbanes-Oxley, 2nd Edition*.

The following considerations need to be made, irrespective of the choice of impact description method:

- Define impact scales (these are discussed in the Describing Risk—Expressing Impact section) linked to the impact description method chosen so that they are clear and unambiguous for everyone and truly represent business objectives.
- Ensure that the chosen method and scales also allow easy definition of risk appetite, i.e., what is acceptable and unacceptable risk, in the same terms across the enterprise.

⁶ Westerman, G.; R. Hunter; 'IT Risk—Turning Business Threats Into Competitive Advantage', Harvard Business School Press, USA, 2007

4. EXPRESSING AND DESCRIBING RISK

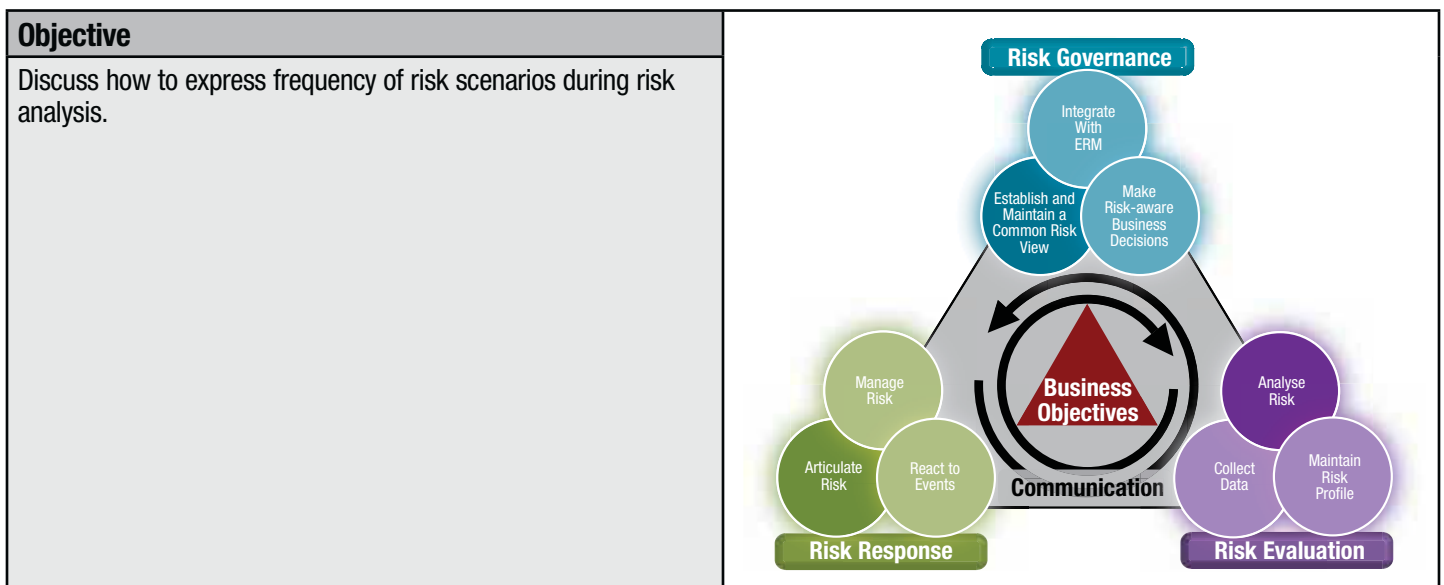
- Ensure that IT-related events and scenarios are clearly mapped to the business impact descriptions; this means that dependencies between events (e.g., hardware failure) and ultimate business impact and consequence (e.g., customers cannot place orders, resulting in customer dissatisfaction) need to be mapped and included in any risk analysis.

The following example demonstrates how COBIT can be used to achieve the link between the ‘atomic’ IT event and business goals, i.e., how this event can jeopardise one or several business goals:

- Impact is expressed in business-relevant terms, using the words of the ‘business goals’ as used in COBIT. For example, the enterprise, running an online travel business, has as its major business goals: ‘improve customer service’ and ‘service continuity’.
- The COBIT framework maps the business goals to IT goals (how the goals of the IT department support the achievement of the business goals), and this link is read in the other direction: Not achieving an IT goal might have a negative impact on the achievement of a business goal. In the example, the ‘service continuity’ business goal implies that IT pays importance to some specific IT goals, e.g., third-party relationship management, reducing application defects, ensuring minimum business impact in case of an IT disruption.
- This cascade is continued down to the IT process level and IT activity level, using the same principle that not achieving a ‘lower-level’ goal will jeopardise the achievement of the ‘higher-level’ goal. The IT goals set in the example would require a number of IT processes to be excellent, including COBIT processes PO8 *Manage quality*, AI4 *Enable operation and use of IT*, AI6 *Manage changes*, AI7 *Install and accredit solutions*, DS2 *Manage third-party services*, DS4 *Ensure continuous service*, DS10 *Manage problems*, DS12 *Manage the physical environment* and some others. This would require the activities (as described in the process model for each COBIT IT process) to be executed well.
- When analysing IT risk scenarios, each risk scenario can be linked to one or more IT processes, i.e., if the process does not perform, the frequency and/or impact of the scenario will increase (see chapter 5, Capability Risk Factors in the Risk Analysis Process section). Applying this cascade backwards, it is possible to trace all potential impact paths that an event can have on business goals, and use this information in risk analyses. In the example, this means that any disruption of the mentioned IT processes, e.g., lack of project management (PO8), inadequate software testing (AI7), bad third-party relationship management or service level management (DS1, DS2), can have a negative impact on the achievement of the stated service-oriented business goals. However, when these processes are really mature and being performed, this means that the enterprise is in good shape to achieve the stated business goals.

For those enterprises subject to Basel II regulations, more guidance can also be found in the ISACA publication *IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance*.

Describing Risk—Expressing Frequency



When analysing risk scenarios (see chapter 5), two properties of each risk scenario need to be assessed: frequency and magnitude. This section deals with frequency of risk scenarios occurring. The estimation of the frequency takes into account a number of parameters, including all risk factors (see chapter 5, Risk Scenarios Explained section for more details) and past occurrences.

Some risk management methods use the term ‘likelihood’ or ‘probability’. In Risk IT, the term ‘frequency’ is preferred, expressed as the ‘number of times an event occurs in a given time period’ because it allows for more precision when dealing with events that occur more than once in a given time period. If a certain event (e.g., project delay) occurs once in a year or 10 times in a year, the concept of likelihood would assign a value of 1 to both events. When using frequency, the cases can be better differentiated.

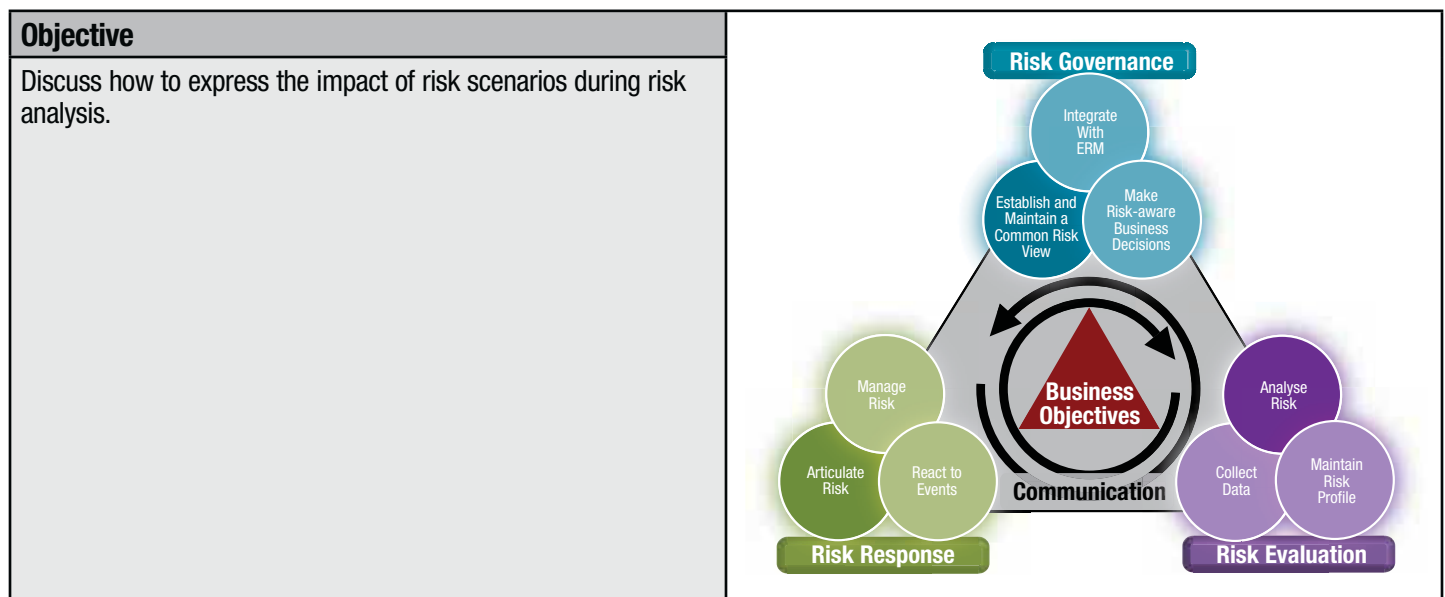
Figure 25 proposes a scheme that can be used for expressing the frequency of risk scenarios occurring. The example uses a 0 to 5 scale, with a frequency threshold associated with each scale value. In the example, a logarithmic scale has been used for frequency although, in many cases, this is not mandatory; linear scales can be used as well. Alternatively, an index scale can be used. Frequency is then translated into a number from 0 to 100, e.g., based on a logarithmic scale or any other sort of scale. The choice for either method depends on how the results of the risk analysis will be presented, e.g., in a risk matrix. See the Risk Maps section for more information. In **figure 25**, a risk scenario that is estimated to occur five times in a year gets the score of 3.

Frequency Rating	Times Occurring per Year
5	100
4	10
3	1
2	0.1
1	0.01
0	0.001

Some enterprises prefer a three-level scale instead of a five-level scale. The advantage of such a scale is that analyses will go faster and might look a bit easier; however, there is a loss of precision, and using a three-level scale has a tendency to create a lot of ‘middle’ values because of people being averse to creating extreme cases, leading to even more inaccuracies.

Some enterprises assign labels, e.g., ‘very frequent’, ‘frequent’, ‘infrequent’, ‘rare’, to the scales mentioned in **figure 25**. The use of only these labels as means of expressing frequency is not advisable because they can mean different things for different risk scenarios and consequently can generate confusion. For example, an attempt for network intrusion through the firewall might happen hundreds of times per day, which may be considered ‘average’; an ‘average’ frequency of a hardware failure (e.g., disk crash) might be once every two or three years. So the word ‘average’ means different frequencies for two different scenarios and, hence, is not well suited as an objective and unambiguous indicator of frequency.

Describing Risk—Expressing Impact



When analysing risk scenarios (see chapter 5), two properties of each risk scenario need to be assessed: frequency and magnitude. This section deals with magnitude (or impact) when risk scenarios occur.

‘Magnitude’ and ‘impact’ are used almost interchangeably throughout this guide, although they can carry slightly different nuances: magnitude is a more objective, hard description of how big something is, whereas impact is a more subjective description of what this means for enterprises, and how it may impact business objectives. The technique to describe impact, explained in this section, includes both aspects.

Risk analysis requires the estimation of the frequency of adverse events and their impact (expressed in business terms). Many enterprises use their own developed scales for this purpose, based on one of the techniques described in the Expressing Impact in Business Terms section.

Figure 26 includes an example of such an approach; the example is not prescriptive, i.e., each enterprise should adapt this to its own needs.

The example illustrates that the:

- Enterprise has created a set of impact criteria based on the earlier described FAIR approach
- Enterprise has created a 0 to 5 scale for all impact criteria and has indicated the meaning of each of the scores, e.g., if the rating on the annual customer survey drops below 6.5, a score of 2 is given; if there is a regulatory problem such that the license to do business is revoked, a score of 5 is attributed.
- Scales on the left (0 to 5) make the technique easier to manipulate and allow creation of graphic representations of the risk; however, the right-most column describes the actual impact and makes it possible to argue and defend the impact score given to a particular risk.

4. EXPRESSING AND DESCRIBING RISK

Some enterprises would go one step further and use a system that includes, for all criteria and ranges, a monetary equivalent. However, this is not always an easy exercise.

Figure 26—Example Impact Scales

Business Impact Scales for Risk Assessment				
I	Competitive Advantage— Market Share	Market Share on Target Markets		
	5	<25%		
	4	<30%		
	3	<32%		
	2	<34%		
	1	<35%		
	0	<36%		
II	Productivity— Revenue Loss	% of Revenue		
	5	>10%		
	4	<10%		
	3	<5%		
	2	<2%		
	1	<1%		
	0	<0%		
III	Response— Cost of Response	Amount (US \$)		
	5	>\$10,000,000		
	4	\$10,000,000		
	3	\$5,000,000		
	2	\$2,000,000		
	1	\$1,000,000		
	0	\$0		
IV	Reputation— Customer Satisfaction	Rating on Annual Customer Survey		
	5	<5.0		
	4	<5.5		
	3	<6.0		
	2	<6.5		
	1	<7.0		
	0	<7.5		
V	Reputation— External Perception	Damage		
	5	Continued negative press coverage		
	4			
	3	Negative press coverage		
	2			
	1	News article		
	0			
VI	Legal—Regulatory Non-compliance	Legal	Financial (US \$)	License to Operate
	5	Personal prison	>\$10,000,000	Revoked
	4		\$10,000,000	
	3	Personal conviction	\$5,000,000	Fined
	2		\$2,000,000	
	1		\$1,000,000	
	0		\$0	

There is benefit in using the same metrics groups for frequency and impact across the entire (extended) enterprise: to allow better understanding of risk and easier comparisons across the value chains. Ultimately, most risk analysis methods will require one number or result for impact, aggregating the results of the rating of all underlying criteria. Several methods exist to transform the scores for multiple criteria into one impact score, as illustrated in **figure 27**.

Figure 27—Example Impact Scales With Scoring

Business Impact Scales for Risk Assessments Rating				
I	Competitive Advantage— Market Share	Market Share on Target Markets		2
	5	<25%		
	4	<30%		
	3	<32%		
	2	<34%		
	1	<35%		
	0	>36%		
II	Productivity— Revenue Loss	% of Revenue		2
	5	>10%		
	4	<10%		
	3	<5%		
	2	<2%		
	1	<1%		
	0	0%		
III	Response— Cost of Response	Amount (US \$)		1
	5	> \$10,000,000		
	4	\$10,000,000		
	3	\$5,000,000		
	2	\$2,000,000		
	1	\$1,000,000		
	0	\$0		
IV	Reputation—Customer Satisfaction	Rating on Annual Customer Survey		4
	5	<5.0		
	4	<5.5		
	3	<6.0		
	2	<6.5		
	1	<7.0		
	0	>7.5		
V	Reputation— External Perception	Damage		2
	5	Continued negative press coverage		
	4			
	3	Negative press coverage		
	2			
	1	News article		
	0			

4. EXPRESSING AND DESCRIBING RISK

Figure 27—Example Impact Scales With Scoring (cont.)

VI	Legal—Regulatory Non-compliance	Legal	Financial (US \$)	License to Operate	3
	5	Personal prison	>\$10,000,000	Revoked	
	4		\$10,000,000		
	3	Personal conviction	\$5,000,000	Fined	
	2		\$2,000,000		
	1		\$1,000,000		
	0		\$0		
Overall Impact Score					
		Average	(Scale 0-5)		2.3
		Maximum	(Scale 0-5)		4.0
		Index100	(Scale 0-100)		46

In this example, a particular risk scenario is analysed and each criterion is scored. At the bottom, three different resulting impact scores are given:

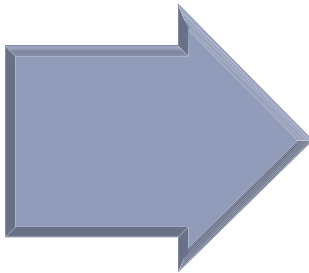
- The average impact rating over all six criteria, in this example resulting in a score of 2.3. This sounds logical, although mathematically it makes little sense. The numbers are only ordinal numbers, and behind each number is a completely different meaning, so ultimately the average of these scores does not carry a real meaning. However, it provides a rough indication—in the sense that an average of 4 will probably be a higher risk than an average of 2, which is sufficient for most purposes.
- The maximum score for any underlying criterion is used as total score, resulting in this example of a score of 4. Again, the reasoning may sound logical: if there is an important impact in one dimension, irrespective of the other dimension, that important impact will remain. However, one risk scenario resulting in all scores of 4 is visibly different from another scenario with one score of 4 and all the rest of 1. This method would give both a final score of 4, but obviously the former case is a much more important risk than the latter.
- An index calculation (scale 100), also based on average scores ($\frac{2.3}{5} \times 100$), resulting in an index of 46 in this example. This method is equivalent to the average impact rating.

Each enterprise has to select its own way of expressing the overall impact. There is no ultimate right or wrong; each method has its own merits. See also the Risk Maps section, where the discussion warns against doing advanced math with the ratings obtained here.

For reporting purposes, the thresholds used to measure impact should be set at the enterprise level to ensure consistency of risk reporting between individual units.

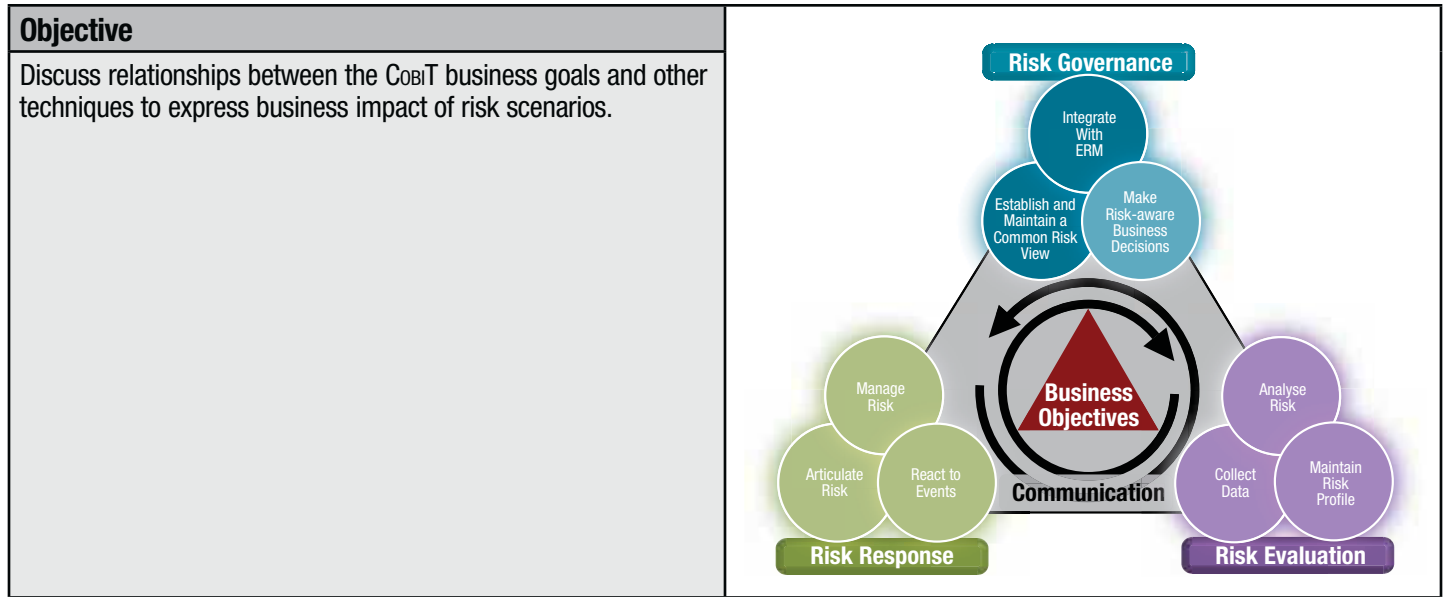
Some enterprises use several impact criteria and use weights to calculate a compound impact score or index. Although elegant at first sight, this can be seen as overly complicating and unnecessary. Indeed, if one or more criteria are very important for an enterprise, the thresholds between the different ratings can be lowered. If, for example, customer satisfaction is very important, rather than using weights to increase the influence of this criterion, one could simply use a set of lower thresholds to generate the same outcome: customer satisfaction is a key risk. **Figure 28** illustrates this example.

Figure 28—Changing Impact Scales to Indicate Importance of an Impact Criterion

Customer Satisfaction	Rating on Annual Customer Survey		Customer Satisfaction	Rating on Annual Customer Survey
5	<5		5	<6
4	<5.5		4	<6.5
3	<6		3	<7
2	<6.5		2	<7.5
1	<7		1	<8
0	>7		0	>8

A final consideration when estimating impact during risk analysis: the best way to obtain reliable and accepted estimations is to involve all stakeholders in scenario-analysis exercises. This can be done through separate assessments, followed by group discussion to achieve consensus, or through workshops.

COBIT Business Goals Mapping With Other Impact Criteria



In the Expressing Impact in Business Terms section, different methods to express business impact are listed. This section contains a number of tables to help understand how these methods and their criteria relate to each other. The business goals defined in COBIT are used as the central concept in these comparisons:

- **Figure 29** describes how the business goals from COBIT can be used to express a (negative) business consequence when they are not achieved.
- **Figure 30** is a mapping between the COBIT business goals and the other possible methods of expressing business impact (Westerman/Hunter).
- **Figure 31** is a mapping between the COBIT business goals and the other possible methods of expressing business impact (COBIT information criteria).
- **Figure 32** is a mapping between the COBIT business goals and the other possible methods of expressing business impact (BSC extended impact criteria).

The purpose of **figures 29 to 32** is to make the link between the COBIT method of expressing business risk (through the use of business goals/BSC) and some of the other methods mentioned in the previous section. This allows users to compare them for coverage and completeness.

In **figures 30 to 32**, a ‘P’ indicates a primary, higher degree of fit; an ‘S’ indicates a secondary, lower degree of fit.

Figure 29 describes COBIT business goals and how they can be reworded to express business impact.

Figure 29—Business Goals and Business Consequences	
Business Goal	Business Impact
Financial Perspective	
Provide a desired return on investment of IT-enabled business investments.	Inadequate financial return on investment of IT-enabled business investments
Manage IT-related business risk.	IT-related risks not managed, leaving the company exposed
Improve corporate governance and transparency.	Inadequate transparency for stakeholders, not meeting client expectations; lack of compliance
Customer Perspective	
Improve customer orientation and service.	Bad or insufficient customer service, resulting in client loss
Offer competitive products and services.	Inadequate products and services, not addressing customer needs, resulting in revenue loss
Establish service continuity and availability.	Inadequate service levels, resulting in customer dissatisfaction and potential revenue loss
Create agility in responding to changing business requirements.	Inability to react to changing market or client requirements on a timely basis, resulting in revenue loss
Achieve cost optimisation of service delivery.	Products or services brought to market at too high a price or inadequate profit margin, potentially resulting in share value and client loss
Obtain reliable and useful information for strategic decision making.	Wrong strategic decisions on new business initiatives, resulting in client/revenue loss and shareholder value

4. EXPRESSING AND DESCRIBING RISK

Figure 29—Business Goals and Business Consequences (cont.)

Business Goal	Business Impact
Internal Perspective	
Improve and maintain business process functionality.	Inefficient and inadequate operations of the enterprise
Lower process costs.	Lower profitability
Provide compliance with external laws, regulations and contracts.	Violation of regulations or contracts, resulting in legal fines/damages or personal legal consequences for board and executives
Provide compliance with internal policies.	Inefficient and inadequate operations of the enterprise, resulting in compliance issues
Manage business change.	Inefficient and inadequate operations of the enterprise, resulting in loss of opportunities
Improve and maintain operational and staff productivity.	Inefficient and inadequate operations of the enterprise, resulting in inadequate productivity and efficiency
Learning and Growth Perspective	
Manage product and business innovation.	Loss of opportunities, low growth, eroding market share
Acquire and maintain skilled and motivated people.	Inability to sustain growth or current operations

Figure 30 describes COBIT business goals and impacts mapped against the Westerman 4A business impacts.

Figure 30—Relation COBIT Business Goals (Westerman/Hunter)

Business Goals—Consequence	4A Business Impact			
	Agility	Accuracy	Access	Availability
Financial Perspective				
Inadequate financial return on investment of IT-enabled business investments	P			
IT-related risks not managed, leaving the company exposed	P	P	P	P
Inadequate financial transparency for stakeholders, not meeting client expectation; lack of compliance	P			
Customer Perspective				
Bad or insufficient customer service, resulting in client loss		S	P	P
Inadequate products and services, not addressing customer needs, resulting in revenue loss	P	S	P	S
Inadequate service levels, resulting in customer dissatisfaction and potential revenue loss		S	P	P
Inability to react to changing market or client requirements on a timely basis, resulting in revenue loss	P			S
Products or services brought to market at too high a price or inadequate profit margin, potentially resulting in share value and client loss	P			
Wrong strategic decisions on new business initiatives, resulting in client/revenue loss and shareholder value	P			
Internal Perspective				
Inefficient and inadequate operations of the enterprise		P		P
Lower profitability	S			
Violation of regulations or contracts, resulting in legal fines/damages or personal legal consequences for board and executives		P	P	
Inefficient and inadequate operations of the enterprise		P	S	S
Inefficient and inadequate operations of the enterprise, resulting in loss of opportunities	P			
Inefficient and inadequate operations of the enterprise, resulting in inadequate productivity and efficiency	P	P		
Learning and Growth Perspective				
Loss of opportunities, low growth, eroding market share	P			
Inability to sustain growth or current operations	P	S		

Figure 31 describes COBIT business goals and impacts mapped against COBIT information criteria.

Figure 31—Mapping Between Business Goals/Consequences and COBIT Information Criteria							
Business Goals—Consequence	COBIT Information Criteria						
	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
Financial Perspective							
Inadequate financial return on investment of IT-enabled business investments		P					
IT-related risks not managed, leaving the company exposed			P	P	P		
Inadequate financial transparency for stakeholders, not meeting client expectation; lack of compliance		S					P
Customer Perspective							
Bad or insufficient customer service, resulting in client loss	P	S		S	S		
Inadequate products and services, not addressing customer needs, resulting in revenue loss	P	S					S
Inadequate service levels, resulting in customer dissatisfaction and potential revenue loss	P	S	S	S	P		
Inability to react to changing market or client requirements on a timely basis, resulting in revenue loss	P	S					
Products or services brought to market at too high a price or inadequate profit margin, potentially resulting in share value and client loss		P					
Wrong strategic decisions on new business initiatives, resulting in client/revenue loss and shareholder value	P		S	S			S
Internal Perspective							
Inefficient and inadequate operations of the enterprise	P	P	S	S	S		S
Lower profitability		P					
Violation of regulations or contracts, resulting in legal fines/damages or personal legal consequences for board and executives			P	S	S	P	
Inefficient and inadequate operations of the enterprise, resulting in compliance issues			P	S	S	P	S
Inefficient and inadequate operations of the enterprise, resulting in loss of opportunities	S	P	S				
Inefficient and inadequate operations of the enterprise, resulting in inadequate productivity and efficiency	P	S			S		
Learning and Growth Perspective							
Loss of opportunities, low growth, eroding market share	S	P					
Inability to sustain growth or current operations	P	S					

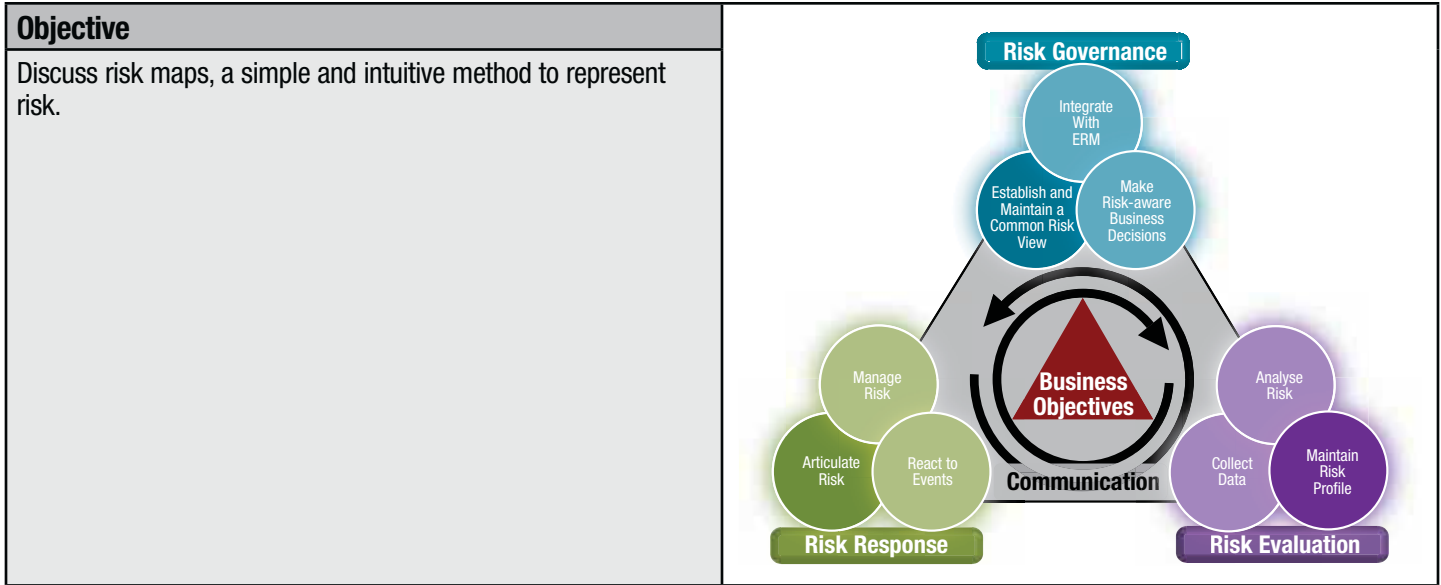
Figure 32 describes COBIT business goals and impacts mapped against some extended BSC criteria.

4. EXPRESSING AND DESCRIBING RISK

Figure 32—Mapping Between Business Goals/Consequences and Extended BSC Criteria

Business Goals—Consequence	Extended BSC Criteria								
	Share Value	Profit and Revenue	Cost of Capital	Market Share	Customer Satisfaction	Customer Service	Regulatory Compliance	Competitive Advantage	Reputation
Financial Perspective									
Inadequate financial return on investment of IT-enabled business investments	P	P	P					S	
IT-related risks are not managed, leaving the company exposed							S		P
Inadequate financial transparency for stakeholders, not meeting client expectation; lack of compliance	P		S				P		
Customer Perspective									
Bad or insufficient customer service, resulting in client loss				P	P	P		S	S
Inadequate products and services, not addressing customer needs, resulting in revenue loss					P	S		S	S
Inadequate service levels, resulting in customer dissatisfaction and potential revenue loss		P			P	P		S	S
Inability to react to changing market or client requirements on a timely basis, resulting in revenue loss		P			P			S	S
Products or services brought to market at too high a price or inadequate profit margin, potentially resulting in share value and client loss		S		S	P				
Wrong strategic decisions on new business initiatives, resulting in client/revenue loss and shareholder value	P	P		P	P			S	S
Internal Perspective									
Inefficient and inadequate operations of the enterprise			P			S			
Lower profitability		P		P				P	
Violation of regulations or contracts, resulting in legal fines/damages or personal legal consequences for board and executives							P		
Inefficient and inadequate operations of the enterprise, resulting in compliance issues							P		
Inefficient and inadequate operations of the enterprise, resulting in loss of opportunities								P	
Inefficient and inadequate operations of the enterprise, resulting in inadequate productivity and efficiency								P	
Learning and Growth Perspective									
Loss of opportunities, low growth, eroding market share	P	P		P				P	
Inability to sustain growth or current operations	P	P		P				P	

Risk Map



In the previous sections, the two fundamental properties of risk, i.e., frequency and magnitude/impact, were discussed.

A common and very easy and intuitive technique to present risk is the risk map, where risks are plotted on a two-dimensional diagram, with frequency and impact being the two dimensions. A sample risk map is shown in **figure 33**.

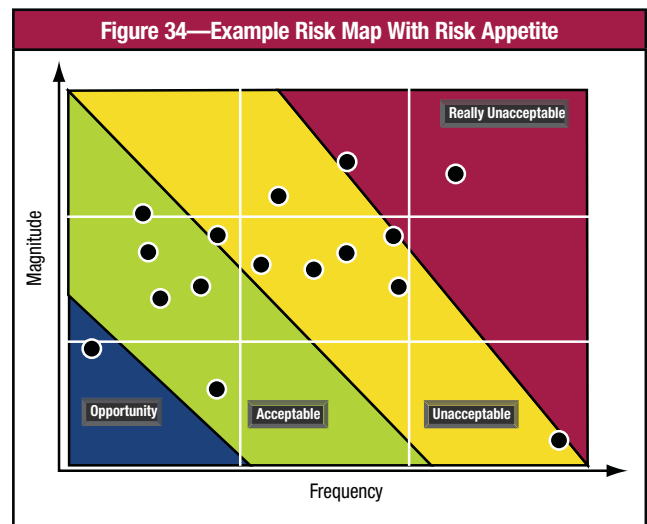
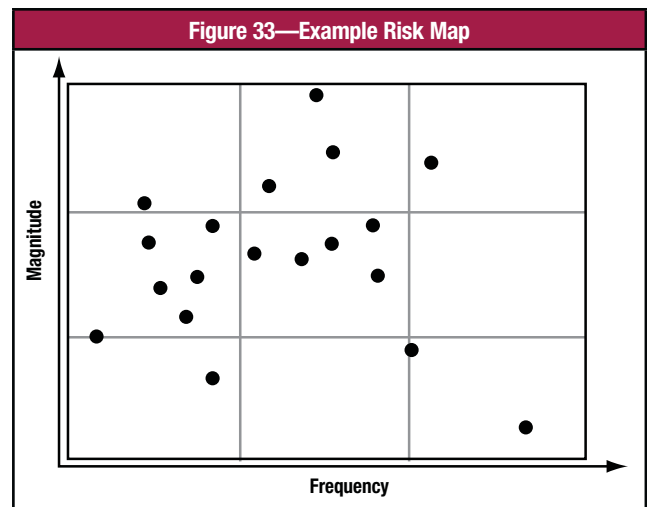
The risk map representation is powerful and provides an immediate and complete view on IT risk and apparent areas for action.

The risk map becomes even more powerful when it is combined with the different zones of risk appetite (see chapter 2). Different risk appetite bands of significance are defined in the risk map using coloured zones, leading to the example in **figure 34**. This version of the risk map immediately identifies those risks that are truly unacceptable and require an immediate response, as defined by the enterprise risk appetite definitions.

At the other end of the spectrum, the risk map could also allow for the identification of opportunities for relaxing controls or taking on more risk, as represented by the blue zone in **figure 34**.

When analysing and describing risk using risk maps and the two dimensions—frequency and magnitude—the following need to be taken into account:

- It is advisable to analyse all risk scenarios that have been identified to obtain a complete view on IT risk and to include them in the risk map.
- It is advisable to maintain the two dimensions of risk separately. Frequency and impact are both valuable information, and both are needed for the definition of the actual response (e.g., which controls to implement, whether to take out insurance coverage).
- The ordinal numbers used to describe frequency and impact in many risk analysis schemes, including the examples given in the previous sections, are numeric, but using them to do any (advanced) math to describe overall risk is deceiving because they carry no real meaning except a quantitative scale/range. The frequency/magnitude ratings are sufficient to get an adequate view of IT risk, but doing any math with them does not add any reliable or actionable insights. It is not advisable to do things such as:
 - Multiply frequency and impact to have a measure for risk (although there might be some indication of relative importance of the risk in this number) since there is no precision in such calculations and the meaning depends on the scales used. Furthermore, it is inadvisable to treat two risk scenarios, one score of 2 for frequency and 4 for impact and one score of 4 for frequency and 2 for impact, as the same risk, unless all impact scales use amounts and are properly and

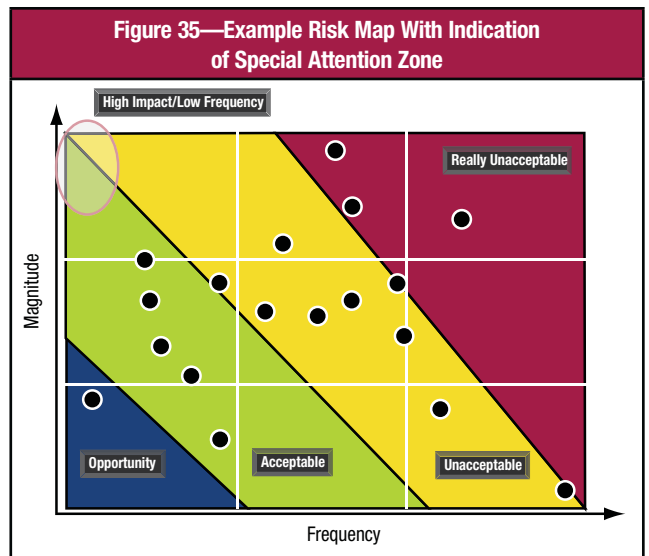


4. EXPRESSING AND DESCRIBING RISK

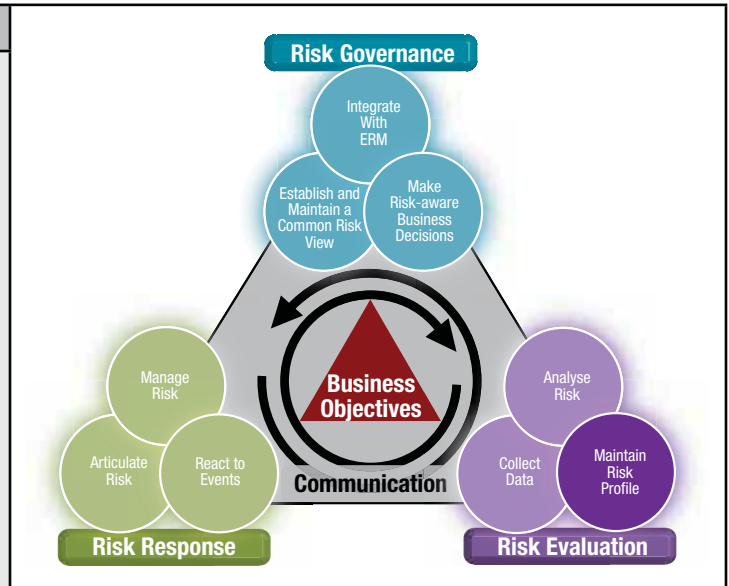
consistently defined. In any other situation, all that can be said is that the two scenarios are within the same risk appetite band.

- Add all the (frequency times impact) products to an overall risk number. This number, although providing some relative insight, does not give any indication of the actual risk exposure.
- Once the enterprise users are comfortable using and communicating with the basic risk map, the concept can be extended to more advanced maps that provide still stronger guides to prioritising actions. These could include maps that compare importance against the perceived gap between current and desired state and the ability to detect against the ability to respond.
- A number of risks (tail events) carry the profile ‘low frequency but high impact’. These cases warrant separate discussions because of their often dramatic impact. In these cases, management needs to decide which risks it will simply accept or which require a response (very often an expensive response). **Figure 35** illustrates this zone.

Risk Register



Objective
Discuss risk registers, their purpose and suggested contents.



The concept of the risk register is related to risk maps and risk scenarios. The risk register can be seen as an extension of the risk map, providing detailed information on each identified risk, including:

- Information on the risk owner
- Information on details of the risk scenario
- Information on detailed scores in the risk analysis
- Detailed information on the risk response and risk response status
- Information on controls (if applicable)

Risk registers are part of the process RE3 *Maintain risk profile* of the Risk IT process model. **Figure 36** shows a possible template for a risk register entry. Risk registers serve as the main reference for all risk-related information, supporting all risk-related decisions. There is no new information in the risk register not covered in the previous sections: a risk register is just a convenient technique to store and maintain all collected information in a useful format for all stakeholders.

The remainder of this section contains a template for a risk register. This template is not meant to be prescriptive, but serves only as an example. Every enterprise needs to develop its own customised template for use throughout the enterprise.

The template shown in **figure 36** makes the following assumptions:

- The enterprise uses a 0 to 5 scale for assessing the frequency and impact/magnitude of risk scenarios.
- The enterprise uses four impact criteria when analysing risk—productivity, cost of response, competitive advantage and legal.
- The overall impact rating is calculated using the mathematical average of the four impact ratings.
- Overall risk is calculated using a risk map, where the values of frequency and impact are plotted (for an example, see the Risk Maps section).

Figure 36—Template Risk Register Entry

Part I—Summary Data						
Risk statement						
Risk owner						
Date of last risk assessment						
Due date for update of risk assessment						
Risk category	<input type="checkbox"/> Strategic (IT benefit/value enablement)	<input type="checkbox"/> Project Delivery (IT programme and project delivery)	<input type="checkbox"/> Operational (IT operations and service delivery)			
Risk classification (copied from risk analysis results)	<input type="checkbox"/> Low	<input type="checkbox"/> Medium	<input type="checkbox"/> High	<input type="checkbox"/> Very high		
Risk response	<input type="checkbox"/> Accept	<input type="checkbox"/> Transfer	<input type="checkbox"/> Mitigate	<input type="checkbox"/> Avoid		
Part II—Risk Description						
Title						
High-level scenario (from list of sample high-level scenarios)						
Detailed scenario description— scenario components	Actor					
	Threat type					
	Event					
	Asset/resource					
	Timing					
Other scenario information						
Part III—Risk Analysis Results						
Frequency of scenario (number of times per year)	0	1	2	3	4	5
	$N \leq 0.01$ <input type="checkbox"/>	$0.01 < N \leq 0.1$ <input type="checkbox"/>	$0.1 < N \leq 1$ <input type="checkbox"/>	$1 < N \leq 10$ <input type="checkbox"/>	$10 < N \leq 100$ <input type="checkbox"/>	$100 < N$ <input type="checkbox"/>
Comments on frequency						
Impact of scenario on business	0	1	2	3	4	5
	1. Productivity Revenue loss over one year					
Impact rating	$I \leq 0.1\%$ <input type="checkbox"/>	$0.1\% < I \leq 1\%$ <input type="checkbox"/>	$1\% < I \leq 3\%$ <input type="checkbox"/>	$3\% < I \leq 5\%$ <input type="checkbox"/>	$5\% < I \leq 10\%$ <input type="checkbox"/>	$10\% < I$ <input type="checkbox"/>
Detailed description of impact						
Part III—Risk Analysis Results (cont.)						
2. Cost of response	Expenses associated with managing the loss event (US \$)					
	$I \leq \$10k$ <input type="checkbox"/>	$\$10k < I \leq \$100k$ <input type="checkbox"/>	$\$100k < I \leq \$1M$ <input type="checkbox"/>	$\$1M < I \leq \$10M$ <input type="checkbox"/>	$\$10M < I \leq \$100M$ <input type="checkbox"/>	$\$100M < I$ <input type="checkbox"/>
Detailed description of impact						
3. Competitive advantage	Drop in customer satisfaction ratings					
	$I \leq 0.5$ <input type="checkbox"/>	$.05 \leq I \leq 1$ <input type="checkbox"/>	$1 < I \leq 1.5$ <input type="checkbox"/>	$1.5 < I \leq 2$ <input type="checkbox"/>	$2 < I \leq 2.5$ <input type="checkbox"/>	$2.5 < I$ <input type="checkbox"/>
Detailed description of impact						
4. Legal	Regulatory compliance—Fines (US \$)					
	None <input type="checkbox"/>	$< \$1M$ <input type="checkbox"/>	$< \$10M$ <input type="checkbox"/>	$< \$100M$ <input type="checkbox"/>	$< \$1B$ <input type="checkbox"/>	$> \$1B$ <input type="checkbox"/>
Detailed description of impact						
Overall Impact rating (average of four impact ratings)						
Overall rating of risk, obtained by combining frequency and impact ratings on risk map	<input type="checkbox"/> Low	<input type="checkbox"/> Medium	<input type="checkbox"/> High	<input type="checkbox"/> Very high		

4. EXPRESSING AND DESCRIBING RISK

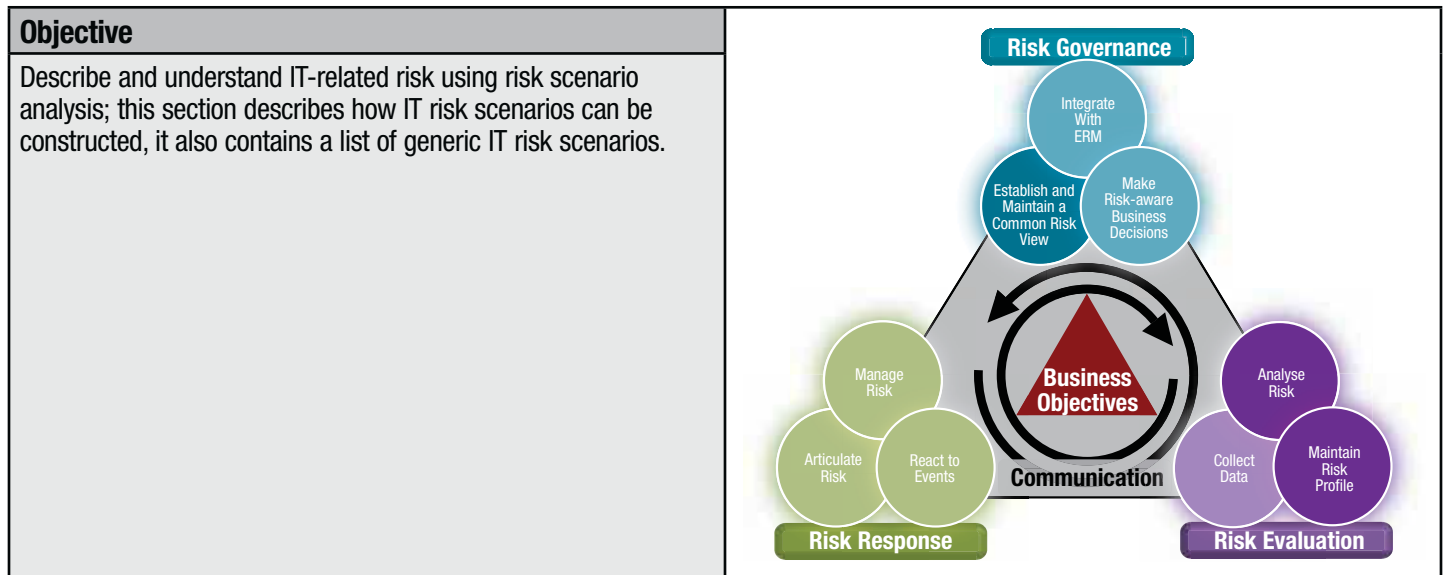
Figure 36—Template Risk Register Entry (cont.)

Part IV—Risk Response			
Risk response for this risk	<input type="checkbox"/> Accept	<input type="checkbox"/> Transfer	<input type="checkbox"/> Mitigate <input type="checkbox"/> Avoid
Justification			
Detailed description of response (not in case of 'accept')	Response Action	Completed	Action Plan
	1.	<input type="checkbox"/>	<input type="checkbox"/>
	2.	<input type="checkbox"/>	<input type="checkbox"/>
	3.	<input type="checkbox"/>	<input type="checkbox"/>
	4.	<input type="checkbox"/>	<input type="checkbox"/>
	5.	<input type="checkbox"/>	<input type="checkbox"/>
	6.	<input type="checkbox"/>	<input type="checkbox"/>
Overall status of risk action plan			
Major issues with risk action plan			
Overall status of completed responses			
Major issues with completed responses			
Part V—Risk Indicators			
Key risk indicators for this risk	1. 2. 3. 4. 5. 6.		

Page intentionally left blank

5. RISK SCENARIOS

Risk Scenarios Explained

**Introduction**

Risk scenario analysis is a technique to make IT risk more concrete and tangible and to allow for proper risk analysis and assessment. It is a core approach to bring realism, insight, organisational engagement, improved analysis and structure to the complex matter of IT risk. The section is structured as follows:

- Description of the scenario analysis (risk analysis) flow, showing the importance and relevance of risk scenarios
- Discussion of risk factors that need to be taken into account when creating and assessing risk scenarios
- Discussion of the different components in a risk scenario
- Guidelines on how to construct a set of relevant risk scenarios

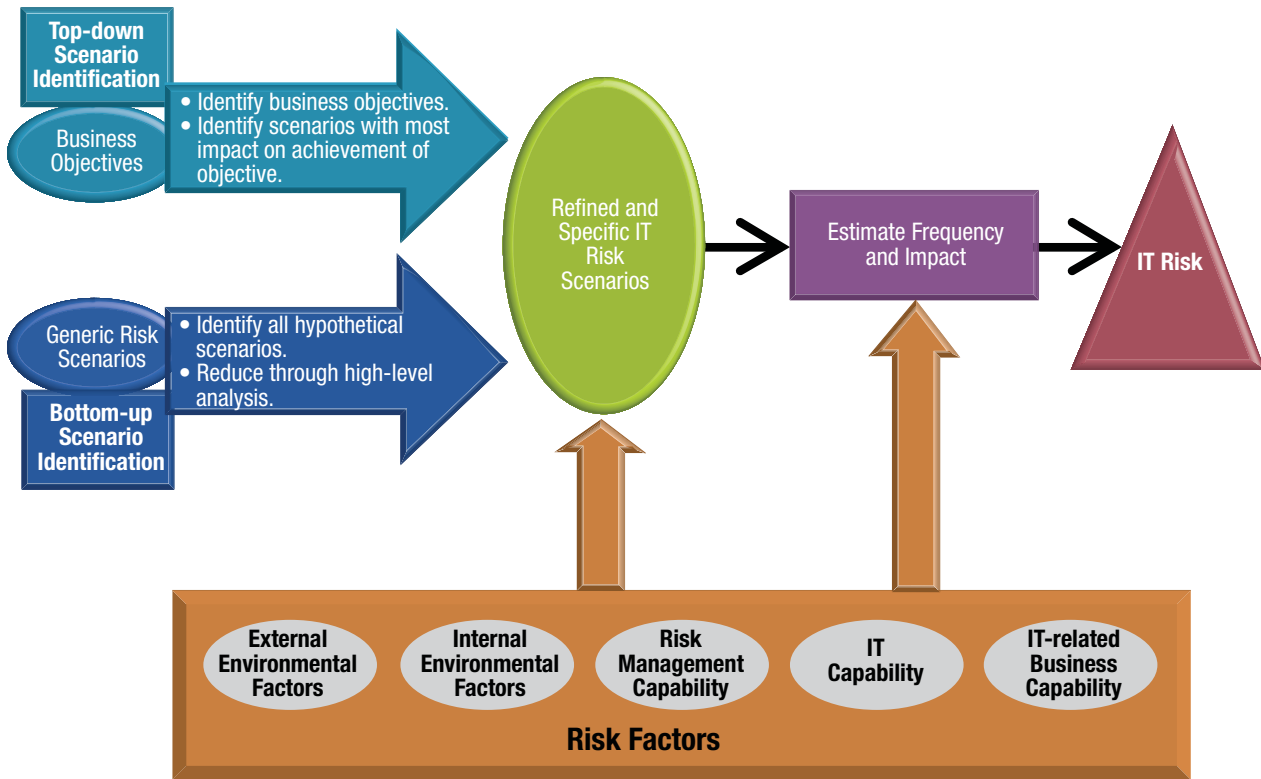
Scenario Analysis Flow

One of the challenges for IT risk management is to identify the important and relevant risks amongst all that can possibly go wrong with IT or in relation to IT, given the pervasive presence of IT and the business dependence on it. One of the techniques to overcome this challenge is the development and use of risk scenarios. Once these scenarios are developed, they are used during the risk analysis, where frequency of the scenario occurring and business impacts are estimated.

Figure 37 shows that risk scenarios can be derived via two different mechanisms:

- A top-down approach, where one starts from the overall business objectives and performs an analysis of the most relevant and probable IT risk scenarios impacting the business objectives. If the impact criteria (as defined in chapter 4, Expressing Impact in Business Terms section) are well aligned with the real value drivers of the enterprise, relevant risk scenarios will be developed.
- A bottom-up approach, where a list of generic scenarios is used to define a set of more concrete and customised scenarios, applied to the individual enterprise situation

Figure 37—IT Risk Scenario Development



The approaches are complementary and should be used simultaneously. Indeed, risk scenarios must be relevant and linked to real business risk. On the other hand, using a set of example generic risk scenarios helps to ensure that no risks are overlooked and provides a more comprehensive and complete view of IT risk.

In practice, the following approach is suggested:

- Use the list of example generic risk scenarios to define a (manageable) set of concrete risk scenarios for the enterprise⁷. In determining a ‘manageable’ set of scenarios a business might begin by considering commonly occurring scenarios in its industry or product area, scenarios representing threat sources that are increasing in number or severity, and scenarios that involve legal and regulatory requirements applicable to the business. Also, some less common situations should be included in the scenarios.
- Perform a validation against the business objectives of the entity. Do the selected risk scenarios address potential impacts on achievement of business objectives of the entity, in support of the overall enterprise’s business objectives?
- Refine the selected scenarios based on this validation; detail them to a level in line with the criticality of the entity⁸.
- Reduce the number of scenarios to a manageable set. ‘Manageable’ does not signify a fixed number, but should be in line with the overall importance (size) and criticality of the unit. There is no general rule, but if scenarios are reasonably and realistically scoped, the enterprise should expect to develop at least a few dozen scenarios.
- Keep all risks in a list so they can be re-evaluated in the next iteration and included for detailed analysis if they have become relevant at that time.
- Include in the scenarios an unspecified event; how to address an incident not covered by other scenarios.

Once the set of risk scenarios is defined, it can be used for risk analysis. In risk analysis, as explained in other sections of this guide, frequency and impact of the scenario are assessed. Important components of this assessment are the risk factors.

A reminder—do not over-rely on the list of example generic risk scenarios. The list, although quite comprehensive, broad and covering most potential risks, needs to be adapted to the enterprise’s specific situation. It is not intended that, going forward, all IT risk management will use the same set of predefined IT risk scenarios. Rather, it is encouraged that this list be used as basis for the development of specific, relevant scenarios.

⁷ It is not recommended that hundreds of detailed risk scenarios be defined for non-critical units or if there is only a very immature risk management capability in the entity. ‘Immature’ in this context is about not fully understanding the real threats to real operations and about avoidance of trying to understand and identify IT risk.

⁸ Critical entities deserve to have risk scenarios defined at a detailed level; non-critical entities can do with quite generic scenarios, not elaborated in too much detail. Note that the entity can be an organisational unit, but can also be something cross-organisational, e.g., a grouping of similar business processes and activities.

Risk Factors

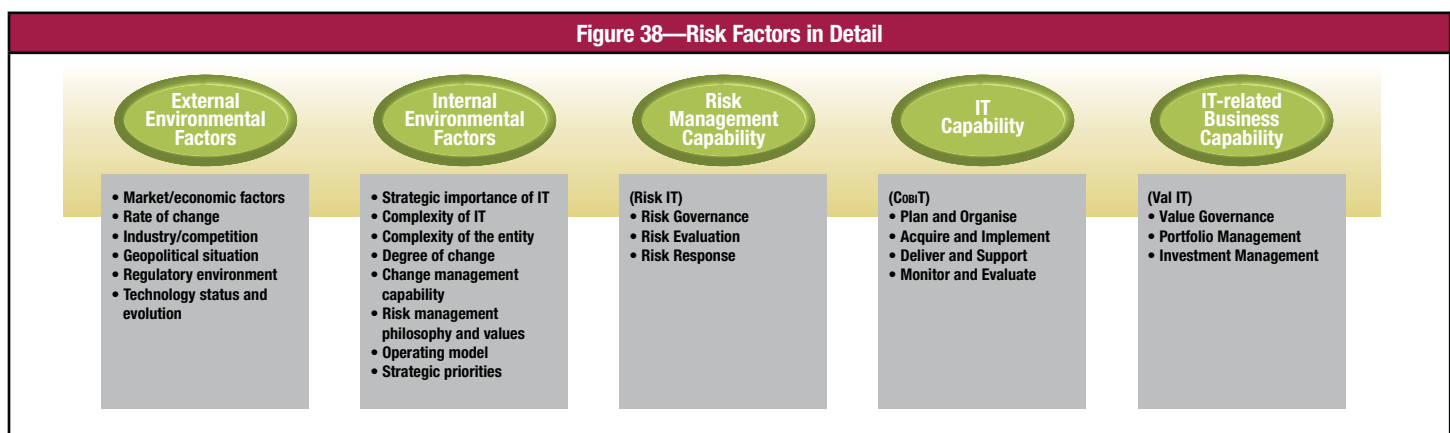
Risk factors are those factors that influence the frequency and/or business impact of risk scenarios. They can be of different natures and can be classified in two major categories:

- Environmental factors, which can be divided into internal and external factors—the difference being the degree of control an enterprise has over them:
 - Internal environmental factors are, to a large extent, under the control of the enterprise, although they may not always be easy to change.
 - External environmental factors are, to a large extent, outside the control of the enterprise.
- Capabilities, i.e., how good the enterprise is in a number of IT-related activities. They can be distinguished in line with ISACA's three major frameworks:
 - IT risk management capabilities—To what extent the enterprise is mature in performing the risk management processes defined in the Risk IT framework
 - IT capabilities—How good the IT processes are as defined in COBIT
 - IT-related business capabilities (or value management), expressed through the Val IT processes

The importance of risk factors lies in the influence they have on the IT risk. They are heavy influencers of the frequency and impact of IT scenarios and should be taken into account during every risk analysis, when frequency and impact are assessed.

Risk factors can also be interpreted as causal factors of the scenario that is materialising, or as vulnerabilities or weaknesses. These are terms often used in other risk management frameworks. Scenario analysis should cover threats and vulnerabilities, and should not only be based on past experience and known current events, but should equally look forward to possible future circumstances.

Figure 38 depicts risk factors, which are discussed in more detail in the following paragraphs.



External Environmental Factors

Environmental IT risk factors, i.e., those circumstances that can increase the frequency or impact of an event **and** which are not always directly controllable by the enterprise⁹, include:

- Market/economic factors—The industry sector in which the enterprise operates, i.e., operating in the financial sector requires different IT requirements and IT capabilities than operating in a manufacturing environment. Other economic factors can be included as well, e.g., nationalisation, mergers and acquisitions, consolidations.
- Rate of change in the market in which the enterprise operates—Are business models changing fundamentally? Is the product or service at the end of an important life-cycle moment?
- Competitive environment in which the enterprise operates
- Geopolitical situation—Is the geographic location subject to frequent natural disasters? Does the local political and overall economic context represent an additional risk?
- Regulatory environment—Is the enterprise subject to new or more strict IT-related regulations or regulations impacting IT? Are there any other compliance requirements beyond regulation (e.g., industry-specific, contractual)?
- Technology status and evolution—Is the enterprise using state-of-the art technology and, more important, how fast are relevant technologies evolving?

⁹ Some environmental factors are controllable in theory (e.g., operating model), but are so pervasive and impractical to handle in practice that they can safely be considered as a 'given' rather than as a variable. This is true for many internal environmental factors; external environmental factors usually are a given.

Internal Environmental Factors

Internal risk factors include:

- Strategic importance of IT in the enterprise—Is IT a strategic differentiator, a functional enabler or a supporting function?
- Complexity of IT—Is IT highly complex (e.g., complex architecture, recent mergers) or is IT simple, standardised and streamlined?
- Complexity of the enterprise, including geographic spread and value chain coverage, e.g., in a manufacturing environment—Does the enterprise manufacture and distribute parts, and/or is it also doing assembly activities?
- Degree of change the enterprise is experiencing
- Change management capability—To what extent is the enterprise capable of organisational change?
- The risk management philosophy of the enterprise (risk averse or risk taking) and, linked with that, the values of the enterprise
- Operating model, i.e., the degree to which the enterprise operates independently or is connected to its clients/suppliers, the degree of centralisation/decentralisation
- Strategic priorities of the enterprise

Risk Management Capability

Risk management capability is an indication of how well the enterprise is executing the core risk management processes, as described in the Risk IT framework. The better executed or more mature the processes, the more capable the risk management programme.

This factor is correlated with the capability of the enterprise to recognise and detect risks and adverse events; hence, it should not be neglected. Risk management capability is a very significant element in the frequency and impact of risk events in an enterprise because it is responsible for management's risk decisions (or lack thereof), as well as for the presence, absence and/or effectiveness of controls that exist within an enterprise.

Risk management capability is also an important component of the overall risk profile of the organisation (see chapter 3, Risk Profiles section).

IT Capability

In the context of risk management and the Risk IT framework on how to achieve this, IT capabilities are associated with the maturity level of IT processes and IT controls. The COBIT framework provides substantial guidance. Mature and well-controlled IT processes are equivalent to high IT capabilities, which can have a positive influence on:

- Reducing the frequency of events, e.g., having good software development processes in place to deliver high-quality and stable software, or having good security measures in place to reduce the number of security-related incidents
- Reducing the business impact when events happen, e.g., having a good BCP/DRP in place when disaster strikes

The following sections provide additional detail about the link between IT capability and risk:

- Chapter 5, Capability Risk Factors in the Risk Analysis Process section, maps the different processes within COBIT and Val IT with risk scenarios, indicating which processes are risk factors (influence impact and/or frequency) for risk scenarios.
- Chapter 8 maps the risk scenarios against specific control objectives (COBIT) or management practices (Val IT) to indicate which of them can help mitigate each risk scenario.

The IT sourcing model is often seen as a separate risk factor. There is no doubt that the sourcing model, e.g., keeping IT in-house or outsourcing parts or complete IT departments, has an important impact on risk and on how to measure it. However, the COBIT process model contains several processes dealing with the selection and management of sourcing models, so this issue is considered as part of the overall IT capability.

IT-related Business Capability

The degree to which business management is capable of managing the direction and performance of IT is an important risk factor. Val IT defines a number of processes and practices aimed at managing value generated by IT for the entire enterprise. In the context of the Risk IT framework, mature IT value management processes are associated with a high capability of the business to manage IT-related affairs.

Indeed, if the business is capable of making the right IT investments, if correct IT partners are selected and if programmes are well selected and managed, the enterprise will generate more value from IT and will miss fewer opportunities.

Referring back to **figure 6**, and to the three risk categories, IT-related business capability is especially a risk factor in the risks in the IT benefit/value enablement category.

IT Risk Scenarios

An IT risk scenario is a description of an IT-related event that can lead to a business impact, when and if it should occur. For risk scenarios to be complete and usable for risk analysis purposes, they should contain the following components, as shown in **figure 39**:

- Actor who generates the threat—Actors can be internal or external and they can be human or non-human:
 - Internal actors are within the enterprise, e.g., staff, contractors.
 - External actors include outsiders, competitors, regulators and the market.

Not every type of threat requires an actor, e.g., failures or natural causes.

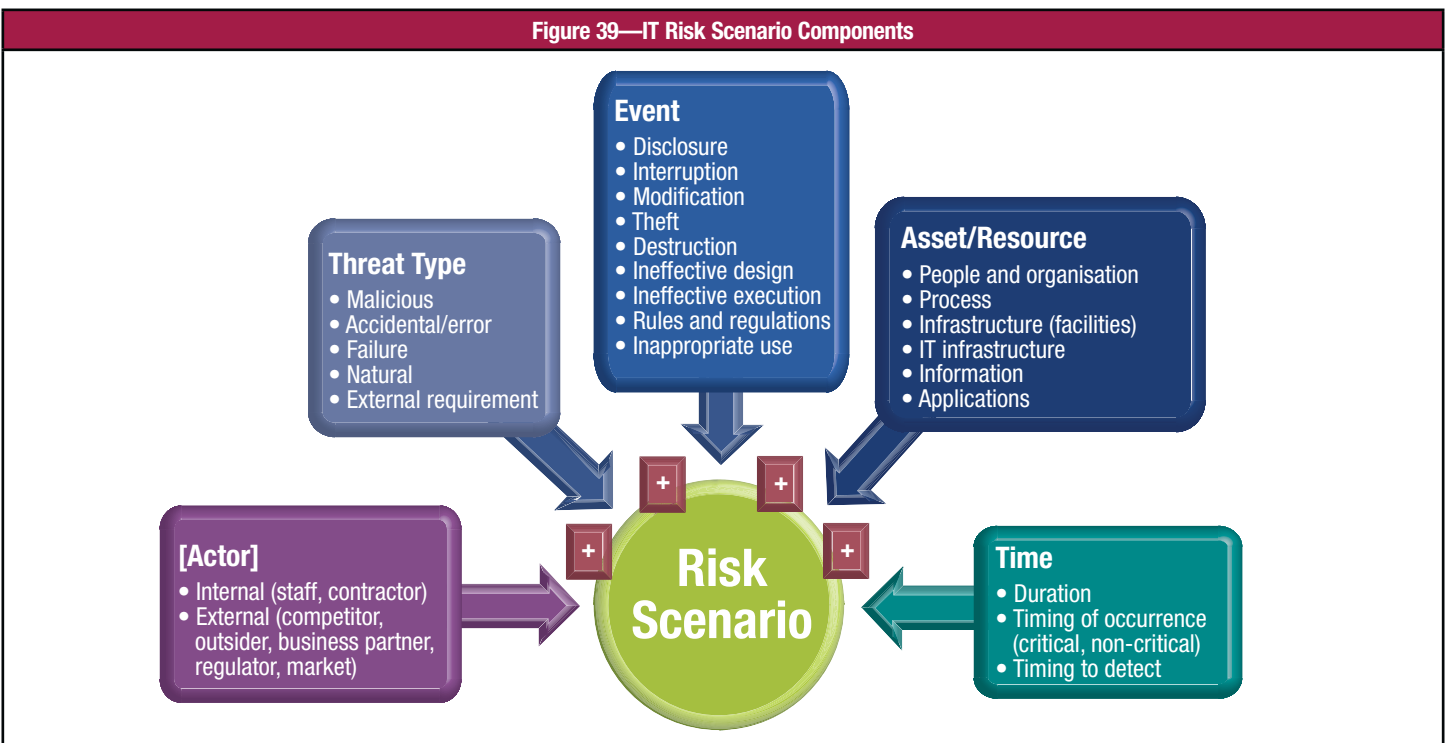
- Threat type (the nature of the event)—Is it malicious? If not, is it accidental or is it a failure of a well-defined process? Is it a natural event?

- An event—Is it disclosure (of confidential information), interruption (of a system, of a project), theft or destruction? Action also includes ineffective design (of systems, processes, etc.) or ineffective execution of processes (e.g., change management procedures, acquisition procedures, project prioritisation processes).
- An asset/resource (on which the scenario acts)—An asset is any object of value to the enterprise that can be affected by the event and lead to business impact. A resource is anything that helps to achieve IT goals. Assets and resources can be identical, e.g., IT hardware is an important resource because all IT applications use it, and at the same time, it is an asset because it has a certain value to the enterprise. Assets/resources include:
 - People and organisation
 - IT processes, e.g., modelled as COBIT or Val IT processes, or business processes
 - Physical infrastructure, facilities, equipment, etc.
 - IT infrastructure, including computing hardware, network infrastructure, middleware
 - Other enterprise architecture components, including:
 - Information
 - Applications

Assets can be critical or not, e.g., a client-facing web site of a major bank compared to the web site of the local garage or the intranet of the software development group. Critical resources will probably attract a greater number of attacks or greater attention on failure; hence, the frequency of related scenarios will probably be higher. It takes skill, experience and thorough understanding of dependencies to understand the difference between a critical asset and a non-critical asset.

- Timing dimension, where the following could be described, if relevant to the scenario:
 - The duration of the event (extended outage of a service or data centre)
 - The timing (Does the event occur at a critical moment?)
 - Time lag between the event and consequence (Is there an immediate consequence, e.g., network failure, immediate downtime, or a delayed consequence, e.g., wrong IT architecture with accumulated high costs over a time span of several years?)

It is important to stay aware of the differences between loss events, threat events and vulnerability events. When a risk scenario materialises, a loss event occurs. The loss event has been triggered by a threat event (threat plus event in **figure 39**). Frequency and impact of the threat event leading to a loss event are influenced by the risk factors or vulnerability. Vulnerability is usually a state or can be increased/decreased by vulnerability events, e.g., the weakening of controls. One should not mix these three types of events into one big ‘risk list’.



Referring back to the three broad categories of risk defined in the Risk IT framework (see **figure 6**), all risk scenarios can be classified under one (or more) of these categories:

- IT benefit/value enablement risk—Associated with (missed) opportunities to use technology to improve efficiency or effectiveness of business processes, or to use technology 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. This ties to portfolio management (as described in the Val IT framework).
- IT operation and service delivery risk—Associated with the operational stability, availability, protection and recoverability of IT services and can bring destruction or reduction of value to the enterprise

A following section, Example Risk Scenarios, defines a list of example generic risk scenarios and how they are classified into these three categories.

Scenario Development

The use of scenarios is key to risk management and the technique is applicable to any enterprise. Each enterprise needs to build a set of scenarios (containing the components described previously) as a starting point to conduct its risk analysis.

Building a scenario means, in theory, that each possible value of every component is combined. Each combination should then be assessed for relevance and realism and, if found to be relevant, entered into the risk register. In practice, this is, of course, not possible, e.g., a situation with 20 major applications supported by three major technology platforms. The number of theoretically possible scenarios already approaches 100,000, which is not feasible to maintain. The number of scenarios to be developed and analysed should be kept to a much smaller number in order to remain manageable since every possible combination cannot be retained.

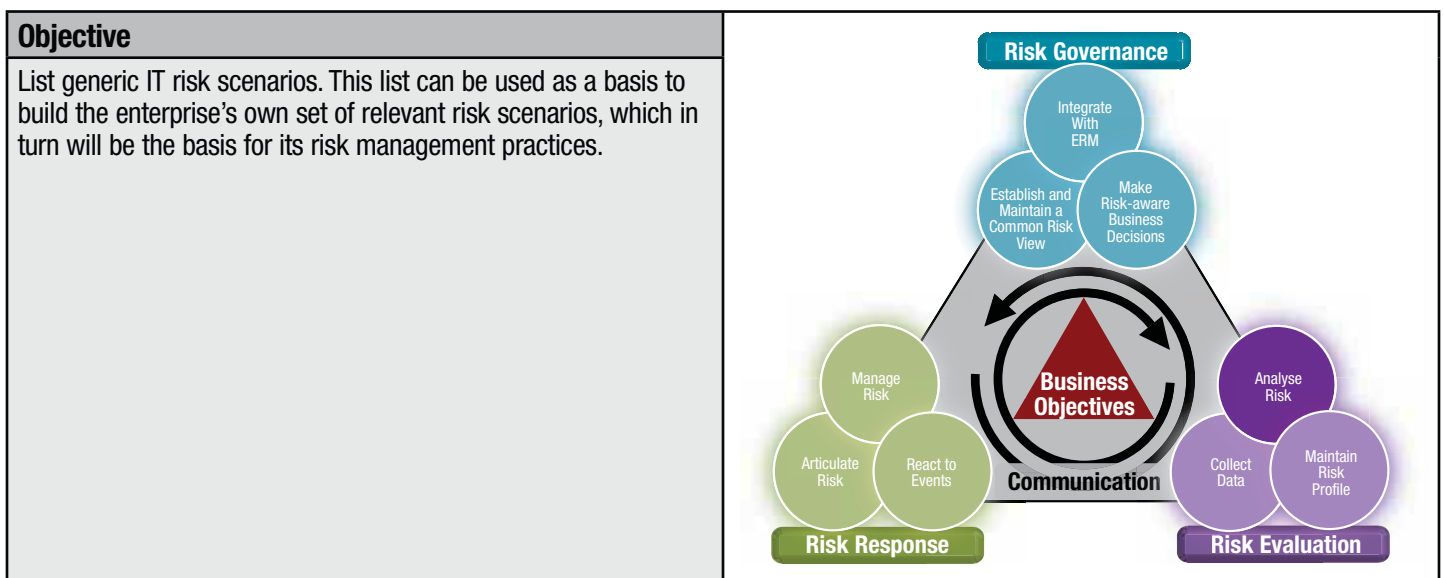
Some guidance and considerations for the development and maintenance of manageable numbers of relevant scenarios follow:

- Risk factors and the enterprise change over time; hence, scenarios will change over time, over the course of a project or over the evolution of technology. For example, it is essential that the CRO develop a schedule and the CIO work with the business lines to review and update scenarios for relevance and importance as dictated by the pace of change. Frequency of this exercise depends on the overall risk profile of the entity and should be done at least on an annual basis, or when important changes occur.
- The number of imaginable scenarios is possibly infinite and, as explained previously, good risk management cannot include infinite lists. One technique of keeping the number of scenarios manageable is to propagate a standard set of generic scenarios through the enterprise (see the following Example Risk Scenarios section) and develop more detailed and concrete scenarios when required and warranted by the risk profile only at lower (entity) levels. The assumptions made when grouping or generalising should be well understood by all and adequately documented because they may hide certain risks or be confusing when looking at risk response, e.g., if ‘insider threat’ is not well defined within a scenario, then it may not be clear whether this threat includes privileged and non-privileged insiders. The differences between these aspects of a scenario can be critical when one is trying to understand the frequency and magnitude of events (their significance), as well as control opportunities.
- Risk management helps to deal with the enormous complexity of today’s IT environments by prioritising potential action according to its value in mitigating risk. Risk management is about reducing complexity, not generating it, hence another plea for working with a manageable number of risk scenarios. However, the retained number of scenarios still needs to accurately reflect realistic and relevant scenarios.
- There should be a sufficient number of risk scenario scales reflecting the complexity of the enterprise and the extent of exposures to which the enterprise is subject.
- Similarly, for risk reporting purposes, entities should not report upon all specific and detailed scenarios, but could do so by using the generic risk structure. For example, an entity may have taken generic scenario 15 (project quality), translated it into five scenarios for its major projects, subsequently conducted a risk analysis for each of the scenarios, then aggregated or summarised the results and reported back using the generic scenario header ‘project quality’.
- Developing a manageable and relevant set of risk scenarios requires:
 - Expertise and experience, to not overlook relevant scenarios and not be drawn into highly unrealistic¹⁰ or irrelevant scenarios. While the avoidance of scenarios that are unrealistic or irrelevant is important in properly utilising limited resources, some attention should be paid to situations that are highly infrequent and unpredictable, but which could have a cataclysmic impact on the enterprise.
 - A thorough understanding of the environment. This includes the IT environment (e.g., infrastructure, applications, dependencies between applications, infrastructure components), the overall business environment, and an understanding of how and which IT environments support the business environment to understand the business impact.
 - The intervention and common views of all parties involved—senior management, which has the decision power; business management, which has the best view on business impact; IT, which has the understanding of what can go wrong with IT; and risk management, which can moderate and structure the debate amongst the other parties. The process of developing scenarios usually benefits from a brainstorming/workshop approach. In such a setting, a high-level assessment is usually required to reduce the number of scenarios to a manageable, but relevant and representative, number.
- Scenario analysis is not just an analytical exercise involving ‘risk experts’. Scenario analysis does indeed provide analysis outputs, but a significant benefit of scenario analysis is achieving organisational buy-in from enterprise entities and business lines, risk management, IT, finance, compliance and other parties. Gaining this buy-in is the reason why scenario analysis should be a carefully facilitated process.
- In addition to co-ordinating with management, it is recommended that selected members of the staff who are familiar with the detailed operations be included in discussions, where appropriate. Staff are often more familiar with vulnerabilities in technology and processes that can be exploited.
- When developing scenarios, worst-case events should not be included because they rarely materialise, whereas less-severe incidents happen more often.
- *The Risk IT Framework* discusses the upside of risk, including some of the opportunities generating positive impact that should be considered as well in the scenario list. (See the Example Risk Scenarios section for examples.)

¹⁰ Unrealistic signifies not fixed in time or static. What used to be unthinkable, mainly because it never happened or because it happened too long ago, becomes realistic as soon as it occurs again. A striking example are the 11 September 2001 terrorist attacks in the US. It is human nature for things that have not yet happened, even when they are theoretically possible, to be estimated as not possible or extremely unlikely. Only when they occur will they be taken seriously in risk assessments. This may be regarded as lack of foresight or lack of due care, but it is actually the essence of risk management—trying to shape and contain the future based on past experience and future predictions.

- Simple scenarios, once developed, should be further developed into more complex scenarios, showing cascading and/or coincidental impacts and reflecting dependencies. For example:
 - A scenario of having a major hardware failure can be combined with the scenario of failed DRP.
 - A scenario of major software failure can trigger database corruption and, in combination with poor data management backups, can lead to serious consequences, or at least consequences of a different magnitude than a software failure alone.
 - A scenario of internal apathy to a major external event
- Attention should be paid to so-called ‘systemic’ and/or ‘contagious’ risk scenarios:
 - Contagious—Events that happen at several of the enterprise’s business partners within a very short time frame. An example would be a clearinghouse that can be fully prepared for any sort of emergency by having very sophisticated disaster recovery measures in place, but when a catastrophe happens finds that no transactions are sent by their providers and hence is temporarily out of business.
 - Systemic—Something happens with an important business partner, affecting a large group of enterprises within an area or industry. An example would be a nationwide air traffic control system that goes down for an extended period of time (six hours), affecting air traffic on a very large scale.
- Scenario development is instrumental in understanding risk and will also help to address the issue of detectability. It is an important step in moving away from a situation where the enterprise ‘does not know what it does not know’. Indeed, the collaborative approach for scenario development assists in identifying risks to which the enterprise, until then, would not have realised it was subject to (and hence would never have thought of putting in place any countermeasures). Once the full set of risks is identified during scenario generation, risk analysis will assess frequency and magnitude of the scenarios. Questions to be asked include: Will the enterprise ever detect that the risk scenario has materialised? Will the enterprise notice something has gone wrong so it can react appropriately? Generating scenarios and creatively thinking of what can go wrong will automatically raise (and, hopefully, cause response to) the question of detectability.
- Detectability of scenarios includes two steps: visibility and recognition. The enterprise must be in a position that it can observe anything going wrong, and it needs the capability to recognise an observed event as something wrong.

Example Risk Scenarios



This chapter contains a set of generic IT risk scenarios, built in line with the model described in the previous section of this guide. The set of generic scenarios contains examples of negative outcomes, but also examples where a risk, when managed well, can lead to a positive outcome.

A word of warning: **Figure 40** does not replace the creative and reflective phase that every scenario-creating exercise should contain. In other words, it is not recommended that an enterprise blindly use this list and assume that no other risk scenarios are possible, or assume that every scenario contained in the list is applicable to the enterprise. Intelligence and experience are needed to derive a relevant and customised list of scenarios starting from this generic list.

Figure 40 is a table including the following information:

- High-level risk scenario—High-level description of the type of scenario (e.g., IT project selection). In total there are 36 high-level scenarios.
- Risk scenario components—Five columns indicating some possible components for each of the five components of a risk scenario (e.g., for scenario 18, destruction of infrastructure, the threat type can be accidental or malicious, leading to two different scenarios). Multiple values are possible in some of the columns, e.g., events can happen at non-critical times or at very critical times.

- The risk category—The category to which scenarios derived from this generic scenario will fit, using the three risk categories explained in *The Risk IT Framework*:
 - IT benefit/value enablement risk—Associated with (missed) opportunities to use technology to improve the 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. This ties to investment portfolio management (as described in the Val IT framework).
 - IT operations and service delivery risk—Associated with the operational stability, availability, protection and recoverability of IT services, which can bring destruction or reduction of value to the enterprise.
- A ‘P’ indicates a primary (higher degree) fit and an ‘S’ a secondary (lower degree) fit.
- Example scenarios with a negative outcome—For each high-level scenario, one or several small examples are given of scenarios with a negative outcome, indicating whether the outcome is more of a value destruction or a failure to gain value (either the column ‘Fail to Gain’ or ‘Lose Value’ will be highlighted). In total, 72 generic risk scenarios are included with possible negative outcomes.
- Example scenarios with a positive outcome—These indicate whether they are about value preservation or value generation by highlighting the ‘Gain Value’ or ‘Preserve Value’ column.

For the remainder of this section (and the following sections), only generic scenarios will be used since specific scenarios can be easily deduced.

As defined in the Risk Scenarios section, an IT risk scenario is a description of an IT-related event that can lead to a business impact, when and if it should occur. Hence, the generic scenarios will, once customised, serve as input to risk analysis activities, where the ultimate business impact (amongst others) needs to be established. The Expressing Impact in Business Terms section of chapter 4 presents a number of techniques and options for translating IT risks into business terms.

Example:

Scenario 2, New technologies in **figure 40**, is an example of ‘failure to adopt and exploit new technologies on a timely basis’. Making this specific for a telecommunication company, an illustration could be failure to adopt and exploit a technology such as data mining, which enables the detection of new trends in customer usage behaviour. Using the extended BSC criteria as described in the Introduction section of chapter 4 as the approach, the business impacts could include customer satisfaction (individual customers may be less well served if trends are not detected) and profit (growth) since more profitable price plans will not be introduced.

Figure 40—Generic IT Risk Scenarios

#	High-level Risk Scenario	Risk Scenario Components						Risk Category/Group		Risk		Risk Consequence		Risk		Risk Consequence	
		Actor	Threat Type	Event	Asset/Resources	Time	IT Benefit/Value Enablement	IT Programme and Project Delivery	IT Operations and Service Delivery	Negative Example Scenarios	Fail to Gain	Lose Value	Positive Example Scenarios	Gain Value	Preserve Value		
1	IT programme selection	Internal	Failure	Ineffective execution	Process (portfolio management)	Timing (non-critical) Duration (extended) Detection (slow)	P	S	<ul style="list-style-type: none"> Wrong programmes selected for implementation, misaligned with corporate strategy and priorities Duplication amongst different initiatives New important programme creates long-term incompatibility with the enterprise architecture 	Fail to Gain	Lose Value	<ul style="list-style-type: none"> Programmes leading to successful new business initiatives selected for execution 	Gain Value	Preserve Value			
2	New technologies	Internal	Failure	Ineffective design	Process (technology selection) Enterprise architecture (technology)	Timing (non-critical) Duration (extended) Detection (slow)	P	S	<ul style="list-style-type: none"> Failure to adopt and exploit new technologies (i.e., functionality, optimisation) on a timely basis New and important technology trends not identified Inability to use the technology to realise desired outcomes (e.g., failure to make required business model or organisational changes) 	Fail to Gain	Lose Value	<ul style="list-style-type: none"> New technologies for new initiatives or more efficient operations adopted and exploited 	Gain Value	Preserve Value			

Figure 40—Generic IT Risk Scenarios (cont.)

#	High-level Risk Scenario	Risk Scenario Components				Risk Category/Group			Risk		Risk Consequence					
		Actor	Threat Type	Event	Asset/Resources	Time	IT Benefit/Value Enablement	IT Programme and Project Delivery	IT Operations and Service Delivery	Negative Example Scenarios	Fail to Gain	Lose Value	Positive Example Scenarios	Gain Value	Risk	Risk Consequence
3	Technology selection	Internal	Failure	Ineffective execution	Process (technology selection) Enterprise architecture (technology)	Timing (non-critical) Duration (extended) Detection (slow)	P		S	Negative Example Scenarios	Fail to Gain	Lose Value	Positive Example Scenarios	Gain Value		Preserve Value
4	IT investment decision making	Internal	Failure	Ineffective execution	Process (investment management) People and organisation	Timing (non-critical) Duration (extended) Detection (slow)	P		S	Negative Example Scenarios	Fail to Gain	Lose Value	Positive Example Scenarios	Gain Value		Preserve Value
5	Accountability over IT	Internal	Failure	Ineffective execution	Process (define the IT processes, organisation and relationships) People and organisation	Timing (non-critical) Duration (extended) Detection (moderate)	P		S	Negative Example Scenarios	Fail to Gain	Lose Value	Positive Example Scenarios	Gain Value		Preserve Value
6	Integration of IT within business processes	Internal	Failure	Ineffective execution	Process (define the IT processes, organisation and relationships) People and organisation	Timing (non-critical) Duration (extended) Detection (moderate)	P		S	Negative Example Scenarios	Fail to Gain	Lose Value	Positive Example Scenarios	Gain Value		Preserve Value

Figure 40—Generic IT Risk Scenarios (cont.)

#	High-level Risk Scenario	Risk Scenario Components					Risk Category/Group			Risk		Risk Consequence		
		Actor	Threat Type	Event	Asset/Resources	Time	IT Benefit/Value Enablement	IT Programme and Project Delivery	IT Operations and Service Delivery	Negative Example Scenarios	Fail to Gain	Lose Value	Positive Example Scenarios	Gain Value
7	State of infrastructure technology	Internal	Failure	Ineffective design	Process (acquire and maintain technology infrastructure enterprise architecture (technology))	Timing (non-critical) Duration (extended) Detection (slow)	S	S	S	<ul style="list-style-type: none"> IT technology in use is obsolete and cannot satisfy new business requirements (e.g., networking, security, storage) 	Fail to Gain	<ul style="list-style-type: none"> Modern and stable technology used 	Gain Value	Preserve Value
8	Ageing of application software	Internal	Failure	Ineffective execution	Process (acquire and maintain technology infrastructure enterprise architecture (applications))	Timing (non-critical) Duration (extended) Detection (slow)	P	P	P	<ul style="list-style-type: none"> Old application software (e.g., old technology, poorly documented, expensive to maintain, difficult to extend, not integrated in current architecture) 	Fail to Gain	<ul style="list-style-type: none"> Modern application software, easy to add new process functionality 	Gain Value	Preserve Value
9	Architectural agility and flexibility	Internal	Failure	Ineffective design	Process (determine technological direction) Enterprise architecture	Timing (non-critical) Duration (extended) Detection (slow)	P	S	S	<ul style="list-style-type: none"> Complex and inflexible IT architecture obstructing further evolution and expansion 	Fail to Gain	<ul style="list-style-type: none"> Modern and flexible architecture supports business agility/innovation 	Gain Value	Preserve Value
10	Regulatory compliance	Internal	Failure Malicious	Regulation	Process (ensure compliance with external requirements)	Timing (non-critical) Duration (extended) Detection (slow)	P	S	S	<ul style="list-style-type: none"> Non-compliance with regulations (e.g., accounting, manufacturing) 	Fail to Gain	Gain Value	Gain Value	Preserve Value

Figure 40—Generic IT Risk Scenarios (cont.)

#	High-level Risk Scenario	Risk Scenario Components				Risk Category/Group			Risk Consequence		Risk		Risk Consequence		
		Actor	Threat Type	Event	Asset/Resources	Time	IT Benefit/Value Enablement	IT Programme and Project Delivery	IT Operations and Service Delivery	Negative Example Scenarios	Fail to Gain	Lose Value	Positive Example Scenarios	Gain Value	Preserve Value
11	Software implementation	Internal	Failure	Ineffective execution	Process (enable operation and use) Enterprise architecture (applications)	Timing (non-critical) Duration (moderate) Detection (instant)		P		Operational glitches when new software is made operational Users not prepared to use and exploit new application software					
12	IT project termination	Internal	Failure	Ineffective execution	Process (retire the programme)	Timing (critical) Duration (extended) Detection (Slow)		P		Failing (due to cost, delays, scope creep, changed business priorities) projects not terminated			<ul style="list-style-type: none"> Failing or irrelevant projects stopped on a timely basis 		
13	IT project economics	Internal	Failure	Ineffective execution	Process (monitor and report on the programme)	Timing (non-critical) Duration (extended) Detection (slow)		P		Isolated IT project budget overrun Consistent and important IT projects budget overruns Absence of view on portfolio and project economics			<ul style="list-style-type: none"> IT project completed within agreed-upon budgets 		
14	Project delivery	Internal	Failure	Ineffective execution	Process (monitor and report on the programme)	Timing (non-critical) Duration (extended duration) Detection (slow)	S	P	S	Occasional late IT project delivery by internal development department Routinely important delays in IT project delivery Excessive delays in outsourced IT development project			<ul style="list-style-type: none"> Project delivery on time 		

Figure 40—Generic IT Risk Scenarios (cont.)

#	High-level Risk Scenario	Risk Scenario Components						Risk Category/Group			Risk		Risk Consequence		
		Actor	Threat Type	Event	Asset/Resources	Time	IT Benefit/Value Enablement	IT Programme and Project Delivery	IT Operations and Service Delivery	Negative Example Scenarios	Fail to Gain	Lose Value	Positive Example Scenarios	Gain Value	Preserve Value
15	Project quality	Internal	Failure	Ineffective execution	Process (monitor and report on the programme)	Timing (non-critical) Duration (extended) Detection (slow)	P			<ul style="list-style-type: none"> Insufficient quality of project deliverables (due to software, documentation, compliance with functional requirements) 	Fail to Gain	Lose Value	<ul style="list-style-type: none"> Project delivers to specifications 	Gain Value	Preserve Value
16	Selection/performance of third-party suppliers	Internal	Failure	Ineffective design	Process (manage third-party services) People and organisation	Timing (non-critical) Duration (extended) Detection (slow)	S	P	<ul style="list-style-type: none"> Inadequate support and services delivered by vendors, not in line with service level agreements (SLAs) Inadequate performance of outsourcer in large-scale long-term outsourcing arrangement 			<ul style="list-style-type: none"> Third party acting as strategic partner 			
17	Infrastructure theft	Internal External	Malicious	Theft	Infrastructure	Timing (unknown) Duration (extended) Detection (instant)	S	P	<ul style="list-style-type: none"> Theft of laptop with sensitive data Theft of substantial number of development servers 						
18	Destruction of infrastructure	Internal External	Accidental Malicious	Destruction Inappropriate use	Infrastructure	Timing (unknown) Duration (extended) Detection (instant)	S	P	<ul style="list-style-type: none"> Destruction of data centre (due to sabotage, etc.) Accidental destruction of individual laptops 						

Figure 40—Generic IT Risk Scenarios (cont.)

#	High-level Risk Scenario	Risk Scenario Components				Risk Category/Group			Risk		Risk Consequence		Risk		Risk Consequence	
		Actor	Threat Type	Event	Asset/Resources	Time	IT Benefit/Value Enablement	IT Programme and Project Delivery	IT Operations and Service Delivery	Negative Example Scenarios	Fail to Gain	Lose Value	Positive Example Scenarios	Gain Value	Preserve Value	
19	IT staff	Internal	Failure	Ineffective execution	Process (manage IT human resources) People and organisation	Timing (unknown) Duration (extended) Detection (moderate)	P	P	P	<ul style="list-style-type: none"> Departure or extended unavailability of key IT staff Key development team leaves the enterprise Inability to recruit IT staff 						
20	IT expertise and skills	Internal	Failure	Ineffective design	Process (manage IT human resources) People and organisation	Timing (unknown) Duration (extended) Detection (instant)	P	P	P	<ul style="list-style-type: none"> Lack or mismatch of IT-related skills within IT (e.g., due to new technologies) Lack of business understanding by IT staff 			<ul style="list-style-type: none"> Attracting the appropriate staff increases the service delivery of the IT department Correct staff and skill mix will support project delivery and value 			
21	Software integrity	Internal External	Accidental Malicious	Modification	Process (manage changes and install solutions and changes) Enterprise architecture (software)	Timing (non-critical) Duration (short) Detection (slow)		S	P	<ul style="list-style-type: none"> Intentional modification of software leading to wrong data or fraudulent actions Unintentional modification of software leading to unexpected results Unintentional configuration and change management errors 						

Figure 40—Generic IT Risk Scenarios (cont.)

#	High-level Risk Scenario	Risk Scenario Components					Risk Category/Group			Risk		Risk Consequence		
		Actor	Threat Type	Event	Asset/Resources	Time	IT Benefit/Value Enablement	IT Programme and Project Delivery	IT Operations and Service Delivery	Negative Example Scenarios	Fail to Gain	Lose Value	Positive Example Scenarios	Gain Value
22	Infrastructure (hardware)	Internal External	Accidental Malicious	Modification Destruction Inappropriate use	Infrastructure	Timing (non-critical) Duration (unknown) Detection (instant)		P		<ul style="list-style-type: none"> • Erroneous misconfiguration of hardware components • Damage of critical servers in computer room (e.g., due to accident) • Intentional tampering with hardware (e.g., security devices) 				
23	Software performance	Internal	Failure	Ineffective design	Enterprise architecture (applications)	Timing (non-critical) Duration (unknown) Detection (instant)	S	P		<ul style="list-style-type: none"> • Regular software malfunctioning of critical application software • Intermittent software problems with important system software 				
24	System capacity	Internal	Failure	Ineffective design	Enterprise architecture (technology)	Timing (non-critical) Duration (unknown) Detection (instant)	S	P		<ul style="list-style-type: none"> • Systems cannot handle transaction volumes when user volumes increase • Systems cannot handle system load when new applications or initiatives are deployed 				
25	Ageing of infrastructural software	Internal	Failure	Ineffective design	Process (acquire and maintain technology infrastructure)	Timing (non-critical) Duration (unknown) Detection (instant)		P		<ul style="list-style-type: none"> • Unsupported versions of operating system software still in use • Old database system still used 				

Figure 40—Generic IT Risk Scenarios (cont.)

#	High-level Risk Scenario	Risk Scenario Components					Risk Category/Group			Risk		Risk Consequence			
		Actor	Threat Type	Event	Asset/Resources	Time	IT Benefit/Value Enablement	IT Programme and Project Delivery	IT Operations and Service Delivery	Risk	Risk	Fail to Gain	Lose Value	Positive Example Scenarios	Gain Value
26	Malware	Internal External	Accidental Malicious	Ineffective design Inappropriate use	Process (ensure systems security) Enterprise architecture (applications)	Timing (non-critical) Duration (unknown) Detection (instant)	S	P	P	Negative Example Scenarios	Fail to Gain	Lose Value	Positive Example Scenarios	Gain Value	Preserve Value
27	Logical attacks	Internal External	Malicious	Ineffective design Inappropriate use	Process (ensure systems security) Enterprise architecture (applications)	Timing (non-critical) Duration (unknown) Detection (instant)	S	P	P	Negative Example Scenarios	Fail to Gain	Lose Value	Positive Example Scenarios	Gain Value	Preserve Value
28	Information media	Internal	Failure	Ineffective execution	Process (manage data) Enterprise architecture (information)	Timing (non-critical) Duration (unknown) Detection (instant)	S	S	P	Negative Example Scenarios	Fail to Gain	Lose Value	Positive Example Scenarios	Gain Value	Preserve Value
29	Utilities performance	Internal	Failure	Interruption	Process (manage third-party services) Infrastructure	Timing (unknown) Duration (unknown) Detection (instant)		P	P	Negative Example Scenarios	Fail to Gain	Lose Value	Positive Example Scenarios	Gain Value	Preserve Value

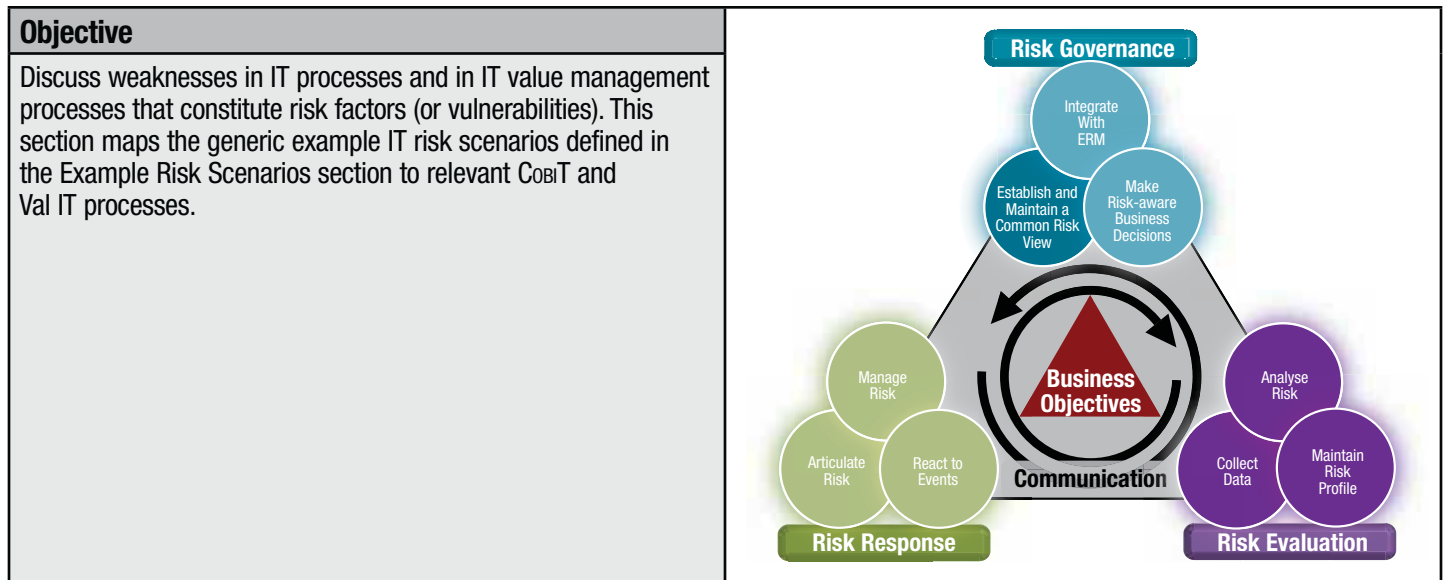
Figure 40—Generic IT Risk Scenarios (cont.)

#	High-level Risk Scenario	Risk Scenario Components					Risk Category/Group			Risk		Risk Consequence		
		Actor	Threat Type	Event	Asset/Resources	Time	IT Benefit/Value Enablement	IT Programme and Project Delivery	IT Operations and Service Delivery	Risk	Risk	Risk Consequence	Risk Consequence	
30	Industrial action	External	Malicious	Interruption	People and organisation	Timing (unknown) Duration (unknown) Detection (instant)	S	S	P	Negative Example Scenarios	Fail to Gain	Lose Value	Gain Value	Preserve Value
31	Data(base) integrity	Failure Malicious	Internal External	Modification	Enterprise architecture	Timing (unknown) Duration (unknown) Detection (unknown)	S		P	Negative Example Scenarios				
32	Logical trespassing	Internal External	Malicious	Ineffective design Inappropriate use Disclosure	Process (ensure systems security) Enterprise architecture (information)	Timing (non-critical) Duration (extended) Detection (slow)	S		P	Negative Example Scenarios				
33	Operational IT errors	Internal	Accidental Failure Malicious	Modification	Process (manage changes) Enterprise architecture	Timing (critical) Duration (extended) Detection (unknown)	S		P	Negative Example Scenarios				

Figure 40—Generic IT Risk Scenarios (cont.)

#	High-level Risk Scenario	Risk Scenario Components					Risk Category/Group			Risk		Risk Consequence			
		Actor	Threat Type	Event	Asset/Resources	Time	IT Benefit/Value Enablement	IT Programme and Project Delivery	IT Operations and Service Delivery	Risk	Risk	Fail to Gain	Lose Value	Positive Example Scenarios	Gain Value
34	Contractual compliance	Internal External	Failure Malicious	Ineffective execution	Process (ensure compliance with external requirements)	Timing (non-critical) Duration (extended) Detection (slow)	P	P	<ul style="list-style-type: none"> Non-compliance with software license agreements (e.g., use and/or distribution of unlicensed software) Contractual obligations as service provider with customers/clients not met 						
35	Environmental	Internal External	Natural	Ineffective design	Process (manage the physical environment) Infrastructure	Timing (unknown) Duration (unknown) Detection (unknown)	S	P	<ul style="list-style-type: none"> Equipment used not environmentally friendly (e.g., power consumption, packaging) 						
36	Acts of nature	External	Natural	Destruction	Process (manage the physical environment) Infrastructure People	Timing (unknown) Duration (unknown) Detection (instant)	S	P	<ul style="list-style-type: none"> Earthquake Tsunami Major storm/hurricane Major wildfire 						

Capability Risk Factors in the Risk Analysis Process



As shown in **figure 37**, the frequency and impact of risk scenarios are influenced by risk factors. This section explains how certain risk factors, i.e., IT capability and business capability for IT, can have a negative (or positive) influence on impact and frequency of certain risk scenarios:

- A very strong IT capability, e.g., very strong IT project development capability, will automatically reduce the frequency of low-quality IT solutions.
- Weak security management will probably lead to increased frequency of security incidents and incidents will have a higher impact.
- Weak IT project investment decision mechanisms may lead to the wrong projects being selected for implementation.

The following frameworks are used:

- COBIT—For expressing IT capability. Mature and well-controlled IT processes are a very strong indicator of high IT capability.
- Val IT—For expressing IT-related business capability. Mature IT value management processes indicate high capability in this area.

Figure 41 includes the same list of example generic risk scenarios as in the Example Risk Scenarios section. It contains the following information:

- Risk scenario title
- Four columns, one for each COBIT domain, where a reference is made to those COBIT processes that can influence frequency or impact of the risk scenario
- Three columns, one for each of the Val IT domains, where a reference is made to those Val IT processes that can influence frequency or impact of the risk scenario

The table can be used during risk assessment exercises (see the risk IT process model, process RE2). It indicates which processes need to be considered when assessing impact and/or frequency of risk scenarios.

Figure 41—Generic IT Risk Scenarios Mapped to COBIT and Val IT Processes

#	High-level Risk Scenario	IT Management Capability (COBIT)				Value Management Capability (Val IT)		
		Plan and Organise (PO)	Acquire and Implement (AI)	Deliver and Support (DS)	Monitor and Evaluate (ME)	Value Governance (VG)	Programme Management (PM)	Investment Management (IM)
1	IT programme selection	P01, P02, P03	AI1, AI3		ME1, ME3	VG1, VG2, VG3, VG5	PM1, PM4, PM5	
2	New technologies	P01, P02, P03	AI1, AI3		ME1	VG3	PM1, PM4	
3	Technology selection	P02, P03	AI1, AI3		ME1			IM1, IM2
4	IT investment decision making	P01, P04, P05, P06	AI1, AI3		ME3	VG1, VG2, VG4	PM1, PM4, PM5	
5	Accountability over IT	P04, P06, P07		DS1, DS2	ME4	VG1		IM1

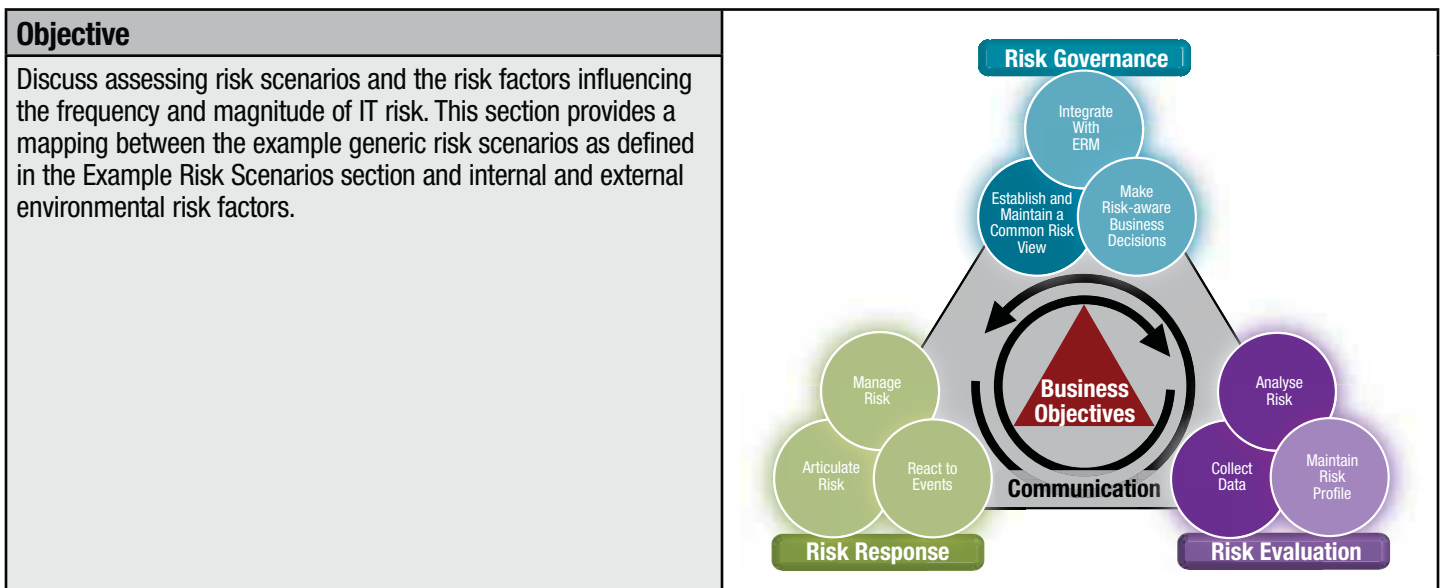
Figure 41—Generic IT Risk Scenarios Mapped to COBIT and Val IT Processes (cont.)

#	High-level Risk Scenario	IT Management Capability (COBIT)				Value Management Capability (Val IT)		
		Plan and Organise (PO)	Acquire and Implement (AI)	Deliver and Support (DS)	Monitor and Evaluate (ME)	Value Governance (VG)	Programme Management (PM)	Investment Management (IM)
6	Integration of IT within business processes	P01, P02, P03, P04	AI1, AI2, AI3					IM1
7	State of infrastructure technology	P01, P03, P05	AI1, AI3, AI5	DS3	ME1		PM1, PM4	
8	Ageing of application software	P01, P03, P05	AI1, AI2, AI5	DS3	ME1			
9	Architectural agility and flexibility	P01, P02, P03, P04, P05	AI1, AI2, AI3, AI5		ME1			
10	Regulatory compliance	P01, P04, P06, P07, P09	AI1	DS4, DS5	ME3			
11	Software implementation	P010	AI2, AI4, AI5, AI6, AI7	DS7, DS8, DS9, DS10, DS13	ME1			
12	IT project termination	P04, P05, P06	AI2, AI3, AI5		ME1, ME4			IM7, IM9, IM10
13	IT project economics	P05, P010	AI5		ME1		PM2, PM5	IM9
14	Project delivery	P07, P08, P010	AI2, AI3, AI4, AI5, AI6, AI7	DS2	ME1			IM9
15	Project quality	P08, P010	AI4, AI6, AI7	DS2	ME1			IM9
16	Selection/performance of third-party suppliers	P04, P05	AI5	DS1, DS2	ME1, ME4			
17	Infrastructure theft	P06, P07		DS12				
18	Destruction of infrastructure			DS12				
19	IT staff	P04, P06, P07	AI5	DS2, DS7	ME1		PM3	
20	IT expertise and skills	P07	AI5	DS2	ME1, ME4		PM3	
21	Software integrity	P08, P010	AI2, AI6, AI7	DS2, DS5, DS9, DS10, DS13	ME1			
22	Infrastructure (hardware)			DS1, DS2, DS5, DS9, DS12, DS13				
23	Software performance	P08, P010	AI2, AI4, AI6, AI7	DS3, DS8, DS10	ME1			
24	System capacity	P02, P03	AI3	DS3	ME1			
25	Ageing of infrastructural software	P03	AI3					
26	Malware	P06	AI6, AI7	DS5, DS12				
27	Logical attacks	P02, P03		DS5, DS12				
28	Information media			DS5, DS11, DS12, DS13				
29	Utilities performance	P03		DS1, DS12				
30	Industrial action	P04, P07						
31	Data(base) integrity	P02	AI1, AI2, AI3, AI5, AI6	DS9, DS11, DS13				
32	Logical trespassing	P04, P06		DS5				

Figure 41—Generic IT Risk Scenarios Mapped to COBIT and Val IT Processes (cont.)

#	High-level Risk Scenario	IT Management Capability (COBIT)				Value Management Capability (Val IT)		
		Plan and Organise (PO)	Acquire and Implement (AI)	Deliver and Support (DS)	Monitor and Evaluate (ME)	Value Governance (VG)	Programme Management (PM)	Investment Management (IM)
33	Operational IT errors			DS7, DS13				
34	Contractual compliance		AI5	DS1, DS2		ME3		
35	Environmental	PO1, PO3	AI5					
36	Acts of nature			DS12				

Environmental Risk Factors in the Risk Analysis Process



As shown in **figure 37**, the frequency and impact of risk scenarios are influenced by risk factors. This section explains how certain risk factors, i.e., internal and external environmental factors, can have a negative (or positive) influence on the frequency and impact of certain risk scenarios:

- A strong competitive environment will make the efficiency of project development and operations more important and, hence, increase the impact of failed projects.
- A highly complex IT architecture will probably increase the frequency of hardware or software malfunctions.
- A difficult geopolitical situation may offer risk factors. For example:
 - A location in a high earthquake risk area will increase the frequency of a potential natural disaster (and will require stronger relevant controls).
 - An unstable political situation might increase the frequency of industrial action or the physical integrity of assets such as data centres, or might create frequent changes in regulations.

Figure 42 provides a link between risk scenarios and the degree to which the environmental risk factors will affect them. This link should be considered when analysing risk, i.e., when assessing frequency and impact of the risk scenario. ‘High’ indicates that when analysing the risk scenario, the risk factor at hand (when important) will highly influence the frequency and/or impact of the scenario. The purpose of this table is to serve as a memory aid and support in the risk analysis process; it is not prescriptive, only indicative. Those factors that are noted as ‘medium’ or ‘low’ (empty box), have less influence on the frequency and/or impact of the risk scenario.

Figure 42 includes the same list of example generic risk scenarios as defined in the Example Risk Scenarios section. The figure contains the following additional information in two groups of columns:

- **External environmental risk factors**—For each separate risk factor (see the Risk Scenarios Explained section), an indication is included as to the extent this factor can influence the scenario. The table should be read as follows: If a cell contains the value ‘high’, this means that for this scenario, frequency and impact of the scenario will be more important if the risk factor at hand is more important. For scenario 1 (IT programme selection), the external environmental risk factors ‘Rate of Change’, ‘Competition’ and ‘Technology Status and Evolution’ are marked ‘high’, indicating that when these three factors are high, e.g., a very competitive environment, the frequency and magnitude for this scenario might be influenced in the negative sense (i.e., higher risk). For the same risk scenario, there is a medium influence of regulatory requirements listed. Although the need to address, for example, new privacy issues, may influence the risk of programmes not being aligned with the business objective of compliancy. However, the complexity and strategic importance of IT are much more influential to the possible risks related to ‘IT programme selection’. In this example, it is safe to say that the geopolitical situation of the enterprise does not have any significant influence on this risk scenario.
- **Internal environmental factors**—The same information is reflected here.

Risk factors cannot always be influenced by the enterprise, so in many instances, it is a given that they need to be considered for risk management purposes. This applies mostly to the external environmental factors.

Other risk management frameworks and standards work with the concept ‘vulnerability’ when analysing risk. This concept is equivalent to the Risk IT concept of risk factors.

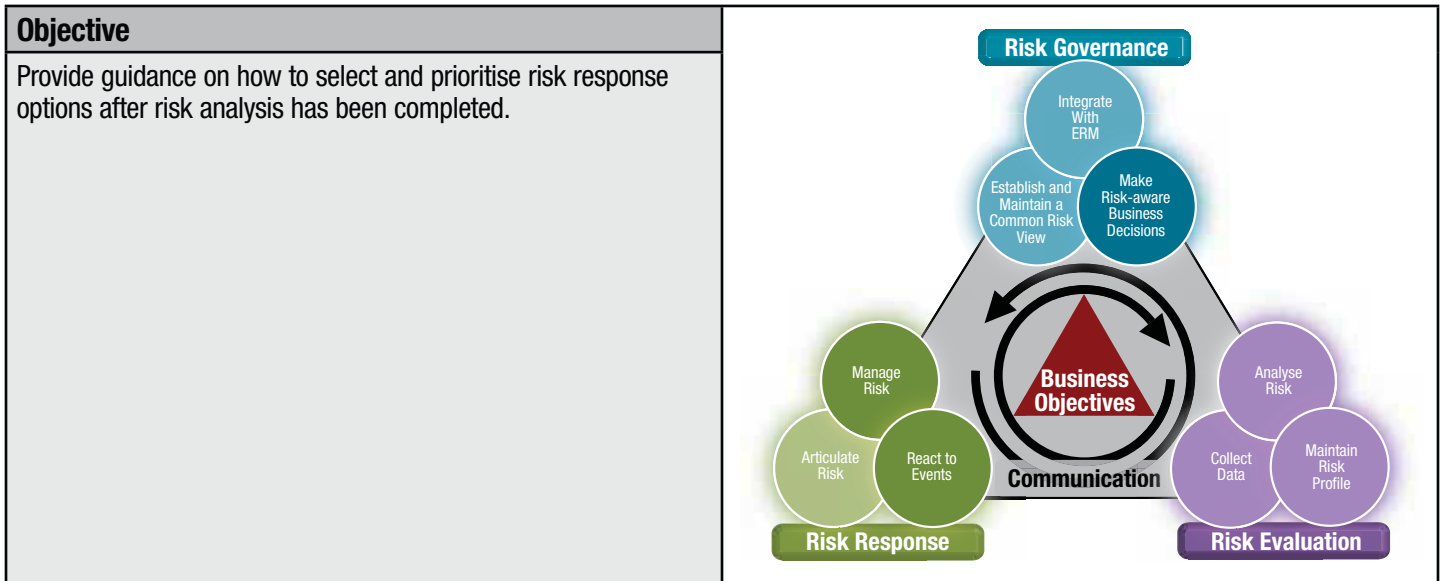
Figure 42—Generic IT Risk Scenarios and Environmental Risk Factors

#	High-level Scenario	External Environmental Risk Factors					Internal Environmental Risk Factors							
		Market	Rate of Change	Competition	Geopolitical Situation	Regulatory Environment	Technology Status and Evolution	Strategic Importance of IT	Complexity of IT	Complexity of the Entity	Degree of Change	Risk Management Philosophy	Risk Appetite	Operating Model
1	IT programme selection	Medium	High	High		Medium	High	High	High	High	High	High	High	High
2	New technologies	Medium	High	High			High	High	High	Medium	High	High	High	Medium
3	Technology selection	Medium	High	High			High	High	High	Medium	High	High	High	High
4	IT investment decision making	High	High	High		High	High	High	High	High	High	High	High	High
5	Accountability over IT			Medium		High		High	High	High	High	High	High	High
6	Integration of IT within business processes		High		Medium	High		High	High	High	High	High	High	High
7	State of infrastructure technology							High	High	Medium	High	High	High	Medium
8	Ageing of application software		High	Medium				High	High	Medium	High	High	High	Medium
9	Architectural agility and flexibility		High	High				Medium	High	High	High	High	High	High
10	Regulatory compliance	High				High			High	High	High	High	High	High
11	Software implementation		Medium						High	Medium	High	High	High	High
12	IT project termination		High	Medium					High	High	High	High	High	High
13	IT project economics		Medium	High				Medium	High	Medium	High	High	High	Medium
14	Project delivery		High	High					High	Medium	High	High	High	High
15	Project quality			High		Medium			High	Medium	High	High	High	Medium
16	Selection/performance of third-party suppliers	Medium	High	High	High	High			High	High	High	High	High	High
17	Infrastructure theft				High				High		High	High	High	
18	Destruction of infrastructure				Medium				High					
19	IT staff	Medium	Medium	High	High			Medium	High	Medium	High	High	High	High
20	IT expertise and skills	Medium	Medium	High	High				High	Medium	High	High	High	High
21	Software integrity					Medium			High	Medium	High	High	High	
22	Infrastructure (hardware)								High		High	High	High	
23	Software performance								High		High	High	High	
24	System capacity			High					High		High	High	High	High
25	Ageing of infrastructural software							High			High	High	High	High
26	Malware			Medium	Medium	High					High	High	Medium	Medium
27	Logical attacks			High	High	High				Medium	High	High	High	High
28	Information media					High					High	High	High	High

Figure 42—Generic IT Risk Scenarios and Environmental Risk Factors (cont.)

#	High-level Scenario	External Environmental Risk Factors					Internal Environmental Risk Factors								
		Market	Rate of Change	Competition	Geopolitical Situation	Regulatory Environment	Technology Status and Evolution	Strategic Importance of IT	Complexity of IT	Complexity of the Entity	Degree of Change	Risk Management Philosophy	Risk Appetite	Operating Model	
29	Utilities performance				High			High							
30	Industrial action			High	High			High		High	High	High	High	Medium	
31	Data(base) integrity			High		Medium		High	Medium			High	High		
32	Logical trespassing				Medium	Medium		High	Medium	Medium	High	High	High		
33	Operational IT errors							High	High	High	High	High	High	Medium	
34	Contractual compliance			High	High	High	Medium	High	Medium	High	High	High	High	High	
35	Environmental				High				Medium			High	High	High	
36	Acts of nature				High							High	High	High	

6. RISK RESPONSE AND PRIORITISATION



Risk Response Options

The purpose of defining a risk response is to bring risk in line with the defined risk tolerance for the enterprise. In other words, a response needs to be defined such that as much future residual risk (current risk with the risk response defined and implemented) as possible (usually depending on budgets available) falls within risk tolerance limits.

This is not a one-time effort; rather, it is part of the risk management process cycle, i.e., activity RR2.3 *Respond to discovered risk exposure and opportunity* of the Risk IT process model.

When risk analysis, after weighing risk vs. potential return, has shown that risk is not aligned with the defined risk tolerance levels, a response is required.

Figure 43 shows the first phase in the risk response flow: after identifying risk scenarios, scenarios are analysed and assessments are made for frequency and magnitude of the risk, taking into account potential return. A critical success factor of this exercise is that the risk scenario list be complete, and equally important is to make sure that the enterprise is in a position to detect risk, as explained previously (see chapter 5, Risk Scenarios Explained section).

When the analysis shows risks deviating from the defined tolerance levels, a response needs to be defined. This response can be any of the four possible responses explained in the following sections.

Risk Avoidance

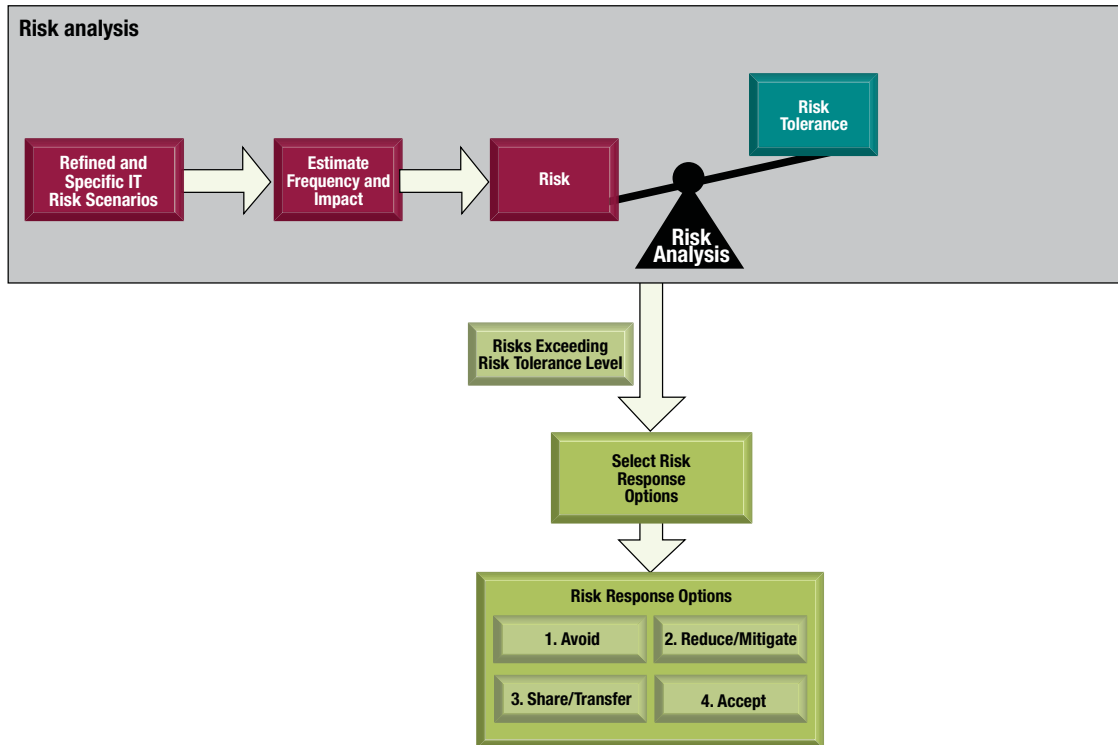
Avoidance means exiting the activities or conditions that give rise to risk. Risk avoidance applies when no other risk response is adequate. This is the case when:

- There is no other cost-effective response that can succeed in reducing the frequency and magnitude below the defined thresholds for risk appetite.
- The risk cannot be shared or transferred.
- The risk is deemed unacceptable by management.

Some IT-related examples of risk avoidance may include:

- Relocating a data centre away from a region with significant natural hazards
- Declining to engage in a very large project when the business case shows a notable risk of failure
- Declining to engage in a project that would build on obsolete and convoluted systems because there is no acceptable degree of confidence that the project will deliver anything workable
- Deciding not to use a certain technology or software package because it would prevent future expansion

Figure 43—Risk Response Options



Risk Reduction/Mitigation

Reduction means that action is taken to detect the risk, followed by action to reduce the frequency and/or impact of a risk. The most common ways of responding to risk include:

- Strengthening overall IT risk management practices, i.e., implement sufficiently mature IT risk management processes as defined by the Risk IT framework
- Introducing a number of control measures¹¹ intended to reduce either frequency of an adverse event happening and/or the business impact of an event, should it happen. This is discussed in the remainder of this section.

Control Activities

Control activities are, in the context of IT risk management, the policies, procedures and practices put into place so that frequency of adverse IT events and/or impact of such events are reduced to acceptable levels. These control activities are also known as IT controls, and they include the following types:

- Entity-level controls:
 - IT strategy, IT technology selection, IT architecture, IT policy setting, IT human resources management, etc.
- General IT controls:
 - Data centre operation controls—Controls such as job setup and scheduling, operator actions, and data backup and recovery procedures
 - System software controls—Controls over the effective acquisition, implementation and maintenance of system software, database management, telecommunications software, security software and utilities
 - Access security controls—Controls that prevent inappropriate and unauthorised use of the system
 - Application system development and maintenance controls—Controls over development methodology, including system design and implementation, that outline specific phases, documentation requirements, change management, and approvals and checkpoints to control the development or maintenance of the project

This list of controls is not exhaustive and the COBIT and Val IT frameworks, as well as other IT standards, contain many other good practices that can be implemented to reduce risk.

For a comprehensive list of controls that can address all risk scenarios (list of example generic risk scenarios as defined in chapter 5, Example Risk Scenarios section), refer to chapter 8.

¹¹ The reader familiar with COBIT will immediately make the association with COBIT and its integrated control framework. In the remainder of this document, in particular in chapter 8, risk scenarios are connected with the controls defined in COBIT and the management practices defined in Val IT.

Some IT-related examples of risk mitigation may include:

- A stock-clearing corporation identified and assessed the risk of its systems not being available for more than three hours and concluded that it would not accept the impact of such an occurrence. The company invested in technology with enhanced failure self-detecting and backup systems to reduce the likelihood of system unavailability.
- An organisation subject to accounting regulations found that it had an important risk for fraudulent or unauthorised use of software and changes, making it subject to legal action. As a result, it strengthened its change management and configuration management processes.

Risk Sharing/Transfer

Sharing means reducing risk frequency or impact by transferring or otherwise sharing a portion of the risk. Common techniques include insurance and outsourcing. Examples include taking out insurance coverage for IT-related incidents, outsourcing part of the IT activities, or sharing IT project risk with the provider through fixed-price arrangements or shared-investment arrangements. In both a physical and legal sense these techniques do not relieve an enterprise of a risk, but can involve the skills of another party in managing the risk and reduce the financial consequence if an adverse event occurs.

Some IT-related examples of risk sharing or transfer may include:

- A large organisation identified and assessed the risk of fire to its infrastructure across diverse geographic regions and assessed the cost of sharing the impact of its risk through insurance coverage. It concluded that, because of the location of its sites, the incremental cost of insurance and related deductibles was not prohibitive, and insurance coverage was taken.
- In a major IT-related investment, project risk may be shared by outsourcing the development to an outsourcer for a fixed price.
- Where application hosting is outsourced, the organisation always remains accountable for protecting client privacy, but if the outsourcer is negligent and a breach occurs, risk (financial impact) might at least be shared with the outsourcer.

Other techniques contributing to risk sharing include:

- Large enterprises with several IT divisions, where IT risk can be transferred to other divisions within the enterprise
- SAS70 Type 2 certification, which allows a service organisation to transfer a portion of a risk back to the client through the Client Considerations Section of the SAS70 Report

Risk Acceptance

Acceptance means that no action is taken relative to a particular risk, and loss is accepted when/if it occurs. This is different from being ignorant of risk; accepting risk assumes that the risk is known, i.e., an informed decision has been made by management to accept it as such. If an enterprise adopts a risk acceptance stance, it should carefully consider who can accept the risk—even more so with IT risk. IT risk should be accepted only by business management (and business process owners), in collaboration with and supported by IT, and acceptance should be communicated to senior management and the board.

Some IT-related examples of risk acceptance may include:

- There may be a risk that a certain project will not deliver the required business functionality by the planned delivery date. Management may decide to accept the risk and proceed with the project.
- Self-insurance is another form of risk acceptance, although this manages only magnitude of the loss and has no impact on frequency.
- If a particular risk is assessed to be extremely rare but very important (catastrophic) and approaches to reduce it are prohibitive, management may decide to accept it.

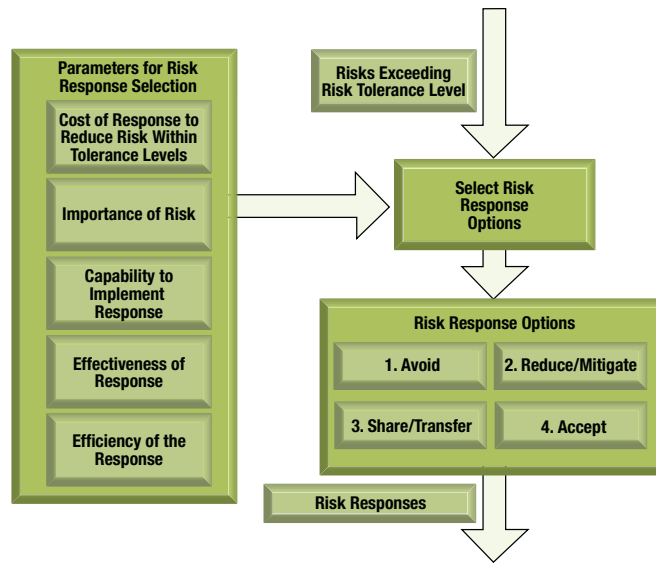
Risk Response Selection and Prioritisation

The previous section listed the available risk response options. In this section, the selection of an appropriate response, i.e., given the risk at hand, how to respond and how to choose between the available response options, is briefly discussed.

The following parameters need to be taken into account in this process, as illustrated in **figure 44**:

- Cost of the response, e.g., in the case of risk transfer, the cost of the insurance premium; in the case of risk mitigation, the cost (capital expense, salaries, consulting) to implement control measures
- Importance of the risk addressed by the response, i.e., its position on the risk map (which reflects combined frequency and magnitude levels)

Figure 44—Risk Response Options and Influencers

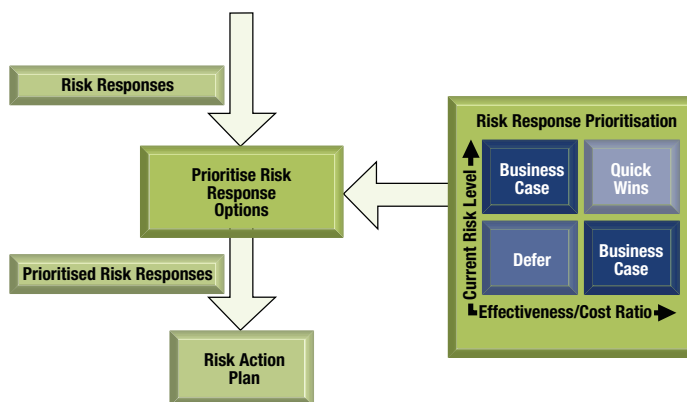


- The enterprise’s capability to implement the response; i.e., when the enterprise is mature in its risk management processes, more sophisticated responses can be implemented; when the enterprise is rather immature, some very basic responses may be better
- Effectiveness of the response, i.e., the extent to which the response will reduce the frequency and impact of the risk
- Efficiency of the response, i.e., the relative benefits promised by the response in comparison to:
 - Other IT-related investments (investing in risk response measures always competes with other IT [or non-IT] investments)
 - Other responses (one response may address several risks while another may not)

It is likely that the aggregated required effort for the mitigation responses, i.e., the collection of controls that need to be implemented or strengthened, will exceed available resources. In this case, prioritisation is required. Using the same criteria as for risk response selection, risk responses can be placed in a quadrant offering three possible options, as shown in **figure 45**:

- Quick wins—Very efficient and effective responses on high risks
- Business case to be made—More expensive or difficult responses to high risks or efficient and effective responses on lower risks, both requiring careful analysis and management decision on investments. The Val IT framework approach may be applied here.
- Deferral—Costly responses to lower risks

Figure 45—Risk Response Prioritisation Options



Some examples of prioritisation include:

- A risk has been identified that the enterprise’s IT architecture is so complex that, within a few years, extending capacity will become difficult and maintaining software will become very expensive. The identified responses consist of strengthening the COBIT PO2 *Define information architecture* process, and starting a large project to overhaul the complete architecture. Given the cost of this project, this response is categorised as ‘business case to be made’.
- A risk of non-compliance with regulations is identified because a number of relatively simple IT procedures are missing. The response consists of creating the missing IT procedures and implementing them. This is classified as a quick win.

6. RISK RESPONSE AND PRIORITISATION

Guidance on Risk Response Selection and Prioritisation

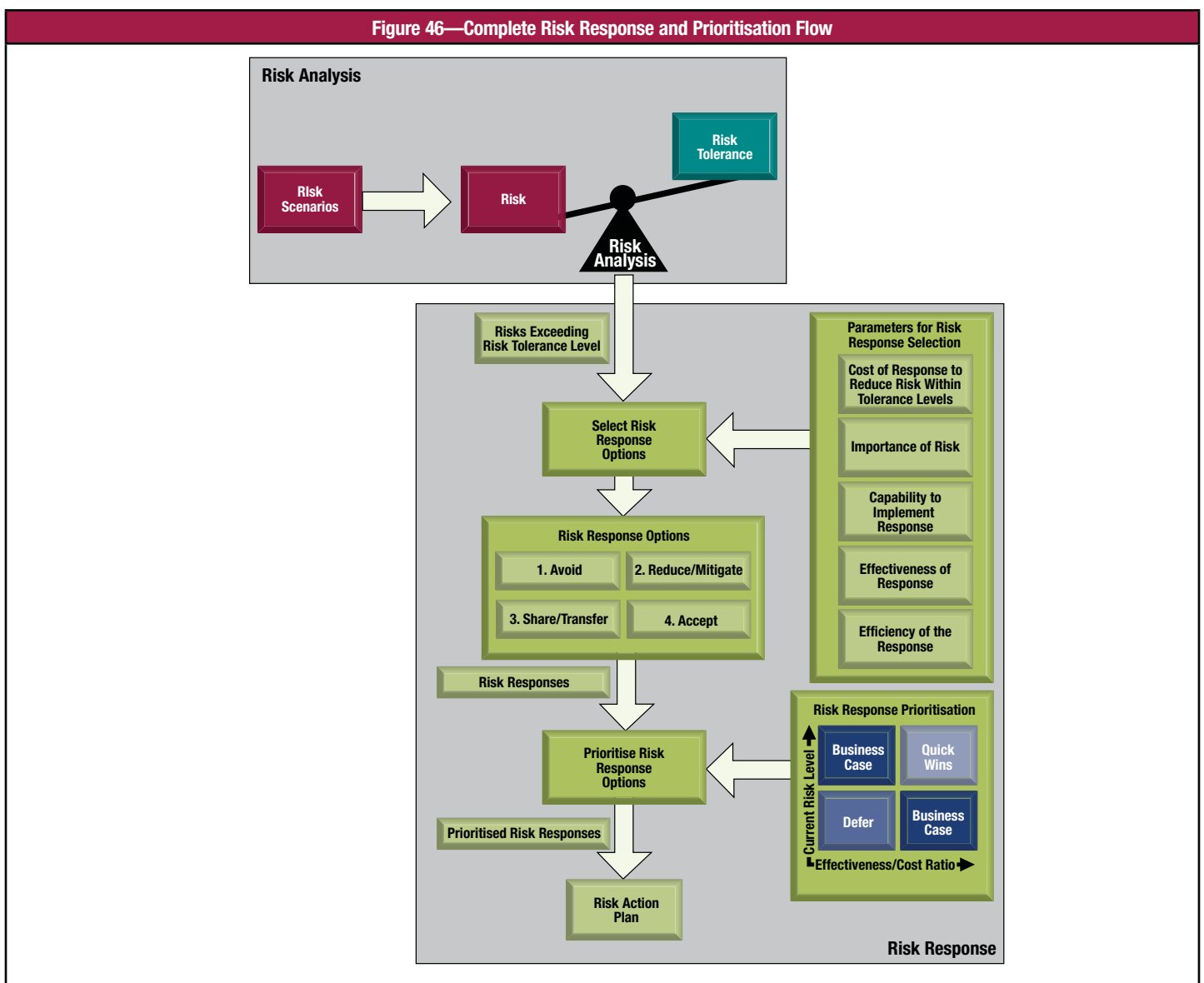
The Risk IT process model includes RACI charts for all IT risk management process activities, including risk response definition and prioritisation. It is suggested that all major stakeholders be involved in those decisions, i.e., senior management, business management, IT and risk management.

Based on the outcomes of risk analysis and the experience gained during definition and prioritisation of the risk response, the enterprise may also decide on more fundamental changes in its position against risk:

- Review the risk tolerance thresholds or temporarily increase or decrease risk tolerance levels.
- Increase (or decrease) resources available for executing risk response.
- Accept risks that normally would exceed risk tolerance thresholds.

In the evaluation and design of risk responses, enterprises should always look for a balanced set of responses, i.e., a combination of awareness/education, process/governance and automation.

Figure 46 shows the complete flow for risk response definition and prioritisation, using all the building blocks explained earlier in this chapter.



Perspectives on Risk Management—What to do Next?

Throughout this guide, several approaches and techniques to strengthen an enterprise's maturity in each of the three process areas of Risk IT are presented. In *The Risk IT Framework*, maturity matrices are provided for evaluation of risk management processes. Wherever an enterprise is in its maturity, undoubtedly the question will arise: 'What to do next?'

To help answer this question, a survey research study of 258 business and IT executives from several countries provides valuable insight. This study was conducted jointly by IBM and the MIT Sloan Center for Information Systems Research¹². A series of questions was asked about IT risk management actions taken, and the IT and business outcomes experienced. These activities were placed into three groups:

- Risk governance represents the policies and processes used to identify, prioritise and identify responses to IT risks. Its definition embraces much of what is in Risk IT's risk evaluation and response.
- IT foundation refers to the actual IT environment (people, process, software and hardware).
- Risk-aware culture includes being aware of risk, being comfortable talking about it and working together to manage it.

Key findings include:

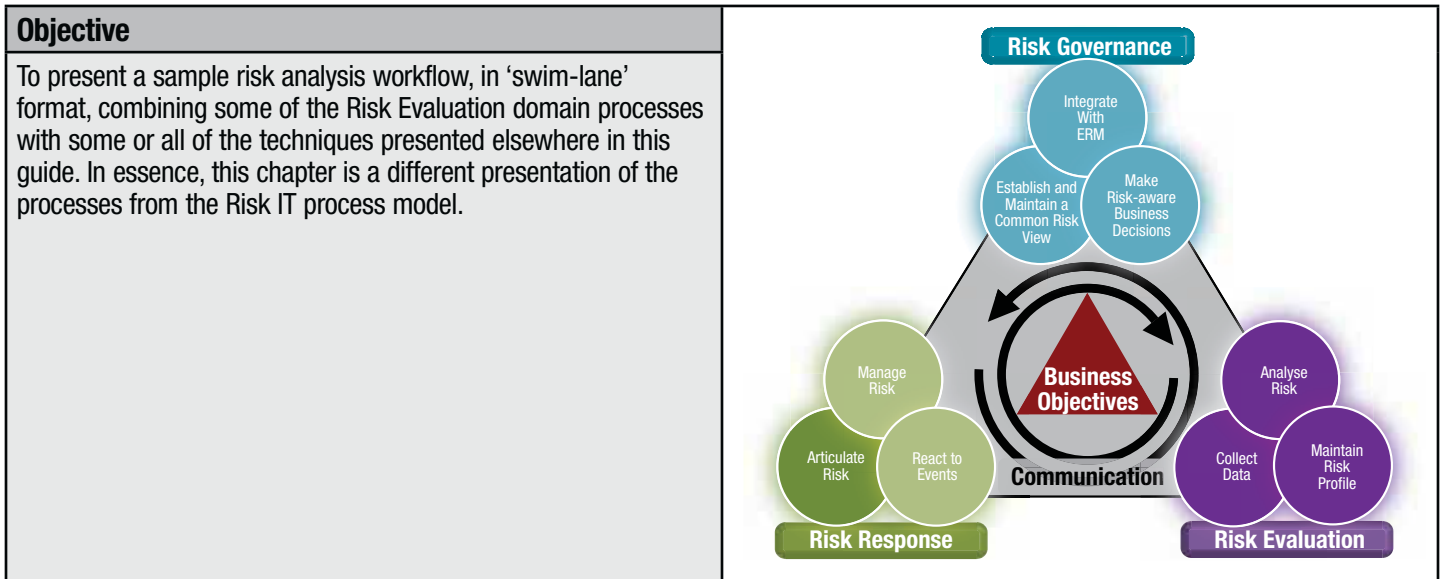
- Enterprises that had balanced maturity in their IT risk actions, meaning higher maturity across all three areas, had significantly better IT and business outcomes. Those outcomes were not just about reducing negative IT incidents. They also included managing costs better, ensuring that current functionality is more fully aligned with business needs, and having more agility to support changes in the business.
- Enterprises with balanced maturity reported more favourable perceptions of IT risk management capability than those that do not employ all three disciplines. Just 10 percent of out-of-balance enterprises say that they effectively manage IT risks, while 72 percent of enterprises with balanced maturity make that claim.
- The role of risk governance is different from the other two areas. The other two areas, IT foundation and risk-aware culture, are associated most directly with effective outcomes. Risk governance acts as the facilitating function to make the other two more effective, and addresses objectives and perceptions of stakeholders—what oversight is about. Risk governance also seems to play a stronger role early, being more highly associated with positive outcomes as firms start their journey, then playing more of a support role as enterprises become more mature and the focus is on more direct business impact of improved IT foundation and risk-aware culture.

The implications from this survey for getting the most from Risk IT include:

- Make good use of the Risk IT maturity matrices to improve (in a balanced) way within the three process areas of Risk IT.
- Once the most significant gaps have been identified, select techniques from this practitioner guide to help close those gaps more quickly and easily. Do not over-invest in those areas. When they reach a reasonable level of improvement, switch to improving others so that they are balanced. This can be thought of as avoiding weak links in a chain.
- Engage the enterprise with the correct participants in the risk governance body, including those people needed to implement improvements in the IT foundation and culture.
- Carry through the Risk IT Risk Evaluation and Risk Response process areas to achieve balanced improvements within the IT foundation and risk-aware culture. Risk IT is intended to provide clear value for the practitioner and the enterprise, through improved business and IT outcomes (just as identified in COBIT and discussed in chapter 4).

¹² Westerman, G.; B. Barnier; 'How Mature Is Your IT Risk Management?', MIT Sloan Center for Information Systems Research Briefing, vol. VIII, no. 3C, December 2008, and Westerman, G.; B. Barnier; 'IT Risk Management: Balanced Maturity Can Yield Big Results', IBM Whitepaper, February 2009

7. A RISK ANALYSIS WORKFLOW



This chapter describes a sample risk analysis workflow. This workflow references activities from the framework and should be regarded as a possible way of working. The guidance provided here ties together a number of concepts and activities to make these usable in a practical manner. More guidance on these concepts can be found in chapters 2, 5 and 6.

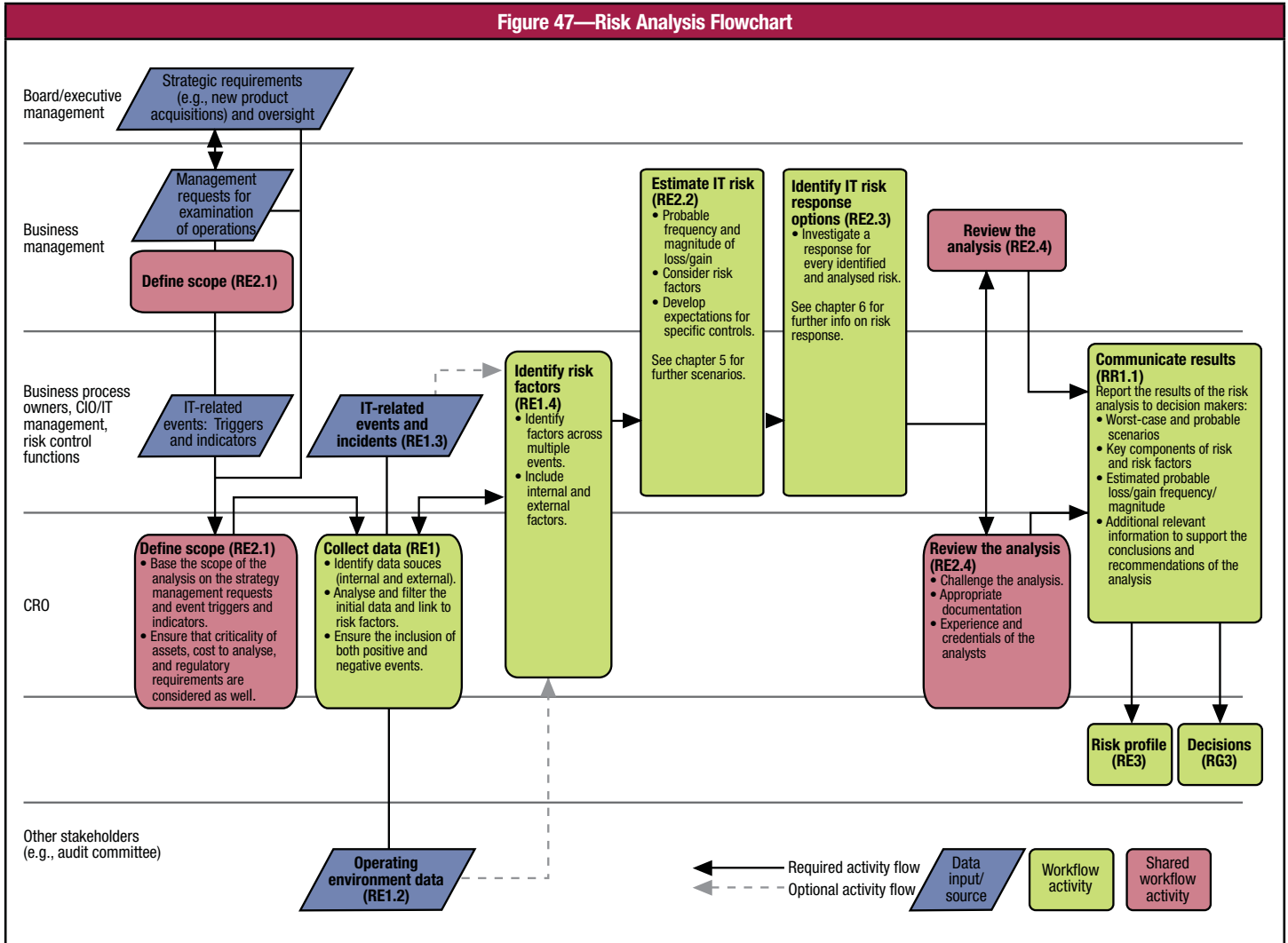
It is imperative that this workflow be seen in a larger context (i.e., the full Risk IT process model) and, therefore, should not exist detached from other IT risk management activities, such as risk profile updating and risk decisions. In this context, the following assumptions are used:

- Risk governance is in place and adequately adapted to the enterprise. This implies the identification of risk methods, the performing of an enterprise IT risk assessment, the definition of thresholds, etc.
- Afterwards, a process should exist to ensure that the risk analysis leads to an update of the risk profile.
- The risk analysis has been initiated. An analysis can be initiated by the CIO, CRO, business management or other interested parties. This initiation is usually triggered by events (i.e., the 'something goes wrong' practice, new business activity, environment change, new management, new compliance requirements) or indicator thresholds that are exceeded and create a sense of urgency with regard to managing risks.
- Further responding to risks and/or events is excluded from this exercise.

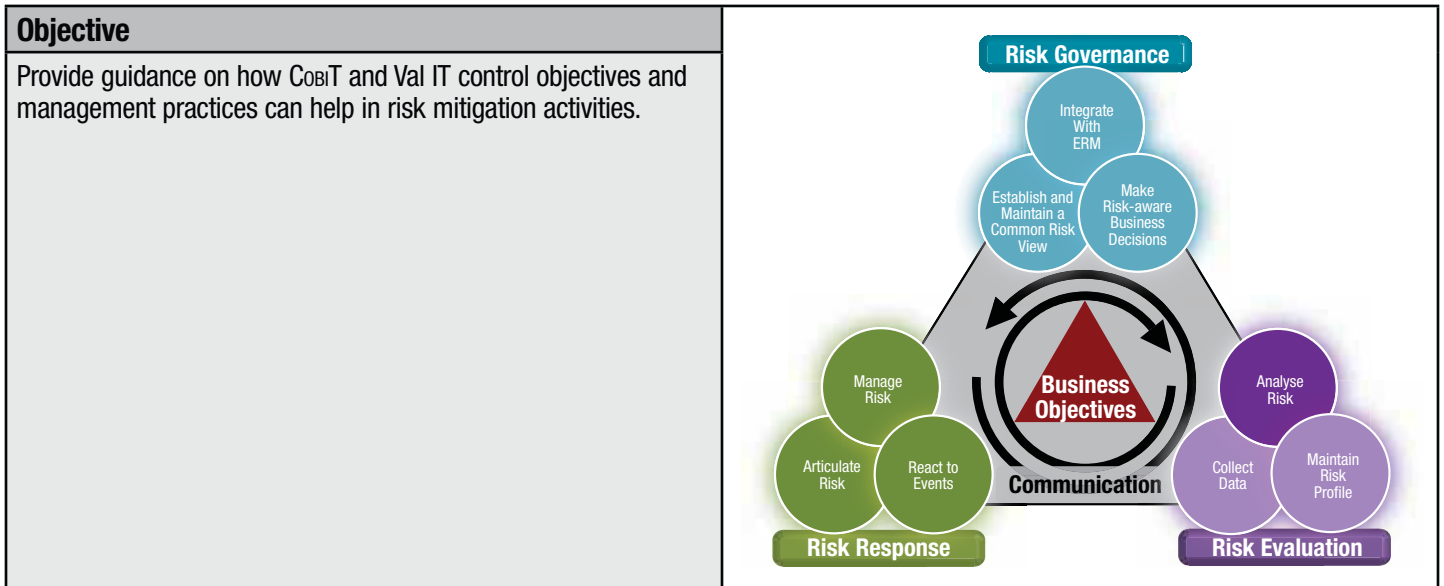
The sample risk analysis workflow (as illustrated in **figure 47**) includes the following steps:

1. Define the scope of the risk analysis—Define the objectives and boundaries of the analysis, taking into account several inputs ranging from strategic questions to the investigation of frequent events. As illustrated in **figure 47**, this step is performed with the input of the involved business representatives. They need to be involved in the decision regarding the assets and areas to take into account.
2. Collect data—Make sure that all possible sources are used to gather relevant data with regard to events leading to a positive and/or negative impact on the business. This includes IT incident repositories, audit reports and change logs, as well as former risk reports and external data, such as IT trend analysis and regulatory changes.
3. Identify common risk factors—Make sure that interrelated events are clustered around the common risk factors. These factors can influence frequency and magnitude of events that have a significant impact on the business. Examples are regulatory changes and international activities.
4. Estimate IT risk—Perform the actual analysis to estimate the frequency and magnitude of the scenarios, taking into account the risk factors (which include all current controls). Scenarios and the way to use these are explained in detail in chapter 5. The defined risk tolerance levels (as explained in chapter 2) need to be taken into account as well. These will serve as the basis for determining the risk response. This exercise needs to be performed by the CIO, CRO and the relevant business representatives in consultation with the risk control functions.
5. Identify risk response options—This is subject to more detailed guidance in chapter 6, including the further elaboration of control activities as a risk-reduction mechanism. This step should be performed in co-operation with the relevant owners of the business processes that depend on the IT areas that are being evaluated.
6. Review the analysis—Challenge the outcome of this exercise before reporting its results to management. Take into account more than just mathematical checks. Reasoning and reasonability are important concepts to challenge as well. The relevant stakeholders on the business side need to be included in the review of the assessment outcome. This will improve the business buy-in to the exercise and its results.
7. Reporting—Provide management with the results of the analysis to support decision-making.

Figure 47—Risk Analysis Flowchart



8. MITIGATION OF IT RISK USING COBIT AND VAL IT



In chapter 6, risk mitigation is identified as one of the options to respond to risk. IT risk mitigation is equivalent to implementing a number of IT controls and/or good IT management practices. Implementing controls is, therefore, a necessary part of good IT risk management, but in itself is not sufficient. The Risk IT process model defines a range of other activities that are also part of good IT risk management.

Risk IT does not define these as part of the framework, but refers to existing good practice frameworks that ISACA already has in place, i.e., COBIT and Val IT. This section contains a mapping between the example generic risk scenarios, as defined in chapter 5, Example Risk Scenarios section, and the COBIT control objectives (including the Application Control [AC] control objectives) and/or the Val IT key management practices, i.e., it provides a link between risk and control.

When using the following table (**figure 48**), the reader should keep in mind that:

- The table does not replace the risk analysis exercise; the risk scenarios presented here are generic and in themselves can cover many derived and varying scenarios (see the examples given in chapter 5, Example Risk Scenarios section). Every enterprise first needs to customise and define its own set of risk scenarios.
- This table needs to be customised; every situation is unique and every risk and all surrounding risk factors need to be considered before risk mitigation measures are defined.
- The suggested controls are not absolute; they need to be weighed in terms of cost/benefit, i.e., how effective they will be in reducing risk and what the cost is to implement (see also chapter 6).
- The suggested list of controls may not be complete for a particular situation, so the user should be prepared to carefully analyse whether any controls need to be added (or taken away) based on each situation. For some scenarios, additional and more detailed guidance may be required. An example is information security risks and controls such as vulnerability management or application security scanning.

Figure 48 contains the following information:

1. Generic scenario—Reference number of example generic risk scenario and title of example generic risk scenario
2. Essential control—Indicator of whether or not the suggested control can be considered an essential control/key management practice. A control/key management practice is considered essential if it has a high effect on reducing either impact or frequency of the scenario.
3. Control reference—Reference of the control/key management practice. This reference includes the COBIT or Val IT process reference (e.g., PO1, for the COBIT process PO1 *Define a strategic IT plan*, or the application control AC1 *Source data preparation and authorisation*) and a reference to the COBIT control objective or Val IT key management practice (e.g., PM1.3 *Define an appropriate investment mix*).
4. Control title—The title of the control/key management practice, as taken from COBIT or Val IT
5. Control description—The full description of the control/key management practice, as taken from COBIT or Val IT
6. Effect on frequency—The relative effect of the control/key management practice on reducing the frequency of the scenario occurring (indicated as medium or high).
7. Effect on impact—The relative effect of the control/key management practice on reducing the impact of the scenario (indicated as medium or high).

It should be noted that only controls that have an estimated effect of medium or high to reduce the frequency or impact of the scenario are listed.

This table can be useful for following purposes:

- Risk assessment and analysis—When frequency and impact need to be assessed. Controls/key management practices need to be taken into account to determine the most probable impact and a realistic frequency assessment; weak or strong controls are very important risk factors.
- Risk mitigation—When risks require mitigation, i.e., controls/key management practices need to be defined and implemented. The table provides a number of suggested controls that can help mitigate the risk at hand and their relative effect on frequency and impact.

Some further guidance on the use of this table:

- The control practices of COBIT provide an additional level of detail to assist in their implementation; this material should be consulted when implementing controls based on COBIT.
- *Enterprise Value: Getting Started With Value Management*¹³ assists in identifying and addressing the main issues that enterprises encounter in relation to value delivery from IT.
- Some enterprises, depending on their maturity level, may find it helpful to start with the table as shown, and append their own customised content at the end of each generic scenario, i.e., adding rows when needed. This helps maintain consistency and accelerates understanding.
- With regard to the application controls, *COBIT and Application Controls: A Management Guide*¹⁴ provides more guidance on the design and implementation, operation and maintenance, and assurance related to application controls.

Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk

Essential Control	Control Reference	Control Title	COBIT Control Objective/Val IT Key Management Practice	Effect on Frequency	Effect on Impact
1. IT programme selection					
Yes	P01	P01.1	IT Value Management		High
Yes	P01	P01.6	IT Portfolio Management		High
Yes	P03	P03.1	Technological Direction Planning		High
Yes	P04	P04.2	IT Strategy Committee	High	Medium
Yes	P04	P04.3	IT Steering Committee	High	Medium

¹³ ISACA, *Enterprise Value: Getting Started With Value Management*, USA, 2008

¹⁴ ISACA, *COBIT® and Application Controls: A Management Guide*, USA, 2009

8. MITIGATION OF IT RISK USING COBIT AND VAL IT

Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk (cont.)

Essential Control	Control Reference	Control Title	COBIT Control Objective/Val IT Key Management Practice	Effect on Frequency	Effect on Impact	
1. IT programme selection (cont.)						
Yes	PO5	PO5.2	Prioritisation Within IT Budget	Implement a decision-making process to prioritise the allocation of IT resources for operations, projects and maintenance to maximise IT's contribution to optimising the return on the enterprise's portfolio of IT-enabled investment programmes and other IT services and assets.	Medium	High
Yes	AI1	AI1.1	Definition and Maintenance of Business Functional and Technical Requirements	Identify, prioritise, specify and agree on business functional and technical requirements, covering the full scope of all initiatives required to achieve the expected outcomes of the IT-enabled investment programme.	High	Medium
Yes	PM4	PM4.1	Evaluate and Assign Relative Scores to Programme Business Cases	Perform detailed assessments of the programme business cases, evaluating strategic alignment; business benefits, both financial and non-financial; risks, including delivery risks and benefits risks; and availability of resources. Assign a relative score to each programme based on evaluation criteria and their weightings for the category of investment applicable to each programme.		High
	PO6	PO6.5	Communication of IT Objectives and Direction	Communicate awareness and understanding of business and IT objectives and direction to appropriate stakeholders and users throughout the enterprise.		Medium
	PM1	PM1.3	Define an Appropriate Investment Mix	The allocation of funds for IT-enabled investments must be aligned with the strategic direction of the enterprise. The investment mix must achieve the right balance on a number of dimensions, which could include, but are not limited to, an appropriate balance of short- and long-term returns, financial and non-financial benefits, and high-risk vs. low-risk investments.	Medium	Medium
	PM4	PM4.2	Create Overall Investment Portfolio View	Assess the impact on the overall investment portfolio of adding each candidate programme. Determine the impact on the investment portfolio mix. Identify any changes that might be required to other programmes in the investment portfolio as a result of adding each programme, and assess the impact and viability of those changes.	Medium	Medium
	IM1	IM1.3	Evaluate the Initial Programme Concept Business Case	Perform an initial triage of the programme concept business case looking at strategic alignment; benefits, both financial and non-financial; expenditures required; resources needed and contention for them; risks; and fit with the overall investment portfolio. Determine whether the programme concept has sufficient potential to justify proceeding to full programme definition and evaluation. If the decision is to proceed, the CIO should sign off on the technical aspects of the programme, and the business sponsor should approve and sign off on the initial programme concept business case.	Medium	
2. New technologies						
Yes	PO3	PO3.1	Technological Direction Planning	Analyse existing and emerging technologies, and plan which technological direction is appropriate to realise the IT strategy and the business systems architecture. Identify in the plan which technologies have the potential to create business opportunities. The plan should address systems architecture, technological direction, migration strategies and contingency aspects of infrastructure components.	High	
Yes	PO3	PO3.3	Monitor Future Trends and Regulations	Establish a process to monitor the business sector, industry, technology, infrastructure, legal and regulatory environment trends. Incorporate the consequences of these trends into the development of the IT technology infrastructure plan.	High	High
Yes	PM1	PM1.4	Translate the Business Strategy and Goals into IT Strategy and Goals	Identify the broad categories of information systems, applications, data, IT services, infrastructure, IT assets, resources, skills, practices, controls and relationships needed to underpin the business strategy. Document and agree upon an IT strategy and goals, taking into account the interrelationships between the business strategy and the IT services, assets and other resources, and identifying and leveraging synergies that can be achieved.		High
	PO2	PO2.1	Enterprise Information Architecture Model	Establish and maintain an enterprise information model to enable application development and decision-supporting activities, consistent with IT plans as described in PO1. The model should facilitate the optimal creation, use and sharing of information by the business in a way that maintains integrity and is flexible, functional, cost-effective, timely, secure and resilient to failure.	Medium	

Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk (cont.)

Essential Control	Control Reference	Control Title	COBIT Control Objective/Val IT Key Management Practice	Effect on Frequency	Effect on Impact	
2. New technologies (cont.)						
	PM1	PM1.3	Define an Appropriate Investment Mix	The allocation of funds for IT-enabled investments must be aligned with the strategic direction of the enterprise. The investment mix must achieve the right balance on a number of dimensions, which could include, but are not limited to, an appropriate balance of short- and long-term returns, financial and non-financial benefits, and high-risk vs. low-risk investments.	Medium	
3. Technology selection						
Yes	PO3	PO3.5	IT Architecture Board	Establish an IT architecture board to provide architecture guidelines and advice on their application, and to verify compliance. This entity should direct IT architecture design, ensuring that it enables the business strategy and considers regulatory compliance and continuity requirements. This is related/linked to PO2 <i>Define the information architecture.</i>	Medium	High
Yes	PO6	PO6.5	Communication of IT Objectives and Direction	Communicate awareness and understanding of business and IT objectives and direction to appropriate stakeholders and users throughout the enterprise.		High
Yes	AI1	AI1.1	Definition and Maintenance of Business Functional and Technical Requirements	Identify, prioritise, specify and agree on business functional and technical requirements, covering the full scope of all initiatives required to achieve the expected outcomes of the IT-enabled investment programme.		High
Yes	AI1	AI1.2	Risk Analysis Report	Identify, document and analyse risks associated with the business requirements and solution design as part of the organisation's process for the development of requirements.	Medium	High
Yes	AI1	AI1.3	Feasibility Study and Formulation of Alternative Courses of Action	Develop a feasibility study that examines the possibility of implementing the requirements. Business management, supported by the IT function, should assess the feasibility and alternative courses of action and make a recommendation to the business sponsor.	High	High
Yes	AI1	AI1.4	Requirements and Feasibility Decision and Approval	Verify that the process requires the business sponsor to approve and sign off on business functional and technical requirements and feasibility study reports at predetermined key stages. The business sponsor should make the final decision with respect to the choice of solution and acquisition approach.	Medium	High
Yes	IM2	IM2.2	Perform Analysis of Alternatives	Identify alternative courses of action to achieve the desired business outcomes. Assess the relative benefits, costs, risks and timing for each identified course of action. Select the course of action that has the highest potential rate of return and value, at an affordable cost with an acceptable level of risk. Document the selection criteria (which must be common for all options) and the rationale for recommending the selected course of action. Business management should assess the current and future business impact of the alternative courses of action, and the IT function should assess the technical impact.	Medium	High
	PO1	PO1.4	IT Strategic Plan	Create a strategic plan that defines, in co-operation with relevant stakeholders, how IT goals will contribute to the enterprise's strategic objectives and related costs and risks. It should include how IT will support IT-enabled investment programmes, IT services and IT assets. It should define how the objectives will be met, the measurements to be used and the procedures to obtain formal sign-off from the stakeholders. The IT strategic plan should cover investment/operational budget, funding sources, sourcing strategy, acquisition strategy, and legal and regulatory requirements. The strategic plan should be sufficiently detailed to allow for the definition of tactical IT plans.	Medium	
	PO2	PO2.1	Enterprise Information Architecture Model	Establish and maintain an enterprise information model to enable application development and decision-supporting activities, consistent with IT plans as described in PO1. The model should facilitate the optimal creation, use and sharing of information by the business in a way that maintains integrity and is flexible, functional, cost-effective, timely, secure and resilient to failure.	Medium	Medium
	PO3	PO3.2	Technological Infrastructure Plan	Create and maintain a technology infrastructure plan that is in accordance with the IT strategic and tactical plans. The plan should be based on the technological direction and include contingency arrangements and direction for acquisition of technology resources. It should consider changes in the competitive environment, economies of scale for information systems staffing and investments, and improved interoperability of platforms and applications.		Medium

8. MITIGATION OF IT RISK USING COBIT AND VAL IT

Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk (cont.)

Essential Control	Control Reference	Control Title	COBIT Control Objective/Val IT Key Management Practice	Effect on Frequency	Effect on Impact	
3. Technology selection (cont.)						
	P04	P04.3	IT Steering Committee	Establish an IT steering committee (or equivalent) composed of executive, business and IT management to: <ul style="list-style-type: none"> • Determine prioritisation of IT-enabled investment programmes in line with the enterprise's business strategy and priorities • Track status of projects and resolve resource conflicts • Monitor service levels and service improvements 		
	P05	P05.2	Prioritisation Within IT Budget	Implement a decision-making process to prioritise the allocation of IT resources for operations, projects and maintenance to maximise IT's contribution to optimising the return on the enterprise's portfolio of IT-enabled investment programmes and other IT services and assets.	Medium	Medium
	P010	P010.5	Project Scope Statement	Define and document the nature and scope of the project to confirm and develop amongst stakeholders a common understanding of project scope and how it relates to other projects within the overall IT-enabled investment programme. The definition should be formally approved by the programme and project sponsors before project initiation.		Medium
	IM2	IM2.1	Develop a Clear and Complete Understanding of the Candidate Programme	Utilise appropriate methods and techniques, involving all key stakeholders, to develop and document a complete and shared understanding of the expected business outcomes (intermediate, or lead, and end, or lag, outcomes) of the candidate programmes, how they will be measured, and the full scope of initiatives required to achieve the expected outcomes. These initiatives should include all changes required to the nature of the enterprise's business, business processes, skills and competencies of personnel, enabling technology and organisational structure. The nature of each initiative's contribution, how that contribution will be measured and all key assumptions should be identified. Relevant metrics or similar indicators to monitor the validity of these assumptions should be identified. Key risks, both to the successful completion of individual initiatives and the achievement of the desired outcomes, should also be identified and, where possible, mitigating actions should be included.	Medium	
4. IT investment decision making						
Yes	P04	P04.3	IT Steering Committee	Establish an IT steering committee (or equivalent) composed of executive, business and IT management to: <ul style="list-style-type: none"> • Determine prioritisation of IT-enabled investment programmes in line with the enterprise's business strategy and priorities • Track status of projects and resolve resource conflicts • Monitor service levels and service improvements 	Medium	High
Yes	P010	P010.4	Stakeholder Commitment	Obtain commitment and participation from the affected stakeholders in the definition and execution of the project within the context of the overall IT-enabled investment programme.		High
Yes	VG2	VG2.5	Establish, Implement and Communicate Roles, Responsibilities and Accountabilities	Establish, implement and communicate roles, responsibilities and accountabilities for all personnel in the enterprise in relation to the portfolios of business investment programmes; individual investment programmes; and IT services, assets and resources to allow sufficient authority to exercise the roles and responsibilities assigned. These roles should include: investment decision making, programme sponsorship, programme management, project management, service delivery and associated support roles. Accountability for all roles, including for achieving the business benefits, delivering required capabilities and controlling the expenditures, should be clearly assigned and monitored. Accountabilities should be accepted explicitly by those to whom they are assigned, and their performance should be assessed accordingly.	High	Medium
	P04	P04.15	Relationships	Establish and maintain an optimal co-ordination, communication and liaison structure between the IT function and various other interests inside and outside the IT function, such as the board, executives, business units, individual users, suppliers, security officers, risk managers, the corporate compliance group, outsourcers and offsite management.	Medium	

Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk (cont.)

Essential Control	Control Reference	Control Title	COBIT Control Objective/Val IT Key Management Practice	Effect on Frequency	Effect on Impact
4. IT investment decision making (cont.)					
	P05	P05.5	Benefit Management		Medium
	VG2	VG2.6	Establish Organisational Structures	Medium	
	PM3	PM3.2	Understand the Current and Future Demand (for business human resources)	Medium	
5. Accountability over IT					
Yes	A14	A14.2	Knowledge Transfer to Business Management	Medium	High
Yes	VG1	VG1.1	Develop an Understanding of the Significance of IT and Role of Governance	High	Medium
	P04	P04.2	IT Strategy Committee		Medium
	P04	P04.3	IT Steering Committee		Medium
	P04	P04.10	Supervision		Medium
	P05	P05.5	Benefit Management	Medium	Medium
	P010	P010.4	Stakeholder Commitment		Medium

8. MITIGATION OF IT RISK USING COBIT AND VAL IT

Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk (cont.)

Essential Control	Control Reference	Control Title	COBIT Control Objective/Val IT Key Management Practice	Effect on Frequency	Effect on Impact	
5. Accountability over IT (cont.)						
	VG1	VG1.2	Establish Effective Reporting Lines	Establish effective reporting lines that allow the CIO to engage the enterprise leadership as the advocate of the significance of IT for the enterprise. The reporting line of the CIO should be commensurate with the importance of IT to the enterprise.	Medium	
	VG2	VG2.6	Establish Organisational Structures	Establish appropriate boards, committees and support structures including, but not limited to, one or more investment and services board(s), an IT strategy committee, an IT planning or steering committee, and an IT architecture board. Establish and maintain an optimal co-ordination, communication and liaison structure between the IT function and other stakeholders, such as other business functions, users (which might include business customers), corporate functions, suppliers, outsourcers and others.	High	
	VG2	VG2.5	Establish, Implement and Communicate Roles, Responsibilities and Accountabilities	Establish, implement and communicate roles, responsibilities and accountabilities for all personnel in the enterprise in relation to the portfolios of business investment programmes; individual investment programmes; and IT services, assets and resources to allow sufficient authority to exercise the roles and responsibilities assigned. These roles should include: investment decision making, programme sponsorship, programme management, project management, service delivery and associated support roles. Accountability for all roles, including for achieving the business benefits, delivering required capabilities and controlling the expenditures, should be clearly assigned and monitored. Accountabilities should be accepted explicitly by those to whom they are assigned, and their performance should be assessed accordingly.	Medium	Medium
	PM3	PM3.2	Understand the Current and Future Demand (for business human resources)	Understand the current and future demand for business human resources based on the current investment portfolio and a forward view of the investment portfolio. Identify and pay special attention to key business personnel who are in short supply and who might be needed, especially those personnel who undertake day-to-day functions who might also be needed for undertaking additional work on investment programmes.	Medium	Medium
6. Integration of IT within business processes						
Yes	PO1	PO1.2	Business-IT Alignment	Establish processes of bi-directional education and reciprocal involvement in strategic planning to achieve business and IT alignment and integration. Mediate between business and IT imperatives so priorities can be mutually agreed.	High	High
Yes	PO4	PO4.4	Organisational Placement of the IT Function	Place the IT function in the overall organisational structure with a business model contingent on the importance of IT within the enterprise, specifically its criticality to business strategy and the level of operational dependence on IT. The reporting line of the CIO should be commensurate with the importance of IT within the enterprise.	High	
Yes	PO4	PO4.15	Relationships	Establish and maintain an optimal co-ordination, communication and liaison structure between the IT function and various other interests inside and outside the IT function, such as the board, executives, business units, individual users, suppliers, security officers, risk managers, the corporate compliance group, outsourcers and offsite management.	High	Medium
Yes	PO10	PO10.4	Stakeholder Commitment	Obtain commitment and participation from the affected stakeholders in the definition and execution of the project within the context of the overall IT-enabled investment programme.	High	
Yes	VG1	VG1.5	Ensure Alignment and Integration of Business and IT Strategies With Key Business Goals	The business and IT strategies should be integrated, clearly linking enterprise, business and IT goals, and should be broadly communicated and regularly reviewed.		High
Yes	VG2	VG2.6	Establish Organisational Structures	Establish appropriate boards, committees and support structures including, but not limited to, one or more investment and services board(s), an IT strategy committee, an IT planning or steering committee, and an IT architecture board. Establish and maintain an optimal co-ordination, communication and liaison structure between the IT function and other stakeholders, such as other business functions, users (which might include business customers), corporate functions, suppliers, outsourcers and others.	High	

Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk (cont.)

Essential Control	Control Reference		Control Title	COBIT Control Objective/Val IT Key Management Practice	Effect on Frequency	Effect on Impact
6. Integration of IT within business processes (cont.)						
Yes	PM1	PM1.2	Identify Opportunities for IT to Influence and Support the Business Strategy	Make sure there is a common and agreed-upon understanding between IT and the other business functions regarding the potential opportunities for IT to influence and support the business strategy. Ensure that these are broadly communicated.	High	
	P03	P03.5	IT Architecture Board	Establish an IT architecture board to provide architecture guidelines and advice on their application, and to verify compliance. This entity should direct IT architecture design, ensuring that it enables the business strategy and considers regulatory compliance and continuity requirements. This is related/linked to P02 <i>Define the information architecture.</i>	Medium	
	P04	P04.3	IT Steering Committee	Establish an IT steering committee (or equivalent) composed of executive, business and IT management to: <ul style="list-style-type: none"> • Determine prioritisation of IT-enabled investment programmes in line with the enterprise's business strategy and priorities • Track status of projects and resolve resource conflicts • Monitor service levels and service improvements 	Medium	
	P06	P06.5	Communication of IT Objectives and Direction	Communicate awareness and understanding of business and IT objectives and direction to appropriate stakeholders and users throughout the enterprise.		Medium
	AI1	AI1.1	Definition and Maintenance of Business Functional and Technical Requirements	Identify, prioritise, specify and agree on business functional and technical requirements, covering the full scope of all initiatives required to achieve the expected outcomes of the IT-enabled investment programme.	Medium	
7. State of infrastructure technology						
Yes	P01	P01.3	Assessment of Current Capability and Performance	Assess the current capability and performance of solution and service delivery to establish a baseline against which future requirements can be compared. Define performance in terms of IT's contribution to business objectives, functionality, stability, complexity, costs, strengths and weaknesses.	High	
Yes	P03	P03.2	Technological Infrastructure Plan	Create and maintain a technology infrastructure plan that is in accordance with the IT strategic and tactical plans. The plan should be based on the technological direction and include contingency arrangements and direction for acquisition of technology resources. It should consider changes in the competitive environment, economies of scale for information systems staffing and investments, and improved interoperability of platforms and applications.	High	High
Yes	P03	P03.4	Technology Standards	To provide consistent, effective and secure technological solutions enterprisewide, establish a technology forum to provide technology guidelines, advice on infrastructure products and guidance on the selection of technology, and measure compliance with these standards and guidelines. This forum should direct technology standards and practices based on their business relevance, risks and compliance with external requirements.	High	
Yes	AI3	AI3.3	Infrastructure Maintenance	Develop a strategy and plan for infrastructure maintenance, and ensure that changes are controlled in line with the organisation's change management procedure. Include periodic reviews against business needs, patch management, upgrade strategies, risks, vulnerabilities assessment and security requirements.	Medium	High
	P01	P01.4	IT Strategic Plan	Create a strategic plan that defines, in co-operation with relevant stakeholders, how IT goals will contribute to the enterprise's strategic objectives and related costs and risks. It should include how IT will support IT-enabled investment programmes, IT services and IT assets. IT should define how the objectives will be met, the measurements to be used and the procedures to obtain formal sign-off from the stakeholders. The IT strategic plan should cover investment/operational budget, funding sources, sourcing strategy, acquisition strategy, and legal and regulatory requirements. The strategic plan should be sufficiently detailed to allow for the definition of tactical IT plans.		

8. MITIGATION OF IT RISK USING COBIT AND VAL IT

Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk (cont.)

Essential Control	Control Reference	Control Title	COBIT Control Objective/Val IT Key Management Practice	Effect on Frequency	Effect on Impact	
7. State of infrastructure technology (cont.)						
	PO3	PO3.1	Technological Direction Planning	Analyse existing and emerging technologies, and plan which technological direction is appropriate to realise the IT strategy and the business systems architecture. Identify in the plan which technologies have the potential to create business opportunities. The plan should address systems architecture, technological direction, migration strategies and contingency aspects of infrastructure components.	Medium	
	AI3	AI3.1	Technological Infrastructure Acquisition Plan	Produce a plan for the acquisition, implementation and maintenance of the technological infrastructure that meets established business functional and technical requirements and is in accord with the organisation's technology direction.	Medium	
	AI3	AI3.2	Infrastructure Resource Protection and Availability	Implement internal control, security and auditability measures during configuration, integration and maintenance of hardware and infrastructure software to protect resources and ensure availability and integrity. Responsibilities for using sensitive infrastructure components should be clearly defined and understood by those who develop and integrate infrastructure components. Their use should be monitored and evaluated.	Medium	Medium
	DS13	DS13.5	Preventive Maintenance for Hardware	Define and implement procedures to ensure timely maintenance of infrastructure to reduce the frequency and impact of failure or performance degradation.	Medium	
8. Ageing of application software						
Yes	AI2	AI2.6	Major Upgrades to Existing Systems	In the event of major changes to existing systems that result in significant change in current designs and/or functionality, follow a similar development process as that used for the development of new systems.		High
Yes	AI2	AI2.10	Application Software Maintenance	Develop a strategy and plan for the maintenance of software applications.	Medium	High
	PO1	PO1.3	Assessment of Current Capability and Performance	Assess the current capability and performance of solution and service delivery to establish a baseline against which future requirements can be compared. Define performance in terms of IT's contribution to business objectives, functionality, stability, complexity, costs, strengths and weaknesses.		Medium
	PO1	PO1.4	IT Strategic Plan	Create a strategic plan that defines, in co-operation with relevant stakeholders, how IT goals will contribute to the enterprise's strategic objectives and related costs and risks. It should include how IT will support IT-enabled investment programmes, IT services and IT assets. IT should define how the objectives will be met, the measurements to be used and the procedures to obtain formal sign-off from the stakeholders. The IT strategic plan should cover investment/operational budget, funding sources, sourcing strategy, acquisition strategy, and legal and regulatory requirements. The strategic plan should be sufficiently detailed to allow for the definition of tactical IT plans.	Medium	
	PO3	PO3.1	Technological Direction Planning	Analyse existing and emerging technologies, and plan which technological direction is appropriate to realise the IT strategy and the business systems architecture. Identify in the plan which technologies have the potential to create business opportunities. The plan should address systems architecture, technological direction, migration strategies and contingency aspects of infrastructure components.		
	PO3	PO3.2	Technological Infrastructure Plan	Create and maintain a technology infrastructure plan that is in accordance with the IT strategic and tactical plans. The plan should be based on the technological direction and include contingency arrangements and direction for acquisition of technology resources. It should consider changes in the competitive environment, economies of scale for information systems staffing and investments, and improved interoperability of platforms and applications.		
	PO3	PO3.4	Technology Standards	To provide consistent, effective and secure technological solutions enterprisewide, establish a technology forum to provide technology guidelines, advice on infrastructure products and guidance on the selection of technology, and measure compliance with these standards and guidelines. This forum should direct technology standards and practices based on their business relevance, risks and compliance with external requirements.	Medium	

Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk (cont.)

Essential Control	Control Reference	Control Title	COBIT Control Objective/Val IT Key Management Practice	Effect on Frequency	Effect on Impact	
8. Ageing of application software (cont.)						
	AI1	AI1.3	Feasibility Study and Formulation of Alternative Courses of Action	Develop a feasibility study that examines the possibility of implementing the requirements. Business management, supported by the IT function, should assess the feasibility and alternative courses of action and make a recommendation to the business sponsor.	Medium	Medium
	AC4	AC4	Processing Integrity and Validity	Maintain the integrity and validity of data throughout the processing cycle. Detection of erroneous transactions does not disrupt the processing of valid transactions.	Medium	
	AC5	AC5	Output Review, Reconciliation and Error Handling	Establish procedures and associated responsibilities to ensure that output is handled in an authorised manner, delivered to the appropriate recipient, and protected during transmission; that verification, detection and correction of the accuracy of output occur; and that information provided in the output is used.	Medium	
9. Architectural agility and flexibility						
Yes	P03	P03.1	Technological Direction Planning	Analyse existing and emerging technologies, and plan which technological direction is appropriate to realise the IT strategy and the business systems architecture. Identify in the plan which technologies have the potential to create business opportunities. The plan should address systems architecture, technological direction, migration strategies and contingency aspects of infrastructure components.	High	
	P01	P01.2	Business-IT Alignment	Establish processes of bi-directional education and reciprocal involvement in strategic planning to achieve business and IT alignment and integration. Mediate between business and IT imperatives so priorities can be mutually agreed upon.	Medium	
	P02	P02.1	Enterprise Information Architecture Model	Establish and maintain an enterprise information model to enable application development and decision-supporting activities, consistent with IT plans as described in P01. The model should facilitate the optimal creation, use and sharing of information by the business in a way that maintains integrity and is flexible, functional, cost-effective, timely, secure and resilient to failure.	Medium	Medium
	P03	P03.5	IT Architecture Board	Establish an IT architecture board to provide architecture guidelines and advice on their application, and to verify compliance. This entity should direct IT architecture design, ensuring that it enables the business strategy and considers regulatory compliance and continuity requirements. This is related/linked to P02 <i>Define the information architecture.</i>	Medium	Medium
10. Regulatory compliance						
Yes	P06	P06.1	IT Policy and Control Environment	Define the elements of a control environment for IT, aligned with the enterprise's management philosophy and operating style. These elements should include expectations/requirements regarding delivery of value from IT investments, appetite for risk, integrity, ethical values, staff competence, accountability and responsibility. The control environment should be based on a culture that supports value delivery while managing significant risks, encourages cross-divisional co-operation and teamwork, promotes compliance and continuous process improvement, and handles process deviations (including failure) well.		High
Yes	ME3	ME3.1	Identification of External Legal, Regulatory and Contractual Compliance Requirements	Identify, on a continuous basis, local and international laws, regulations, and other external requirements that must be complied with for incorporation into the organisation's IT policies, standards, procedures and methodologies.	High	High
	ME3	ME3.3	Evaluation of Compliance With External Requirements	Confirm compliance of IT policies, standards, procedures and methodologies with legal and regulatory requirements.	Medium	
11. Software implementation						
Yes	AI2	AI2.8	Software Quality Assurance (QA)	Develop, resource and execute a software QA plan to obtain the quality specified in the requirements definition and the organisation's quality policies and procedures.		High
Yes	AI4	AI4.4	Knowledge Transfer to Operations and Support Staff	Transfer knowledge and skills to enable operations and technical support staff to effectively and efficiently deliver, support and maintain the system and associated infrastructure.	High	Medium

8. MITIGATION OF IT RISK USING COBIT AND VAL IT

Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk (cont.)

Essential Control	Control Reference	Control Title	COBIT Control Objective/Val IT Key Management Practice	Effect on Frequency	Effect on Impact
11. Software implementation (cont.)					
Yes	AI7	AI7.3	Implementation Plan	Establish an implementation and fallback/backout plan. Obtain approval from relevant parties.	High
Yes	AI7	AI7.7	Final Acceptance Test	Ensure that business process owners and IT stakeholders evaluate the outcome of the testing process as determined by the test plan. Remediate significant errors identified in the testing process, having completed the suite of tests identified in the test plan and any necessary regression tests. Following evaluation, approve promotion to production.	
	AI4	AI4.2	Knowledge Transfer to Business Management	Transfer knowledge to business management to allow those individuals to take ownership of the system and data, and exercise responsibility for service delivery and quality, internal control, and application administration.	Medium
	AI4	AI4.3	Knowledge Transfer to End Users	Transfer knowledge and skills to allow end users to effectively and efficiently use the system in support of business processes.	
	AI7	AI7.1	Training	Train the staff members of the affected user departments and the operations group of the IT function in accordance with the defined training and implementation plan and associated materials, as part of every information systems development, implementation or modification project.	Medium
	AI7	AI7.2	Test Plan	Establish a test plan based on organisationwide standards that defines roles, responsibilities, and entry and exit criteria. Ensure that the plan is approved by relevant parties.	Medium
	AI7	AI7.9	Post-implementation Review	Establish procedures in line with the organisational change management standards to require a post-implementation review as set out in the implementation plan.	Medium
	AC3	AC3	Accuracy, Completeness and Authenticity Checks	Ensure that transactions are accurate, complete and valid. Validate data that were input, and edit or return for correction as close to the point of origination as possible.	Medium
	AC4	AC4	Processing Integrity and Validity	Maintain the integrity and validity of data throughout the processing cycle. Detection of erroneous transactions does not disrupt the processing of valid transactions.	Medium
	AC5	AC5	Output Review, Reconciliation and Error Handling	Establish procedures and associated responsibilities to ensure that output is handled in an authorised manner, delivered to the appropriate recipient, and protected during transmission; that verification, detection and correction of the accuracy of output occurs; and that information provided in the output is used.	Medium
	AC6	AC6	Transaction Authentication and Integrity	Before passing transaction data between internal applications and business/operational functions (within or outside the enterprise), check data for proper addressing, authenticity of origin and integrity of content. Maintain authenticity and integrity during transmission or transport.	Medium
12. IT project termination					
Yes	PO10	PO10.13	Project Performance Measurement, Reporting and Monitoring	Measure project performance against key project performance scope, schedule, quality, cost and risk criteria. Identify any deviations from the plan. Assess the impact of deviations on the project and overall programme, and report results to key stakeholders. Recommend, implement and monitor remedial action, when required, in line with the programme and project governance framework.	High
Yes	PO10	PO10.14	Project Closure	Require that, at the end of each project, the project stakeholders ascertain whether the project delivered the planned results and benefits. Identify and communicate any outstanding activities required to achieve the planned results of the project and the benefits of the programme, and identify and document lessons learned for use on future projects and programmes.	High

Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk (cont.)

Essential Control	Control Reference	Control Title	COBIT Control Objective/Val IT Key Management Practice	Effect on Frequency	Effect on Impact
12. IT project termination (cont.)					
Yes	IM10	IM10.1	Retire the Programme	High	High
	P04	P04.3	IT Steering Committee	Medium	Medium
	P05	P05.3	IT Budgeting		
	P05	P05.4	Cost Management		Medium
	ME1	ME1.2	Definition and Collection of Monitoring Data	Medium	
	VG5	VG5.3	Define Reporting Methods and Techniques	Medium	
	IM9	IM9.1	Monitor and Report on Programme (solution delivery) Performance		High

8. MITIGATION OF IT RISK USING COBIT AND VAL IT

Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk (cont.)

Essential Control	Control Reference	Control Title	COBIT Control Objective/Val IT Key Management Practice	Effect on Frequency	Effect on Impact	
13. IT project economics						
Yes	P05	P05.4	Cost Management	Implement a cost management process comparing actual costs to budgets. Costs should be monitored and reported. Where there are deviations, these should be identified in a timely manner and the impact of those deviations on programmes should be assessed. Together with the business sponsor of those programmes, appropriate remedial action should be taken and, if necessary, the programme business case should be updated.	High	High
Yes	P010	P010.13	Project Performance Measurement, Reporting and Monitoring	Measure project performance against key project performance scope, schedule, quality, cost and risk criteria. Identify any deviations from the plan. Assess the impact of deviations on the project and overall programme, and report results to key stakeholders. Recommend, implement and monitor remedial action, when required, in line with the programme and project governance framework.	High	Medium
	P04	P04.3	IT Steering Committee	Establish an IT steering committee (or equivalent) composed of executive, business and IT management to: <ul style="list-style-type: none"> • Determine prioritisation of IT-enabled investment programmes in line with the enterprise's business strategy and priorities • Track status of projects and resolve resource conflicts • Monitor service levels and service improvements 		Medium
	VG5	VG5.3	Define Reporting Methods and Techniques	Relevant portfolio, programme and IT (technological and functional) performance should be reported to the board and executive management in a timely and accurate manner. Management reports of the enterprise's progress towards identified goals should be provided for review by senior management. Status reports should include the extent to which planned objectives have been achieved, deliverables obtained, performance targets met and risks mitigated. Reporting should be integrated amongst IT and other business functions so inter-relationships are clear.	Medium	Medium
14. Project delivery						
Yes	P010	P010.13	Project Performance Measurement, Reporting and Monitoring	Measure project performance against key project performance scope, schedule, quality, cost and risk criteria. Identify any deviations from the plan. Assess the impact of deviations on the project and overall programme, and report results to key stakeholders. Recommend, implement and monitor remedial action, when required, in line with the programme and project governance framework.		High
Yes	P010	P010.14	Project Closure	Require that, at the end of each project, the project stakeholders ascertain whether the project delivered the planned results and benefits. Identify and communicate any outstanding activities required to achieve the planned results of the project and the benefits of the programme, and identify and document lessons learned for use on future projects and programmes.	Medium	High
Yes	IM9	IM9.1	Monitor and Report on Programme (solution delivery) Performance	Monitor the performance of the overall programme, and the projects within the programme, including the contributions of the business and IT functions to the projects, and report to the ISB and the executives in a timely, complete and accurate fashion. Reporting may include performance against the programme plan in terms of schedule, funding and completeness and quality of functionality, user satisfaction, and the status of business and IT function internal controls, including the continuing acceptance of accountabilities for delivering capabilities.		High
	IM4	IM4.2	Develop a Benefits Realisation Plan	For each key outcome, identify and document current baseline and target performance to be achieved; the method for measuring each key outcome; the identified and accepted accountability for achieving the outcome; the expected delivery schedule; and the monitoring process, which should include a detailed benefits register, along with an explanation of the risks that may threaten the achievement of each key outcome and how those risks will be mitigated.	Medium	
15. Project quality						
Yes	P08	P08.3	Development and Acquisition Standards	Adopt and maintain standards for all development and acquisition that follow the life cycle of the ultimate deliverable, and include sign-off at key milestones based on agreed-upon sign-off criteria. Consider software coding standards; naming conventions; file formats; schema and data dictionary design standards; user interface standards; interoperability; system performance efficiency; scalability; standards for development and testing; validation against requirements; test plans; and unit, regression and integration testing.		High
Yes	P010	P010.10	Project Quality Plan	Prepare a quality management plan that describes the project quality system and how it will be implemented. The plan should be formally reviewed and agreed to by all parties concerned and then incorporated into the integrated project plan.		High

Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk (cont.)

Essential Control	Control Reference	Control Title	COBIT Control Objective/Val IT Key Management Practice	Effect on Frequency	Effect on Impact
15. Project quality (cont.)					
	P03	P03.4	Technology Standards	To provide consistent, effective and secure technological solutions enterprisewide, establish a technology forum to provide technology guidelines, advice on infrastructure products and guidance on the selection of technology, and measure compliance with these standards and guidelines. This forum should direct technology standards and practices based on their business relevance, risks and compliance with external requirements.	Medium
	P010	P010.4	Stakeholder Commitment	Obtain commitment and participation from the affected stakeholders in the definition and execution of the project within the context of the overall IT-enabled investment programme.	Medium
	P010	P010.14	Project Closure	Require that, at the end of each project, the project stakeholders ascertain whether the project delivered the planned results and benefits. Identify and communicate any outstanding activities required to achieve the planned results of the project and the benefits of the programme, and identify and document lessons learned for use on future projects and programmes.	Medium
16. Selection/performance of third-party suppliers					
Yes	AI5	AI5.3	Supplier Selection	Select suppliers according to a fair and formal practice to ensure a viable best fit based on specified requirements. Requirements should be optimised with input from potential suppliers.	Medium
Yes	DS2	DS2.2	Supplier Relationship Management	Formalise the relationship management process for each supplier. The relationship owners should liaise on customer and supplier issues and ensure the quality of the relationship based on trust and transparency (e.g., through SLAs).	High
Yes	DS2	DS2.3	Supplier Risk Management	Identify and mitigate risks relating to suppliers' ability to continue effective service delivery in a secure and efficient manner on a continual basis. Ensure that contracts conform to universal business standards in accordance with legal and regulatory requirements. Risk management should further consider non-disclosure agreements (NDAs), escrow contracts, continued supplier viability, compliance with security requirements, alternative suppliers, penalties and rewards, etc.	High
Yes	DS2	DS2.4	Supplier Performance Monitoring	Establish a process to monitor service delivery to ensure that the supplier is meeting current business requirements and continuing to adhere to the contract agreements and SLAs, and that performance is competitive with alternative suppliers and market conditions.	High
	AI5	AI5.1	Procurement Control	Develop and follow a set of procedures and standards that is consistent with the business organisation's overall procurement process and acquisition strategy to acquire IT-related infrastructure, facilities, hardware, software and services needed by the business.	Medium
	AI5	AI5.2	Supplier Contract Management	Set up a procedure for establishing, modifying and terminating contracts for all suppliers. The procedure should cover, at a minimum, legal, financial, organisational, documentary, performance, security, intellectual property, and termination responsibilities and liabilities (including penalty clauses). All contracts and contract changes should be reviewed by legal advisors.	Medium
	AI5	AI5.4	Resources Acquisition	Protect and enforce the organisation's interests in all acquisition contractual agreements, including the rights and obligations of all parties in the contractual terms for the acquisition of software, development resources, infrastructure and services.	Medium
17. Infrastructure theft					
Yes	P06	P06.3	IT Policies Management	Develop and maintain a set of policies to support IT strategy. These policies should include policy intent; roles and responsibilities; exception process; compliance approach; and references to procedures, standards and guidelines. Their relevance should be confirmed and approved regularly.	High
Yes	P07	P07.6	Personnel Clearance Procedures	Include background checks in the IT recruitment process. The extent and frequency of periodic reviews of these checks should depend on the sensitivity and/or criticality of the function and should be applied for employees, contractors and vendors.	High

8. MITIGATION OF IT RISK USING COBIT AND VAL IT

Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk (cont.)

Essential Control	Control Reference	Control Title	COBIT Control Objective/Val IT Key Management Practice	Effect on Frequency	Effect on Impact
17. Infrastructure theft (cont.)					
Yes	AI3	AI3.2	Infrastructure Resource Protection and Availability		High
Yes	DS6	DS6.4	Cost Model Maintenance		High
Yes	DS12	DS12.2	Physical Security Measures	Medium	High
	DS12	DS12.3	Physical Access		Medium
18. Destruction of infrastructure					
Yes	DS12	DS12.2	Physical Security Measures	High	
Yes	DS12	DS12.3	Physical Access	High	
Yes	DS12	DS12.5	Physical Facilities Management	High	
	DS12	DS12.4	Protection Against Environmental Factors	Medium	
19. IT staff					
Yes	P07	P07.1	Personnel Recruitment and Retention	High	
Yes	P07	P07.4	Personnel Training	High	Medium
Yes	P07	P07.5	Dependence Upon Individuals		High
	P04	P04.5	IT Organisational Structure		Medium
	P07	P07.8	Job Change and Termination		Medium

Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk (cont.)

Essential Control	Control Reference	Control Title	COBIT Control Objective/Val IT Key Management Practice	Effect on Frequency	Effect on Impact	
19. IT staff (cont.)						
	PM3	PM3.6	Create and Maintain an Inventory of IT Human Resources	Create and maintain an inventory of IT human resources currently available to the enterprise, their competencies, their current and committed assignments and their utilisation. Identify and pay special attention to key IT personnel who are currently available but are in short supply and might be needed.	Medium	Medium
	PM3	PM3.7	Understand the Current and Future Demand (for IT human resources)	Understand the current and future demand for IT human resources based on a current and a forward view of the investment portfolio. Identify and pay special attention to key IT personnel who are in short supply and who might be needed, especially those personnel who undertake day-to-day functions who might also be needed for undertaking additional work on investment programmes.	Medium	Medium
	PM3	PM3.8	Identify Shortfalls (between current and future IT human resource demand)	Identify shortfalls between the current and future IT human resource demand and current and planned IT human resource supply. Especially consider conflicts in demands between the needs of investment programmes and day-to-day workloads. Develop high-level sourcing strategies and plans to address the shortfall and any surpluses.	Medium	Medium
20. IT expertise and skills						
Yes	P07	P07.1	Personnel Recruitment and Retention	Maintain IT personnel recruitment processes in line with the organisation's personnel policies and procedures (e.g., hiring, positive work environment, orientation). Implement processes to ensure that the organisation has an appropriately deployed IT workforce with the skills necessary to achieve organisational goals.	High	
Yes	P07	P07.4	Personnel Training	Provide IT employees with appropriate orientation when hired and ongoing training to maintain their knowledge, skills, abilities, internal controls and security awareness at the level required to achieve organisational goals.	High	
Yes	P07	P07.5	Dependence Upon Individuals	Minimise the exposure to critical dependency on key individuals through knowledge capture (documentation), knowledge sharing, succession planning and staff backup.		High
Yes	P07	P07.7	Employee Job Performance Evaluation	Require a timely evaluation to be performed on a regular basis against individual objectives derived from the organisation's goals, established standards and specific job responsibilities. Employees should receive coaching on performance and conduct whenever appropriate.	Medium	High
	P07	P07.2	Personnel Competencies	Regularly verify that personnel have the competencies to fulfil their roles on the basis of their education, training and/or experience. Define core IT competency requirements and verify that they are being maintained, using qualification and certification programmes where appropriate.	Medium	
	P07	P07.8	Job Change and Termination	Take expedient actions regarding job changes, especially job terminations. Knowledge transfer should be arranged, responsibilities reassigned and access rights removed such that risks are minimised and continuity of the function is guaranteed.		Medium
	PM3	PM3.6	Create and Maintain an Inventory of IT Human Resources	Create and maintain an inventory of IT human resources currently available to the enterprise, their competencies, their current and committed assignments and their utilisation. Identify and pay special attention to key IT personnel who are currently available but are in short supply and might be needed.	Medium	Medium
	PM3	PM3.7	Understand the Current and Future Demand (for IT human resources)	Understand the current and future demand for IT human resources based on a current and a forward view of the investment portfolio. Identify and pay special attention to key IT personnel who are in short supply and who might be needed, especially those personnel who undertake day-to-day functions who might also be needed for undertaking additional work on investment programmes.	Medium	Medium
	PM3	PM3.8	Identify Shortfalls (between current and future IT human resource demand)	Identify shortfalls between the current and future IT human resource demand and current and planned IT human resource supply. Especially consider conflicts in demands between the needs of investment programmes and day-to-day workloads. Develop high-level sourcing strategies and plans to address the shortfall and any surpluses.	Medium	Medium

8. MITIGATION OF IT RISK USING COBIT AND VAL IT

Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk (cont.)

Essential Control	Control Reference	Control Title	COBIT Control Objective/Val IT Key Management Practice	Effect on Frequency	Effect on Impact	
21. Software integrity						
Yes	AI2	AI2.7	Development of Application Software	Ensure that automated functionality is developed in accordance with design specifications, development and documentation standards, QA requirements, and approval standards. Ensure that all legal and contractual aspects are identified and addressed for application software developed by third parties.		
Yes	AI2	AI2.10	Application Software Maintenance	Develop a strategy and plan for the maintenance of software applications.	High	
Yes	AI6	AI6.1	Change Standards and Procedures	Set up formal change management procedures to handle, in a standardised manner, all requests (including maintenance and patches) for changes to applications, procedures, processes, system and service parameters, and the underlying platforms.	High	Medium
Yes	AI7	AI7.9	Post-implementation Review	Establish procedures in line with the organisational change management standards to require a post-implementation review as set out in the implementation plan.		High
Yes	DS5	DS5.3	Identity Management	Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the person responsible for security. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement authentication and enforce access rights.	High	
Yes	DS9	DS9.3	Configuration Integrity Review	Periodically review the configuration data to verify and confirm the integrity of the current and historical configuration. Periodically review installed software against the policy for software usage to identify personal or unlicensed software or any software instances in excess of current license agreements. Report, act on and correct errors and deviations.		High
Yes	AC3	AC3	Accuracy, Completeness and Authenticity Checks	Ensure that transactions are accurate, complete and valid. Validate data that were input, and edit or return for correction as close to the point of origination as possible.	High	
Yes	AC4	AC4	Processing Integrity and Validity	Maintain the integrity and validity of data throughout the processing cycle. Detection of erroneous transactions does not disrupt the processing of valid transactions.	High	
Yes	AC5	AC5	Output Review, Reconciliation and Error Handling	Establish procedures and associated responsibilities to ensure that output is handled in an authorised manner, delivered to the appropriate recipient, and protected during transmission; that verification, detection and correction of the accuracy of output occurs; and that information provided in the output is used.	High	
Yes	AC6	AC6	Transaction Authentication and Integrity	Before passing transaction data between internal applications and business/operational functions (within or outside the enterprise), check data for proper addressing, authenticity of origin and integrity of content. Maintain authenticity and integrity during transmission or transport.	High	
	PO8	PO8.3	Development and Acquisition Standards	Adopt and maintain standards for all development and acquisition that follow the life cycle of the ultimate deliverable, and include sign-off at key milestones based on agreed-upon sign-off criteria. Consider software coding standards; naming conventions; file formats; schema and data dictionary design standards; user interface standards; interoperability; system performance efficiency; scalability; standards for development and testing; validation against requirements; test plans; and unit, regression and integration testing.	Medium	
	PO8	PO8.6	Quality Measurement, Monitoring and Review	Define, plan and implement measurements to monitor continuing compliance to the quality management system (QMS), as well as the value the QMS provides. Measurement, monitoring and recording of information should be used by the process owner to take appropriate corrective and preventive actions.	Medium	
	AI2	AI2.8	Software Quality Assurance (QA)	Develop, resource and execute a software QA plan to obtain the quality specified in the requirements definition and the organisation's quality policies and procedures.	Medium	

Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk (cont.)

Essential Control	Control Reference	Control Title	COBIT Control Objective/Val IT Key Management Practice	Effect on Frequency	Effect on Impact	
21. Software integrity (cont.)						
	DS5	DS5.9	Malicious Software Prevention, Detection and Correction	Put preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the organisation to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).	Medium	
22. Infrastructure (hardware)						
Yes	AI3	AI3.2	Infrastructure Resource Protection and Availability	Implement internal control, security and auditability measures during configuration, integration and maintenance of hardware and infrastructure software to protect resources and ensure availability and integrity. Responsibilities for using sensitive infrastructure components should be clearly defined and understood by those who develop and integrate infrastructure components. Their use should be monitored and evaluated.	High	
Yes	DS12	DS12.2	Physical Security Measures	Define and implement physical security measures in line with business requirements to secure the location and the physical assets. Physical security measures must be capable of effectively preventing, detecting and mitigating risks relating to theft, temperature, fire, smoke, water, vibration, terror, vandalism, power outages, chemicals or explosives.	High	
Yes	DS12	DS12.3	Physical Access	Define and implement procedures to grant, limit and revoke access to premises, buildings and areas according to business needs, including emergencies. Access to premises, buildings and areas should be justified, authorised, logged and monitored. This should apply to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.	High	
	DS9	DS9.3	Configuration Integrity Review	Periodically review the configuration data to verify and confirm the integrity of the current and historical configuration. Periodically review installed software against the policy for software usage to identify personal or unlicensed software or any software instances in excess of current license agreements. Report, act on and correct errors and deviations.	Medium	
23. Software performance						
Yes	AI2	AI2.10	Application Software Maintenance	Develop a strategy and plan for the maintenance of software applications.	High	
Yes	DS3	DS3.5	Monitoring and Reporting	Continuously monitor the performance and capacity of IT resources. Data gathered should serve two purposes: <ul style="list-style-type: none"> • To maintain and tune current performance within IT and address such issues as resilience, contingency, current and projected workloads, storage plans, and resource acquisition • To report delivered service availability to the business, as required by the SLAs Accompany all exception reports with recommendations for corrective action.	High	
Yes	DS10	DS10.2	Problem Tracking and Resolution	Ensure that the problem management system provides for adequate audit trail facilities that allow tracking, analysing and determining the root cause of all reported problems considering: <ul style="list-style-type: none"> • All associated configuration items • Outstanding problems and incidents • Known and suspected errors • Tracking of problem trends Identify and initiate sustainable solutions addressing the root cause, raising change requests via the established change management process. Throughout the resolution process, problem management should obtain regular reports from change management on progress in resolving problems and errors. Problem management should monitor the continuing impact of problems and known errors on user services. In the event that this impact becomes severe, problem management should escalate the problem, perhaps referring it to an appropriate board to increase the priority of the request for change (RFC) or to implement an urgent change as appropriate. Monitor the progress of problem resolution against SLAs.	High	Medium
	AI2	AI2.8	Software Quality Assurance (QA)	Develop, resource and execute a software QA plan to obtain the quality specified in the requirements definition and the organisation's quality policies and procedures.	Medium	Medium

8. MITIGATION OF IT RISK USING COBIT AND VAL IT

Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk (cont.)

Essential Control	Control Reference	Control Title	COBIT Control Objective/Val IT Key Management Practice	Effect on Frequency	Effect on Impact	
23. Software performance (cont.)						
	DS8	DS8.5	Reporting and Trend Analysis	Produce reports of service desk activity to enable management to measure service performance and service response times and to identify trends or recurring problems, so service can be continually improved.	Medium	
	AC1	AC1	Source Data Preparation and Authorisation	Ensure that source documents are prepared by authorised and qualified personnel following established procedures, taking into account adequate segregation of duties regarding the origination and approval of these documents. Errors and omissions can be minimised through good input form design. Detect errors and irregularities so they can be reported and corrected.	Medium	
	AC2	AC2	Source Data Collection and Entry	Establish that data input is performed in a timely manner by authorised and qualified staff. Correction and resubmission of data that were erroneously input should be performed without compromising original transaction authorisation levels. Where appropriate for reconstruction, retain original source documents for the appropriate amount of time.	Medium	
	AC3	AC3	Accuracy, Completeness and Authenticity Checks	Ensure that transactions are accurate, complete and valid. Validate data that were input, and edit or return for correction as close to the point of origination as possible.	Medium	
	AC4	AC4	Processing Integrity and Validity	Maintain the integrity and validity of data throughout the processing cycle. Detection of erroneous transactions does not disrupt the processing of valid transactions.	Medium	
	AC5	AC5	Output Review, Reconciliation and Error Handling	Establish procedures and associated responsibilities to ensure that output is handled in an authorised manner, delivered to the appropriate recipient, and protected during transmission; that verification, detection and correction of the accuracy of output occurs; and that information provided in the output is used.	Medium	
	AC6	AC6	Transaction Authentication and Integrity	Before passing transaction data between internal applications and business/operational functions (within or outside the enterprise), check data for proper addressing, authenticity of origin and integrity of content. Maintain authenticity and integrity during transmission or transport.	Medium	
24. System capacity						
Yes	DS3	DS3.1	Performance and Capacity Planning	Establish a planning process for the review of performance and capacity of IT resources to ensure that cost-justifiable capacity and performance are available to process the agreed-upon workloads as determined by the SLAs. Capacity and performance plans should leverage appropriate modelling techniques to produce a model of the current and forecasted performance, capacity and throughput of the IT resources.	High	
	AI3	AI3.3	Infrastructure Maintenance	Develop a strategy and plan for infrastructure maintenance, and ensure that changes are controlled in line with the organisation's change management procedure. Include periodic reviews against business needs, patch management, upgrade strategies, risks, vulnerabilities assessment and security requirements.	Medium	
	DS3	DS3.2	Current Performance and Capacity	Assess current performance and capacity of IT resources to determine if sufficient capacity and performance exist to deliver against agreed-upon service levels.		
	DS3	DS3.3	Future Performance and Capacity	Conduct performance and capacity forecasting of IT resources at regular intervals to minimise the risk of service disruptions due to insufficient capacity or performance degradation, and identify excess capacity for possible redeployment. Identify workload trends and determine forecasts to be input to performance and capacity plans.		Medium
	DS3	DS3.4	IT Resources Availability	Provide the required capacity and performance, taking into account aspects such as normal workloads, contingencies, storage requirements and IT resource life cycles. Provisions such as prioritising tasks, fault-tolerance mechanisms and resource allocation practices should be made. Management should ensure that contingency plans properly address availability, capacity and performance of individual IT resources.	Medium	

Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk (cont.)

Essential Control	Control Reference		Control Title	COBIT Control Objective/Val IT Key Management Practice	Effect on Frequency	Effect on Impact
24. System capacity (cont.)						
	DS3	DS3.5	Monitoring and Reporting	Continuously monitor the performance and capacity of IT resources. Data gathered should serve two purposes: <ul style="list-style-type: none"> To maintain and tune current performance within IT and address such issues as resilience, contingency, current and projected workloads, storage plans, and resource acquisition To report delivered service availability to the business, as required by the SLAs Accompany all exception reports with recommendations for corrective action.	Medium	Medium
25. Ageing of infrastructural software						
Yes	PO3	PO3.2	Technological Infrastructure Plan	Create and maintain a technology infrastructure plan that is in accordance with the IT strategic and tactical plans. The plan should be based on the technological direction and include contingency arrangements and direction for acquisition of technology resources. It should consider changes in the competitive environment, economies of scale for information systems staffing and investments, and improved interoperability of platforms and applications.	High	Medium
Yes	PO3	PO3.5	IT Architecture Board	Establish an IT architecture board to provide architecture guidelines and advice on their application, and to verify compliance. This entity should direct IT architecture design, ensuring that it enables the business strategy and considers regulatory compliance and continuity requirements. This is related/linked to PO2 <i>Define the information architecture.</i>	High	
Yes	AI1	AI1.1	Definition and Maintenance of Business Functional and Technical Requirements	Identify, prioritise, specify and agree on business functional and technical requirements, covering the full scope of all initiatives required to achieve the expected outcomes of the IT-enabled investment programme.	High	
Yes	AI3	AI3.3	Infrastructure Maintenance	Develop a strategy and plan for infrastructure maintenance, and ensure that changes are controlled in line with the organisation's change management procedure. Include periodic reviews against business needs, patch management, upgrade strategies, risks, vulnerabilities assessment and security requirements.	Medium	High
	AI3	AI3.1	Technological Infrastructure Acquisition Plan	Produce a plan for the acquisition, implementation and maintenance of the technological infrastructure that meets established business functional and technical requirements and is in accord with the organisation's technology direction.	Medium	
	AI3	AI3.2	Infrastructure Resource Protection and Availability	Implement internal control, security and auditability measures during configuration, integration and maintenance of hardware and infrastructure software to protect resources and ensure availability and integrity. Responsibilities for using sensitive infrastructure components should be clearly defined and understood by those who develop and integrate infrastructure components. Their use should be monitored and evaluated.	Medium	Medium
26. Malware						
Yes	DS5	DS5.5	Security Testing, Surveillance and Monitoring	Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited in a timely manner to ensure that the approved enterprise's information security baseline is maintained. A logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.	High	
Yes	DS5	DS5.9	Malicious Software Prevention, Detection and Correction	Put preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the organisation to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).	High	High
	PO6	PO6.3	IT Policies Management	Develop and maintain a set of policies to support IT strategy. These policies should include policy intent; roles and responsibilities; exception process; compliance approach; and references to procedures, standards and guidelines. Their relevance should be confirmed and approved regularly.	Medium	
	PO6	PO6.4	Policy, Standard and Procedures Rollout	Roll out and enforce IT policies to all relevant staff, so they are built into and are an integral part of enterprise operations.	Medium	

8. MITIGATION OF IT RISK USING COBIT AND VAL IT

Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk (cont.)

Essential Control	Control Reference		Control Title	COBIT Control Objective/Val IT Key Management Practice	Effect on Frequency	Effect on Impact
27. Logical attacks						
Yes	PO6	PO6.3	IT Policies Management	Develop and maintain a set of policies to support IT strategy. These policies should include policy intent; roles and responsibilities; exception process; compliance approach; and references to procedures, standards and guidelines. Their relevance should be confirmed and approved regularly.	High	High
Yes	DS4	DS4.2	IT Continuity Plans	Develop IT continuity plans based on the framework and designed to reduce the impact of a major disruption on key business functions and processes. The plans should be based on risk understanding of potential business impacts and address requirements for resilience, alternative processing and recovery capability of all critical IT services. They should also cover usage guidelines, roles and responsibilities, procedures, communication processes, and the testing approach.		High
Yes	DS5	DS5.5	Security Testing, Surveillance and Monitoring	Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited in a timely manner to ensure that the approved enterprise's information security baseline is maintained. A logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.	High	
Yes	DS5	DS5.9	Malicious Software Prevention, Detection and Correction	Put preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the organisation to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).	High	
Yes	DS5	DS5.10	Network Security	Use security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion detection) to authorise access and control information flows from and to networks.	High	Medium
Yes	DS11	DS11.6	Security Requirements for Data Management	Define and implement policies and procedures to identify and apply security requirements applicable to the receipt, processing, storage and output of data to meet business objectives, the organisation's security policy and regulatory requirements.	High	
	PO4	PO4.9	Data and System Ownership	Provide the business with procedures and tools, enabling it to address its responsibilities for ownership of data and information systems. Owners should make decisions about classifying information and systems and protecting them in line with this classification.	Medium	
	PO6	PO6.4	Policy, Standard and Procedures Rollout	Roll out and enforce IT policies to all relevant staff, so they are built into and are an integral part of enterprise operations.	Medium	
	AI2	AI2.4	Application Security and Availability	Address application security and availability requirements in response to identified risks and in line with the organisation's data classification, information architecture, information security architecture and risk tolerance.		
	DS5	DS5.1	Management of IT Security	Manage IT security at the highest appropriate organisational level, so the management of security actions is in line with business requirements.	Medium	Medium
	DS5	DS5.3	Identity Management	Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security-responsible person. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement authentication and enforce access rights.	Medium	
	DS5	DS5.7	Protection of Security Technology	Make security-related technology resistant to tampering, and do not disclose security documentation unnecessarily.	Medium	
	AC1	AC1	Source Data Preparation and Authorisation	Ensure that source documents are prepared by authorised and qualified personnel following established procedures, taking into account adequate segregation of duties regarding the origination and approval of these documents. Errors and omissions can be minimised through good input form design. Detect errors and irregularities so they can be reported and corrected.	Medium	

Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk (cont.)

Essential Control	Control Reference	Control Title	COBIT Control Objective/Val IT Key Management Practice	Effect on Frequency	Effect on Impact	
27. Logical attacks (cont.)						
	AC2	AC2	Source Data Collection and Entry	Establish that data input is performed in a timely manner by authorised and qualified staff. Correction and resubmission of data that were erroneously input should be performed without compromising original transaction authorisation levels. Where appropriate for reconstruction, retain original source documents for the appropriate amount of time.	Medium	
	AC3	AC3	Accuracy, Completeness and Authenticity Checks	Ensure that transactions are accurate, complete and valid. Validate data that were input, and edit or return for correction as close to the point of origination as possible.	Medium	
	AC4	AC4	Processing Integrity and Validity	Maintain the integrity and validity of data throughout the processing cycle. Detection of erroneous transactions does not disrupt the processing of valid transactions.	Medium	
	AC5	AC5	Output Review, Reconciliation and Error Handling	Establish procedures and associated responsibilities to ensure that output is handled in an authorised manner, delivered to the appropriate recipient, and protected during transmission; that verification, detection and correction of the accuracy of output occurs; and that information provided in the output is used.	Medium	
	AC6	AC6	Transaction Authentication and Integrity	Before passing transaction data between internal applications and business/operational functions (within or outside the enterprise), check data for proper addressing, authenticity of origin and integrity of content. Maintain authenticity and integrity during transmission or transport.	Medium	
28. Information media						
Yes	DS11	DS11.2	Storage and Retention Arrangements	Define and implement procedures for effective and efficient data storage, retention and archiving to meet business objectives, the organisation's security policy and regulatory requirements.	High	Medium
Yes	DS11	DS11.4	Disposal	Define and implement procedures to ensure that business requirements for protection of sensitive data and software are met when data and hardware are disposed or transferred.	High	
Yes	DS11	DS11.5	Backup and Restoration	Define and implement procedures for backup and restoration of systems, applications, data and documentation in line with business requirements and the continuity plan.		High
	DS5	DS5.11	Exchange of Sensitive Data	Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin.	Medium	
	DS11	DS11.3	Media Library Management System	Define and implement procedures to maintain an inventory of stored and archived media to ensure their usability and integrity.	Medium	Medium
	DS11	DS11.6	Security Requirements for Data Management	Define and implement policies and procedures to identify and apply security requirements applicable to the receipt, processing, storage and output of data to meet business objectives, the organisation's security policy and regulatory requirements.	Medium	
	DS12	DS12.2	Physical Security Measures	Define and implement physical security measures in line with business requirements to secure the location and the physical assets. Physical security measures must be capable of effectively preventing, detecting and mitigating risks relating to theft, temperature, fire, smoke, water, vibration, terror, vandalism, power outages, chemicals or explosives.	Medium	
	DS12	DS12.3	Physical Access	Define and implement procedures to grant, limit and revoke access to premises, buildings and areas according to business needs, including emergencies. Access to premises, buildings and areas should be justified, authorised, logged and monitored. This should apply to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.	Medium	
	DS13	DS13.4	Sensitive Documents and Output Devices	Establish appropriate physical safeguards, accounting practices and inventory management over sensitive IT assets, such as special forms, negotiable instruments, special purpose printers or security tokens.	Medium	

8. MITIGATION OF IT RISK USING COBIT AND VAL IT

Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk (cont.)

Essential Control	Control Reference	Control Title	COBIT Control Objective/Val IT Key Management Practice	Effect on Frequency	Effect on Impact
29. Utilities performance					
Yes	DS4	DS4.8	IT Services Recovery and Resumption	Plan the actions to be taken for the period when IT is recovering and resuming services. This may include activation of backup sites, initiation of alternative processing, customer and stakeholder communication, and resumption procedures. Ensure that the business understands IT recovery times and the necessary technology investments to support business recovery and resumption needs.	High
Yes	DS12	DS12.5	Physical Facilities Management	Manage facilities, including power and communications equipment, in line with laws and regulations, technical and business requirements, vendor specifications, and health and safety guidelines.	High
	DS1	DS1.3	Service Level Agreements	Define and agree to SLAs for all critical IT services based on customer requirements and IT capabilities. This should cover customer commitments; service support requirements; quantitative and qualitative metrics for measuring the service approved by the stakeholders; funding and commercial arrangements, if applicable; and roles and responsibilities, including oversight of the SLA. Consider items such as availability, reliability, performance, capacity for growth, levels of support, continuity planning, security and demand constraints.	Medium
	DS3	DS3.4	IT Resources Availability	Provide the required capacity and performance, taking into account aspects such as normal workloads, contingencies, storage requirements and IT resource life cycles. Provisions such as prioritising tasks, fault-tolerance mechanisms and resource allocation practices should be made. Management should ensure that contingency plans properly address availability, capacity and performance of individual IT resources.	
	DS4	DS4.2	IT Continuity Plans	Develop IT continuity plans based on the framework and designed to reduce the impact of a major disruption on key business functions and processes. The plans should be based on risk understanding of potential business impacts and address requirements for resilience, alternative processing and recovery capability of all critical IT services. They should also cover usage guidelines, roles and responsibilities, procedures, communication processes, and the testing approach.	Medium
30. Industrial action					
	PO4	PO4.5	IT Organisational Structure	Establish an internal and external IT organisational structure that reflects business needs. In addition, put a process in place for periodically reviewing the IT organisational structure to adjust staffing requirements and sourcing strategies to meet expected business objectives and changing circumstances.	Medium
	PO7	PO7.1	Personnel Recruitment and Retention	Maintain IT personnel recruitment processes in line with the organisation's personnel policies and procedures (e.g., hiring, positive work environment, orientation). Implement processes to ensure that the organisation has an appropriately deployed IT workforce with the skills necessary to achieve organisational goals.	Medium
	PO7	PO7.5	Dependence Upon Individuals	Minimise the exposure to critical dependency on key individuals through knowledge capture (documentation), knowledge sharing, succession planning and staff backup.	Medium
31. Data(base) integrity					
Yes	PO4	PO4.9	Data and System Ownership	Provide the business with procedures and tools, enabling it to address its responsibilities for ownership of data and information systems. Owners should make decisions about classifying information and systems and protecting them in line with this classification.	High
Yes	AI6	AI6.1	Change Standards and Procedures	Set up formal change management procedures to handle, in a standardised manner, all requests (including maintenance and patches) for changes to applications, procedures, processes, system and service parameters, and the underlying platforms.	High
	PO2	PO2.2	Enterprise Data Dictionary and Data Syntax Rules	Maintain an enterprise data dictionary that incorporates the organisation's data syntax rules. This dictionary should enable the sharing of data elements amongst applications and systems, promote a common understanding of data amongst IT and business users, and prevent incompatible data elements from being created.	Medium

Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk (cont.)

Essential Control	Control Reference	Control Title	COBIT Control Objective/Val IT Key Management Practice	Effect on Frequency	Effect on Impact	
31. Data(base) integrity (cont.)						
	PO2	PO2.3	Data Classification Scheme	Establish a classification scheme that applies throughout the enterprise, based on the criticality and sensitivity (e.g., public, confidential, top secret) of enterprise data. This scheme should include details about data ownership; definition of appropriate security levels and protection controls; and a brief description of data retention and destruction requirements, criticality and sensitivity. It should be used as the basis for applying controls such as access controls, archiving or encryption.		
	PO8	PO8.3	Development and Acquisition Standards	Adopt and maintain standards for all development and acquisition that follow the life cycle of the ultimate deliverable, and include sign-off at key milestones based on agreed-upon sign-off criteria. Consider software coding standards; naming conventions; file formats; schema and data dictionary design standards; user interface standards; interoperability; system performance efficiency; scalability; standards for development and testing; validation against requirements; test plans; and unit, regression and integration testing.	Medium	
	AI6	AI6.2	Impact Assessment, Prioritisation and Authorisation	Assess all requests for change in a structured way to determine the impact on the operational system and its functionality. Ensure that changes are categorised, prioritised and authorised.		Medium
	DS9	DS9.3	Configuration Integrity Review	Periodically review the configuration data to verify and confirm the integrity of the current and historical configuration. Periodically review installed software against the policy for software usage to identify personal or unlicensed software or any software instances in excess of current license agreements. Report, act on and correct errors and deviations.	Medium	Medium
	DS11	DS11.2	Storage and Retention Arrangements	Define and implement procedures for effective and efficient data storage, retention and archiving to meet business objectives, the organisation's security policy and regulatory requirements.	Medium	
	DS11	DS11.3	Media Library Management System	Define and implement procedures to maintain an inventory of stored and archived media to ensure their usability and integrity.	Medium	
	DS11	DS11.5	Backup and Restoration	Define and implement procedures for backup and restoration of systems, applications, data and documentation in line with business requirements and the continuity plan.	Medium	
	DS11	DS11.6	Security Requirements for Data Management	Define and implement policies and procedures to identify and apply security requirements applicable to the receipt, processing, storage and output of data to meet business objectives, the organisation's security policy and regulatory requirements.	Medium	
32. Logical trespassing						
Yes	DS5	DS5.3	Identity Management	Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security-responsible person. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement authentication and enforce access rights.	High	
Yes	DS5	DS5.4	User Account Management	Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.	High	

8. MITIGATION OF IT RISK USING COBIT AND VAL IT

Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk (cont.)

Essential Control	Control Reference	Control Title	COBIT Control Objective/Val IT Key Management Practice	Effect on Frequency	Effect on Impact	
32. Logical trespassing (cont.)						
Yes	DS5	DS5.5	Security Testing, Surveillance and Monitoring	Test and monitor the IT security implementation in a proactive way. IT security should be recredited in a timely manner to ensure that the approved enterprise's information security baseline is maintained. A logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.	High	Medium
	PO4	PO4.9	Data and System Ownership	Provide the business with procedures and tools, enabling it to address its responsibilities for ownership of data and information systems. Owners should make decisions about classifying information and systems and protecting them in line with this classification.	Medium	
	PO4	PO4.14	Contracted Staff Policies and Procedures	Ensure that consultants and contract personnel who support the IT function know and comply with the organisation's policies for the protection of the organisation's information assets such that they meet agreed-upon contractual requirements.	Medium	Medium
	PO6	PO6.3	IT Policies Management	Develop and maintain a set of policies to support IT strategy. These policies should include policy intent; roles and responsibilities; exception process; compliance approach; and references to procedures, standards and guidelines. Their relevance should be confirmed and approved regularly.	Medium	
	PO6	PO6.4	Policy, Standard and Procedures Rollout	Roll out and enforce IT policies to all relevant staff, so they are built into and are an integral part of enterprise operations.	Medium	
	DS5	DS5.11	Exchange of Sensitive Data	Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin.	Medium	
	AC1	AC1	Source Data Preparation and Authorisation	Ensure that source documents are prepared by authorised and qualified personnel following established procedures, taking into account adequate segregation of duties regarding the origination and approval of these documents. Errors and omissions can be minimised through good input form design. Detect errors and irregularities so they can be reported and corrected.	Medium	
	AC2	AC2	Source Data Collection and Entry	Establish that data input is performed in a timely manner by authorised and qualified staff. Correction and resubmission of data that were erroneously input should be performed without compromising original transaction authorisation levels. Where appropriate for reconstruction, retain original source documents for the appropriate amount of time.	Medium	
	AC3	AC3	Accuracy, Completeness and Authenticity Checks	Ensure that transactions are accurate, complete and valid. Validate data that were input, and edit or return for correction as close to the point of origination as possible.	Medium	
	AC4	AC4	Processing Integrity and Validity	Maintain the integrity and validity of data throughout the processing cycle. Detection of erroneous transactions does not disrupt the processing of valid transactions.	Medium	
	AC5	AC5	Output Review, Reconciliation and Error Handling	Establish procedures and associated responsibilities to ensure that output is handled in an authorised manner, delivered to the appropriate recipient, and protected during transmission; that verification, detection and correction of the accuracy of output occurs; and that information provided in the output is used.	Medium	
	AC6	AC6	Transaction Authentication and Integrity	Before passing transaction data between internal applications and business/operational functions (in or outside the enterprise), check it for proper addressing, authenticity of origin and integrity of content. Maintain authenticity and integrity during transmission or transport.	Medium	
33. Operational IT errors						
Yes	PO7	PO7.4	Personnel Training	Provide IT employees with appropriate orientation when hired and ongoing training to maintain their knowledge, skills, abilities, internal controls and security awareness at the level required to achieve organisational goals.	High	Medium
Yes	DS4	DS4.8	IT Services Recovery and Resumption	Plan the actions to be taken for the period when IT is recovering and resuming services. This may include activation of backup sites, initiation of alternative processing, customer and stakeholder communication, and resumption procedures. Ensure that the business understands IT recovery times and the necessary technology investments to support business recovery and resumption needs.		High

Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk (cont.)

Essential Control	Control Reference	Control Title	COBIT Control Objective/Val IT Key Management Practice	Effect on Frequency	Effect on Impact
33. Operational IT errors (cont.)					
Yes	DS7	DS7.1	Identification of Education and Training Needs Establish and regularly update a curriculum for each target group of employees considering: <ul style="list-style-type: none"> • Current and future business needs and strategy • Value of information as an asset • Corporate values (ethical values, control and security culture, etc.) • Implementation of new IT infrastructure and software (i.e., packages, applications) • Current and future skills, competence profiles, and certification and/or credentialing needs as well as required reaccreditation • Delivery methods (e.g., classroom, web-based), target group size, accessibility and timing 		High
Yes	DS7	DS7.2	Delivery of Training and Education Based on the identified education and training needs, identify target groups and their members, efficient delivery mechanisms, teachers, trainers, and mentors. Appoint trainers and organise timely training sessions. Record registration (including prerequisites), attendance and training session performance evaluations.		High
Yes	DS13	DS13.1	Operations Procedures and Instructions Define, implement and maintain procedures for IT operations, ensuring that the operations staff members are familiar with all operations tasks relevant to them. Operational procedures should cover shift handover (formal handover of activity, status updates, operational problems, escalation procedures and reports on current responsibilities) to support agreed-upon service levels and ensure continuous operations.		High
	DS4	DS4.2	IT Continuity Plans Develop IT continuity plans based on the framework and designed to reduce the impact of a major disruption on key business functions and processes. The plans should be based on risk understanding of potential business impacts and address requirements for resilience, alternative processing and recovery capability of all critical IT services. They should also cover usage guidelines, roles and responsibilities, procedures, communication processes and the testing approach.		Medium
	AC1	AC1	Source Data Preparation and Authorisation Ensure that source documents are prepared by authorised and qualified personnel following established procedures, taking into account adequate segregation of duties regarding the origination and approval of these documents. Errors and omissions can be minimised through good input form design. Detect errors and irregularities so they can be reported and corrected.	Medium	
	AC2	AC2	Source Data Collection and Entry Establish that data input is performed in a timely manner by authorised and qualified staff. Correction and resubmission of data that were erroneously input should be performed without compromising original transaction authorisation levels. Where appropriate for reconstruction, retain original source documents for the appropriate amount of time.	Medium	
34. Contractual compliance					
Yes	AI5	AI5.2	Supplier Contract Management Set up a procedure for establishing, modifying and terminating contracts for all suppliers. The procedure should cover, at a minimum, legal, financial, organisational, documentary, performance, security, intellectual property, and termination responsibilities and liabilities (including penalty clauses). All contracts and contract changes should be reviewed by legal advisors.	High	Medium
Yes	DS2	DS2.2	Supplier Relationship Management Formalise the supplier relationship management process for each supplier. The relationship owners should liaise on customer and supplier issues and ensure the quality of the relationship based on trust and transparency (e.g., through SLAs).	High	High
Yes	ME3	ME3.1	Identification of External Legal, Regulatory and Contractual Compliance Requirements Identify, on a continuous basis, local and international laws, regulations, and other external requirements that must be complied with for incorporation into the organisation's IT policies, standards, procedures and methodologies.	High	Medium
Yes	ME3	ME3.3	Evaluation of Compliance With External Requirements Confirm compliance of IT policies, standards, procedures and methodologies with legal and regulatory requirements.	High	
Yes	ME3	ME3.4	Positive Assurance of Compliance Obtain and report assurance of compliance and adherence to all internal policies derived from internal directives or external legal, regulatory or contractual requirements, confirming that any corrective actions to address any compliance gaps have been taken by the responsible process owner in a timely manner.	High	High

8. MITIGATION OF IT RISK USING COBIT AND VAL IT

Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk (cont.)

Essential Control	Control Reference	Control Title	COBIT Control Objective/Val IT Key Management Practice	Effect on Frequency	Effect on Impact	
34. Contractual compliance (cont.)						
	PO6	PO6.1	IT Policy and Control Environment	Define the elements of a control environment for IT, aligned with the enterprise's management philosophy and operating style. These elements should include expectations/requirements regarding delivery of value from IT investments, appetite for risk, integrity, ethical values, staff competence, accountability and responsibility. The control environment should be based on a culture that supports value delivery while managing significant risks, encourages cross-divisional co-operation and teamwork, promotes compliance and continuous process improvement, and handles process deviations (including failure) well.	Medium	
	DS1	DS1.5	Monitoring and Reporting of Service Level Achievements	Continuously monitor specified service level performance criteria. Reports on achievement of service levels should be provided in a format that is meaningful to the stakeholders. The monitoring statistics should be analysed and acted upon to identify negative and positive trends for individual services as well as for services overall.		
35. Environmental						
Yes	AI3	AI3.1	Technological Infrastructure Acquisition Plan	Produce a plan for the acquisition, implementation and maintenance of the technological infrastructure that meets established business functional and technical requirements and is in accord with the organisation's technology direction.	High	
Yes	DS12	DS12.1	Site Selection and Layout	Define and select the physical sites for IT equipment to support the technology strategy linked to the business strategy. The selection and design of the layout of a site should take into account the risk associated with natural and man-made disasters, while considering relevant laws and regulations, such as occupational health and safety regulations.	High	
	PO3	PO3.1	Technological Direction Planning	Analyse existing and emerging technologies, and plan which technological direction is appropriate to realise the IT strategy and the business systems architecture. Identify in the plan which technologies have the potential to create business opportunities. The plan should address systems architecture, technological direction, migration strategies and contingency aspects of infrastructure components.	Medium	
	AI5	AI5.1	Procurement Control	Develop and follow a set of procedures and standards that is consistent with the business organisation's overall procurement process and acquisition strategy to acquire IT-related infrastructure, facilities, hardware, software and services needed by the business.	Medium	
36. Acts of nature						
Yes	DS4	DS4.8	IT Services Recovery and Resumption	Plan the actions to be taken for the period when IT is recovering and resuming services. This may include activation of backup sites, initiation of alternative processing, customer and stakeholder communication, and resumption procedures. Ensure that the business understands IT recovery times and the necessary technology investments to support business recovery and resumption needs.		High
Yes	DS12	DS12.1	Site Selection and Layout	Define and select the physical sites for IT equipment to support the technology strategy linked to the business strategy. The selection and design of the layout of a site should take into account the risk associated with natural and man-made disasters, while considering relevant laws and regulations, such as occupational health and safety regulations.	High	
Yes	DS12	DS12.4	Protection Against Environmental Factors	Design and implement measures for protection against environmental factors. Install specialised equipment and devices to monitor and control the environment.	High	
	DS4	DS4.2	IT Continuity Plans	Develop IT continuity plans based on the framework and designed to reduce the impact of a major disruption on key business functions and processes. The plans should be based on risk understanding of potential business impacts and address requirements for resilience, alternative processing and recovery capability of all critical IT services. They should also cover usage guidelines, roles and responsibilities, procedures, communication processes and the testing approach.		Medium
	DS12	DS12.2	Physical Security Measures	Define and implement physical security measures in line with business requirements to secure the location and the physical assets. Physical security measures must be capable of effectively preventing, detecting and mitigating risks relating to theft, temperature, fire, smoke, water, vibration, terror, vandalism, power outages, chemicals or explosives.	Medium	Medium

Page intentionally left blank

APPENDIX 1. RISK CONCEPTS IN RISK IT VS. OTHER STANDARDS AND FRAMEWORKS

APPENDIX 1. RISK CONCEPTS IN RISK IT VS. OTHER STANDARDS AND FRAMEWORKS

Comparison of Major Features

The Risk IT framework is built upon the six principles defined in *The Risk IT Framework*. **Figure 49** compares Risk IT to a number of other standards and frameworks in the area of (IT-related) risk management and shows to what extent they have included and implemented these principles. The reader can then decide, based upon his/her specific need, which framework or combination of frameworks to use, taking into account the legacy situation in his/her enterprise, the availability of the standard/framework and other factors.

The following frameworks are included in the comparison:

- Committee of Sponsoring Organizations (COSO) of the Treadway Commission, *Enterprise Risk Management—Integrated Framework*, 2004
- ISO/IEC, ISO/FDIS 31000, *Risk Management—Principles and Guidelines*, 2009
- Standards Australia, AS/NZS 4360:2004, *Australian/New Zealand Standard for Risk Management*, 2004
- AIRMIC, ALARM, IRM, ‘A Risk Management Standard’, 2002
- ISO/IEC 20000-1/2:2005: *Information Technology—Service Management—Part 1: Specification and Part 2: Code of Practice*, 2005
- Project Management Institute, *Project Management Body of Knowledge (PMBOK® Guide)*, 4th edition, 2008. This is described as ‘the sum of knowledge within the profession of project management’. It is an American National Standard, ANSI/PMI 99-001-2004.
- ISO/IEC 27005:2008 *Information Technology—Security Techniques—Information Security Risk Management*, 2008,
- ISO/IEC 27001:2005 *Information Technology—Security Techniques—Information Security Management Systems—Requirements* and
- ISO/IEC 27002:2005 *Information Technology—Security Techniques—Code of Practice for Information Security Management*, 2005

Figure 49 illustrates a principle-/feature-based comparison of the different frameworks.

- The first set of columns describes the principles/features and the fact that Risk IT covers these as a baseline for comparison.
- The second set of columns provides the mapping for the risk-management-related frameworks.
- The last set of columns describes the principle/feature coverage by domain-focused frameworks such as those for IT service management, project management and security. These frameworks, by definition of their scope, are not intended to cover the breadth of all IT risk but can be seen as complementary to Risk IT in providing more detail on how to manage IT risk in certain domains.

Figure 49—Risk Management Frameworks and Standards Compared

Principle/Feature	Risk IT	COSO ERM—Integrated Framework, 2004	ISO/FDIS 31000:2009	AS/NZS 4360:2004	ARMS, 2002	ISO 20000: 2005, Parts 1 and 2	PMBOK	ISO/IEC 27005:2008 ISO/IEC 27001:2005 ISO/IEC 27002:2005
Risk IT Principles								
Always connect to business objectives								
Align the management of IT-related business risk with overall ERM								
Balance the costs and benefits of managing risk								
Promote fair and open communication of IT risk								
Establish the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well-defined tolerance levels								
Are a continuous process and part of daily activity								
Additional Features								
Availability (to the general public)								
Comprehensive view on IT (related) risk								
Dedicated focus on risk management practices for specific IT areas (project management, service management, security, etc.)								
Provide a detailed process model with management guidelines and maturity models								
Legend: Blue—Principle/feature is fully covered. Gray—Principle/feature is partially covered. White—Principle/feature is not covered.								

The main characteristics of the Risk IT framework that set it apart from the other standards and frameworks include:

- Risk IT focuses on IT.
- Risk IT aligns with any of the generics/cross-domain enterprise risk standards.
- Risk IT seamlessly aligns with COBIT and Val IT (and from there to other standards, such as PMBOK and PRINCE2, as explained in the detailed COBIT mapping documents)¹⁵.
- Risk IT provides an umbrella for risk across other more focused IT frameworks, practices and process models (e.g., 2700x, 25999, DRI International [DRII] GAP, Business Continuity Institute [BCI] Good Practices, Information Security Forum [ISF], Information Technology Infrastructure Library [ITIL]).

¹⁵ IT Governance Institute, *COBIT® Mapping: Mapping of PMBOK With COBIT® 4.0*, ISACA, USA, 2006 and IT Governance Institute, *COBIT® Mapping: Mapping of PRINCE2 With COBIT® 4.0*, ISACA, USA, 2007

APPENDIX 2. RISK IT AND ISO 31000

The Risk IT framework is about IT risk—in other words, business risk related to the use of IT. The connection to business is clear in the principles on which the framework is built:

- Effective enterprise governance of IT risk:
 - Always connects to business objectives
 - Aligns the management of IT-related business risk with overall ERM
 - Balances the costs and benefits of managing risk
- Effective management of IT risk:
 - Promotes fair and open communication of IT risk
 - Establishes the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well-defined tolerance levels
 - Is a continuous process and part of daily activities

Based on these principles, a process model similar to the models in COBIT and Val IT has been developed around some core concepts.

Figures 50, 51 and 52 compare Risk IT to the ISO 31000 family of (prospective) standards and shows how Risk IT can help to implement these standards when it comes to IT and managing IT risk.

ISO 31000 Risk Management—Guidelines on Principles and Implementation of Risk Management

This standard contains three major clauses:

- Chapter 4, Principles for Managing Risk
- Chapter 5, Risk Management Framework
- Chapter 6, Process for Managing Risk

Principles for Managing Risk

Figure 50 contains the 11 risk management principles defined in ISO 31000 and shows how (and to what extent) Risk IT covers them.

Figure 50—Risk IT Coverage of ISO 31000 Risk Management Principle	
ISO 31000 Principles	Risk IT Coverage
Risk management should create value.	<ul style="list-style-type: none"> • Risk IT addresses both sides of risk management, i.e., protects against hazard and takes the opportunity to create value. • Risk IT principle 'always connect to business objectives'. • Risk IT principle 'balances the costs and benefits of managing risk'.
Risk management should be an integral part of organisational processes.	<ul style="list-style-type: none"> • Risk IT principle 'align the management of IT-related business risk with overall ERM'. • Risk IT principle 'are a continuous process and part of daily activities'. • The Risk IT framework includes a process model that allows integration into ERM processes and into various operational processes.
Risk management should be part of decision making.	<ul style="list-style-type: none"> • Risk IT dedicates an entire process to risk-aware business decisions. • The Risk IT maturity models illustrate how organisational decisions improve based on increasing and appropriate stakeholder involvement and improving quality and availability of risk analysis results. • The Risk IT process model provides a full set of RACI charts, indicating how risk management responsibilities can be assigned throughout the enterprise.
Risk management should explicitly address uncertainty.	<ul style="list-style-type: none"> • Risk IT recommends management practices that estimate IT risk based on scenarios of varying degrees of probability.
Risk management should be systemic and structured.	<ul style="list-style-type: none"> • The Risk IT process model is a systemic and structured way of managing risk. • In the process framework, Risk IT recommends management practices that establish an enterprise-specific IT risk management framework and supporting methods, structured in line with existing enterprisewide methods.
Risk management should be based on the best available information.	<ul style="list-style-type: none"> • Risk IT dedicates an entire process to collecting data in support of risk analysis and risk response decisions.
Risk management should be tailored.	<ul style="list-style-type: none"> • Risk IT principle 'always connect to business objectives'. • Risk IT recommends management practices that co-ordinate IT risk strategy and business risk strategy and adapt IT risk practices to enterprise risk practices.
Risk management should take into account human factors.	<ul style="list-style-type: none"> • Risk IT principle 'establish the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well-defined tolerance levels'. • Risk IT provides a technique to assess risk, where the human factor is an integral part.
Risk management should be transparent and inclusive.	<ul style="list-style-type: none"> • Risk IT principle 'promote fair and open communication of IT risk'. • Risk IT principle 'are a continuous process and part of daily activities'.

Figure 50—Risk IT Coverage of ISO 31000 Risk Management Principles (cont.)

ISO 31000 Principles	Risk IT Coverage
Risk management should be dynamic, iterative and responsive to change.	<ul style="list-style-type: none"> • Risk IT principle 'always connect to business objectives' • Risk IT dedicates an entire process to maintaining the risk profile of the enterprise so that, as the enterprise changes, IT risk management activities will stay in sync. • Risk IT dedicates an entire domain of three processes to risk response activities.
Risk management should be capable of continual improvement and enhancement.	<ul style="list-style-type: none"> • Risk IT includes management practices and information flows supporting process improvements based on data from incident/event post-mortems, adherence to policy and standards, and data on risk-aware culture change. • The Risk IT process model includes goals and metrics that can be used to measure performance, and also includes a maturity model that can be used to enhance risk management processes.

Framework for Managing Risk

ISO 31000 defines a five-block risk management framework. **Figure 51** contains the five blocks and describes how Risk IT addresses each of them.

Figure 51—Risk IT Coverage of ISO 31000 Framework Components

ISO 31000 Framework Components	Risk IT Coverage
Mandate and commitment	<ul style="list-style-type: none"> • Risk IT includes practices to align IT risk management objectives and performance indicators with those of ERM. • Risk IT defines IT risk management roles and suggests the assignment of responsibility and accountability for key activities to these roles. • The Risk IT process model includes specific information to be communicated amongst the key management practices.
Framework design for managing risk	
1. Understanding the organisation and its environment	<ul style="list-style-type: none"> • Risk IT includes management to work with the broader ERM functions to understand the enterprise's external context. • Risk IT includes management practices to understand the internal context, which include determining where/how organisational processes rely on IT for success and comparing existing IT-related capabilities.
2. Risk management policy	<ul style="list-style-type: none"> • Risk IT includes management practices to align risk policies with risk appetite and tolerance. Risk IT includes escalation paths to deal with conflicting situations related to application of risk policy.
3. Integration into organisational processes	<ul style="list-style-type: none"> • Risk IT principle 'are a continuous process and part of daily activities'. • Risk IT dedicates an entire process to this: RG2 <i>Integrate with ERM</i>. • Risk IT includes detailed linkages to CoBIT and Val IT, which model a wide range of IT processes.
4. Accountability	<ul style="list-style-type: none"> • Risk IT defines IT risk management roles and suggests the assignment of responsibility and accountability for key activities to these roles. • Risk IT includes management practices for RG2.1 <i>Establish and maintain accountability for IT risk management</i>.
5. Resources	<ul style="list-style-type: none"> • Risk IT includes management practices for RG2.4 <i>Provide adequate resources for IT risk management</i>.
6. Establishing internal communication and reporting mechanisms	<ul style="list-style-type: none"> • Risk IT includes management practices for RG1.6 <i>Encourage effective communication of IT risk</i>. • The Risk IT process model includes specific information to be communicated amongst the key management practices. • There is a separate section in the framework on communication, with suggested information flows amongst different stakeholders.
7. Establishing external communication and reporting mechanisms	<ul style="list-style-type: none"> • Risk IT includes management practices to communicate ongoing risk management activities and communicate with stakeholders in the event of a crisis or contingency. • There is a separate section in the framework on communication, with suggested information flows amongst different stakeholders.
Implementing risk management	
1. Implementing the framework for managing risk	<ul style="list-style-type: none"> • ISACA will soon release an update to the <i>IT Governance Implementation Guide</i> titled <i>Implementing and Continually Improving IT Governance</i> and it will factor in Risk IT content.
2. Implementing the risk management process	<ul style="list-style-type: none"> • Risk IT includes management practices to develop IT risk management methods based on the Risk IT framework. • Risk IT includes a practitioner guide to help enterprises develop leading-practice IT risk management techniques to embed at the enterprise levels suggested by the Risk IT process model.

Figure 51—Risk IT Coverage of ISO 31000 Framework Components (cont.)

ISO 31000 Framework Components	Risk IT Coverage
Monitoring and review of the framework	<ul style="list-style-type: none"> • Risk IT includes practices to 'Provide independent assurance over IT risk management'
Continual improvement of the framework	<ul style="list-style-type: none"> • Risk IT includes management practices and information flows supporting process improvements based on data from incident/event post-mortems, adherence to policy and standards, and data on risk-aware culture change.

Process for Managing Risk

ISO 31000 describes six major components of risk management processes. **Figure 52** lists each of these components and describes how (and where) Risk IT covers the component.

Figure 52—Risk IT Coverage of ISO 31000 Risk Management Processes

ISO 31000 Risk Management Process	Risk IT Coverage
Communication and consultation	<ul style="list-style-type: none"> • Risk IT includes management practices for RG1.6 <i>Encourage effective communication of IT risk</i>. • The Risk IT process model includes specific information to be communicated amongst the key management practices.
Establishing the context	
1. Establishing the external context	<ul style="list-style-type: none"> • Risk IT includes management to work with the broader ERM functions to understand the enterprise's external context.
2. Establishing the internal context	<ul style="list-style-type: none"> • Risk IT includes management practices to understand the internal context, which include determining where/how organisational processes rely on IT for success and comparing them to existing IT-related capabilities. • <i>The Risk IT Practitioner Guide</i> contains guidance on which external factors to include in risk assessment activities.
3. Establishing the context of the risk management process	<ul style="list-style-type: none"> • Risk IT features a Risk Governance (RG) domain to help ensure that the risk management approach adopted is appropriate to the situation of the enterprise and to the risks affecting the achievement of its objectives. The RG domain includes process goals for: <ul style="list-style-type: none"> – RG1: Ensure that risk management activities align with the enterprise's objective capacity for IT-related loss and leadership's subjective tolerance of it. – RG2: Integrate the IT risk strategy and operations with the business strategic risk decisions that have been made at the enterprise level. – RG3: Ensure that enterprise decisions consider the full range of opportunities and consequences from reliance on IT for success.
4. Developing risk criteria	<ul style="list-style-type: none"> • <i>The Risk IT Practitioner Guide</i> provides guidance for enterprises to develop their specific risk criteria, such as measurement of consequences, defining business impact, establishing risk tolerance thresholds and risk aggregation. • The Risk IT process model includes management practices to establish risk criteria.
Risk assessment	
1. Risk identification	<ul style="list-style-type: none"> • Risk IT includes management practices to identify risks to key enterprise services and products that rely on IT and to identify risk factors that contributed to historical incidents and events. • <i>The Risk IT Practitioner Guide</i> includes specific techniques to identify scenarios based on threat types, actors, actions, etc.
2. Risk analysis	<ul style="list-style-type: none"> • Risk IT features an entire process to analyse risk with the goal of 'develop useful information to support risk decisions that take into account the business relevance of risk factors'.
3. Risk evaluation	<ul style="list-style-type: none"> • The Risk IT process model feeds the decision support data from risk analysis to the RG domain for decisions and prioritisation of risk response actions.

Figure 52—Risk IT Coverage of ISO 31000 Risk Management Processes (cont.)

ISO 31000 Risk Management Process	Risk IT Coverage
Risk treatment	
1. Selection of options	<ul style="list-style-type: none"> • Risk IT includes guidance on the common response options and how they apply to an IT context.
2. Preparing and implementing risk treatment plans	<ul style="list-style-type: none"> • Risk IT links into the portfolio management activities established by Val IT.
Recording the risk management process	<ul style="list-style-type: none"> • Risk IT includes management practices to track key risk decisions and specifies inputs and outputs amongst its management practices.
Monitoring and review	<ul style="list-style-type: none"> • Risk IT includes practices to 'Provide independent assurance over IT risk management' • Risk IT includes management practices and information flows supporting process improvements based on data from incident/event post-mortems, adherence to policy and standards, and data on risk-aware culture change. • The Risk IT process model includes goals and metrics that can be used to measure performance and a maturity model to set a road map for improving risk management processes.

Conclusion

Risk IT addresses all ISO 31000 principles through the Risk IT principles themselves, its conceptual design, or the process model. In addition, the framework and process model aspects are covered in greater detail by *The Risk IT Framework*. All elements are included in Risk IT and are often expanded on or elaborated in greater detail, specifically for IT risk management.

APPENDIX 3. RISK IT AND ISO 27005

ISO/IEC 27005:2008, IT—Security Techniques—Information Security Risk Management

ISO/IEC 27005:2008, *Information Technology—Security Techniques—Information Security Risk Management* (referred to hereafter as ISO 27005), defines an information security risk management process that includes the following process steps:

- Context establishment
- Risk assessment
 - Risk analysis
 - Risk identification
 - Risk estimation
 - Risk evaluation
- Risk treatment
- Risk acceptance
- Risk communication
- Risk monitoring and review

Comparison of ISO 27005 and Risk IT

Figure 53 highlights the different process steps of ISO 27005, a summary of the important concepts of these process steps as well as how (and to what extent) Risk IT covers them.

Overall, it can be noted that the process as defined in ISO 27005 is fully covered by the different processes and practices of the Risk IT process model. The Risk IT model provides more extensive guidance and includes areas not covered by ISO 27005, such as risk governance and reacting to events.

The fundamental difference between the two frameworks is that the Risk IT coverage addresses all IT risk, whereas ISO 27005 focuses specifically on information security risks. ISO 27005 defines information security risk as ‘the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation’. However, the broad definition of IT risk within Risk IT is that it is the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.

Figure 53—Risk IT Coverage of ISO 27005 Process Steps

ISO 27005 Process Step	Important Concepts of the Component	Risk IT Coverage
Context establishment	This process step includes: <ul style="list-style-type: none"> • The development of basic criteria necessary for information security risk management, such as risk evaluation criteria, impact criteria and risk assessment criteria • Defining the scope and boundaries to ensure that all relevant assets are taken into account • Establishing an appropriate organisation for operating information security risk management 	<ul style="list-style-type: none"> • This process step is included in the RG and RE domains of Risk IT: <ul style="list-style-type: none"> – Basic criteria—RG2.3 <i>Adapt IT risk practices to enterprise risk practices.</i> and RG1.2 <i>Propose IT risk tolerance thresholds</i> describe the development of the basic criteria needed for proper IT risk management. – Scoping is incorporated by RE2.1 <i>Define IT risk analysis scope.</i> – Organisation is covered by RG2.1 <i>Establish and maintain accountability for IT risk management</i> and RG2.4 <i>Provide adequate resources for IT risk management.</i> • Additionally for the scoping part, chapter 1 of <i>The Risk IT Practitioner Guide</i> provides extended guidance on IT risk management establishment. • Throughout the entire process model, RACI charts are used to describe a good practice’s roles and responsibilities.
Risk assessment	Risk assessment determines the value of the information assets, identifies the applicable threats and vulnerabilities that exist (or could exist), identifies the existing controls and their effect on the risk identified, determines the potential consequences, and finally prioritises the derived risks and ranks them against the risk evaluation criteria set in the context establishment. This process step includes the analysis and evaluation of risks (see Risk Analysis).	<ul style="list-style-type: none"> • The RE 2 <i>Analyse risk</i> process as described in Risk IT is similar to the ISO 27005 ‘Risk assessment’ process. This RE2 process includes: <ul style="list-style-type: none"> – RE2.1 <i>Define IT risk analysis scope.</i> – RE2.2 <i>Estimate IT risk.</i> – RE2.3 <i>Identify risk response options.</i> – RE2.4 <i>Perform a peer review of IT risk analysis.</i> • <i>The Risk IT Practitioner Guide</i> provides an example of a risk assessment workflow. In general, the elements as described in the ISO 27005 process are all included in the workflow; however, some are structured and named differently, as described in this table.

Figure 53—Risk IT Coverage of ISO 27005 Process Steps (cont.)

ISO 27005 Process Step	Important Concepts of the Component	Risk IT Coverage
Risk analysis	This is composed of the process of identifying and estimating risks (see 'Risk identification' and 'Risk estimation').	<ul style="list-style-type: none"> • RE2 <i>Analyse risk</i> comprises more than what is described by the ISO 27005 process step. RE2 has as its objective developing useful information to support risk decisions that take into account the business relevance of risk factors. • RE1 <i>Collect data</i> serves as input to the analysis of risk (e.g., identifying risk factors, collecting data on the external environment).
Risk identification	Risk identification includes the identification of: <ul style="list-style-type: none"> • Assets • Threats • Existing controls • Vulnerabilities • Consequences 	<ul style="list-style-type: none"> • This process is included in RE2.2 <i>Estimate IT risk</i>. • The sequence used in ISO 27005 to identify risks is partly aligned to the Risk IT approach. The identification of risk comprises the following elements in Risk IT: <ul style="list-style-type: none"> – Risk scenarios – Risk factors • In addition, <i>The Risk IT Practitioner Guide</i> describes a practical technique for identifying risks, namely risk scenario development (see chapter 5).
Risk estimation	The 'Risk estimation' process step includes the following important concepts: <ul style="list-style-type: none"> • Assessment of consequences • Assessment of incident likelihoods • Qualitative/quantitative risk estimation 	<ul style="list-style-type: none"> • RE2.2 <i>Estimate IT risk</i> is the Risk IT equivalent of this process step. • Additional information on how to describe frequency and impact. (Risk IT's equivalents for consequence and likelihood) can be found in <i>The Risk IT Practitioner Guide</i>, chapter 4.
Risk evaluation	In this step, the evaluation criteria and acceptance criteria are used to evaluate the risk. The output is a prioritised list of risks.	<ul style="list-style-type: none"> • This process step is included in RE2.2 <i>Estimate IT risk</i>.
Risk treatment	Risk treatment options include: <ul style="list-style-type: none"> • Risk reduction • Risk retention • Risk avoidance • Risk transfer Once the risk treatment plan has been defined, residual risks need to be determined against the enterprise's risk acceptance criteria.	<ul style="list-style-type: none"> • The treatment of identified risks is included in the RE2.3 <i>Identify risk response options</i> as well as the RR2.3 <i>Respond to discovered risk exposure and opportunity</i> processes. • In addition, further practical guidance is provided in <i>The Risk IT Practitioner Guide</i>, chapter 6.
Risk acceptance	This step comprises the formal acceptance and recording of the suggested risk treatment and residual risk assessment by management.	RG3.4 <i>Accept IT risk</i> is the equivalent in Risk IT
Risk communication	This is a transversal process; information about risk should be exchanged and shared throughout all the steps of the risk management process.	<ul style="list-style-type: none"> • The Risk IT process model includes specific information to be communicated between the key management practices • RG1.5 <i>Promote IT risk-aware culture</i> and RG1.6 <i>Encourage effective communication of IT risk</i> focus on institutionalising the communication on risk. • It is also covered by RE3.6 <i>Develop IT risk indicators</i>. • Practical guidance on risk communication is included in <i>The Risk IT Practitioner Guide</i>, chapter 3.
Risk monitoring and review	Risk factors need to be reviewed to cope with the changing environment. The process and activities need to be updated as well. An overview of the complete risk picture needs to be maintained.	<ul style="list-style-type: none"> • Risk IT defines management and governance components of risk monitoring and review. • The continuous alignment of the existing risk management practices to various internal and external factors are included in RG2 <i>Integrate with ERM</i>. • The review of the risk analysis exercise is included in RE2.4 <i>Perform a peer review of IT risk analysis</i>. • Risk IT includes practices in RG2.5 to 'Provide independent assurance over IT risk management'

Conclusion

Risk IT addresses all of the components described within ISO 27005. Some of the elements are structured or named differently. Risk IT takes a broader view on IT risk management compared with ISO 27005, which is focused on the management of security-related risks. There is, therefore, a strong emphasis in Risk IT on processes and practices to ensure the alignment with business objectives, the acceptance throughout the enterprise and the completeness of the scope, amongst other factors.

APPENDIX 4. RISK IT AND COSO ERM

COSO Enterprise Risk Management—Integrated Framework

The Committee of Sponsoring Organizations (COSO) of the Treadway Commission's *Enterprise Risk Management—Integrated Framework*, also called COSO ERM, defines eight components with regard to the management of enterprise risk. These interrelated components are derived from the way management runs an enterprise and are integrated with the management process. The components are:

- Internal environment
- Objective setting
- Event identification
- Risk assessment
- Risk response
- Control activities
- Information and communication
- Monitoring

Components of COSO ERM

Figure 54 contains the eight components of enterprise risk management that COSO ERM has defined, a summary of the important concepts related to these components, as well as how (and to what extent) Risk IT covers them.

Figure 54—Risk IT Coverage of COSO ERM Components		
COSO ERM Component	Important Concepts of the Component	Risk IT Coverage
Internal environment	<p>This encompasses the tone of an enterprise, influencing the risk consciousness of its people, and is the basis for all other components of ERM, providing discipline and structure. Internal environment factors include an entity's risk management philosophy; its risk appetite; oversight by the board of directors; the integrity, ethical values, and competence of the entity's people; and the way management assigns authority and responsibility, and organises and develops its people.</p> <p>This component of ERM is focused on providing guidance to practitioners with regard to risk management and ensuring that ERM is a way of thinking that is fully embedded in the enterprise.</p>	<p>The concepts described in the chapter about internal environment are all inherently included throughout the Risk IT framework:</p> <ul style="list-style-type: none"> • Risk IT principle 'promote fair and open communication of IT risk'. • Risk IT principle 'establish the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well-defined tolerance levels' clarifies the duties of the top-level executive to institutionalise a risk-aware and risk-conscious culture. • The Risk IT process model includes a Risk Governance process RG1 <i>Establish and maintain a common risk view</i> linking it with the development of structures and practices in order to align the enterprise's risk-related activities. More specifically, RG1.4 covers the alignment of the IT risk policy with enterprise objectives. It is also covered by the process RG2 <i>Integrate with ERM</i>, which covers activities such as establishing enterprise accountability for managing IT risk. • An elaborated distribution of roles and responsibilities is described in chapter 5 of <i>The Risk IT Framework</i>. • Chapter 5 of <i>The Risk IT Framework</i> also covers the awareness and communication of risk, linking it to the promotion of a risk-aware culture. • <i>The Risk IT Practitioner Guide</i> provides guidance in chapter 1 on defining a risk universe and scoping risk management, risk appetite and risk tolerance, and the internal environment risk factors.

Figure 54—Risk IT Coverage of COSO ERM Components (cont.)

COSO ERM Component	Important Concepts of the Component	Risk IT Coverage
<p>Objective setting</p>	<p>COSO ERM states that objectives are set at the strategic level, establishing a basis for operations, reporting and compliance objectives. Every entity faces a variety of risks from external and internal sources, and a precondition to effective event identification, risk assessment and risk response is the establishment of objectives. Objectives are aligned with the entity's risk appetite, which drives risk-tolerance levels for the entity.</p>	<p>This is mostly related to the Risk Governance domain in Risk IT. The following parts of the publication are relevant, specifically for objective setting:</p> <ul style="list-style-type: none"> • Risk IT principle 'always connect to business objectives'. • Risk IT principle 'promote fair and open communication of IT risk'. • The Risk IT process model includes a Risk Governance process RG1 <i>Establish and maintain a common risk view</i>. The goal of this process is to ensure that risk management activities align with the enterprise's objective capacity for IT-related loss and leadership's subjective tolerance of it. • Chapter 5 of <i>The Risk IT Framework</i> covers the awareness and communication of risk. The table on communication to and from stakeholders clarifies the communication stream with regard to objectives. • Risk appetite and tolerance are discussed in <i>The Risk IT Framework</i>, chapter 5. Furthermore, in <i>The Risk IT Practitioner Guide</i>, chapter 2 is devoted to the further elaboration of these concepts in a more practical manner. <p>It is important, however, to acknowledge that within Risk IT, the setting of an enterprise's objectives is treated as an external input.</p>
<p>Event identification</p>	<p>In COSO ERM, this section deals with management identifying potential events that, if they occur, will affect the entity, and determining whether they represent opportunities or whether they might adversely affect the entity's ability to successfully implement strategy and achieve objectives. Events with negative impact represent risks that require management's assessment and response. Events with positive impacts represent opportunities that management channels back into the strategy and objective-setting processes. When identifying events, management considers a variety of internal and external factors that may give rise to risks and opportunities, in the context of the full scope of the enterprise.</p>	<p>Event identification has been further developed and extended in Risk IT. More specifically, the events are covered by the chapters on risk scenarios, which provide a specific technique of event identification that provides structures, components and guidance on building risk scenarios. Therefore, the following parts of the Risk IT family cover the event identification component:</p> <ul style="list-style-type: none"> • <i>The Risk IT Framework</i>, chapter 6, covers the basics of risk scenario development (including event identification). The practitioner guide also provides more hands-on guidance to developing scenarios. • The Risk IT process RG3 <i>Make risk-aware business decisions</i> has a goal that enterprise decisions consider the full range of opportunities and consequences from reliance on IT for success. • <i>The Risk IT Framework</i>, chapter 8, covers risk and opportunity management using CoBIT, Val IT and Risk IT. • In addition, opportunities are implied in a number of processes throughout the process model.

APPENDIX 4. RISK IT AND COSO ERM

Figure 54—Risk IT Coverage of COSO ERM Components (cont.)

COSO ERM Component	Important Concepts of the Component	Risk IT Coverage
<p>Risk assessment</p>	<p>COSO ERM defines risk assessment as allowing an entity to consider the extent to which potential events have an impact on achievement of objectives. Management assesses events from two perspectives—likelihood and impact—and normally uses a combination of qualitative and quantitative methods. The positive and negative impacts of potential events should be examined, individually or by category, across the entity. Risks are assessed on both an inherent and a residual basis.</p>	<ul style="list-style-type: none"> • RG1.1 <i>Perform enterprise IT risk assessment</i> describes an inherent risk assessment as a starting point. Outputs of enterprise IT risk assessment include elements for further development and management attention across the process model, such as: risk focus areas, measurements of risk, high level IT risk scenarios, and key services and supporting business process and systems. • The assessment of risk as described in COSO ERM is reflected and heavily extended in the Risk IT process RE2 <i>Analyse risk</i>. This process covers the steps, such as: <ul style="list-style-type: none"> – Define IT risk analysis scope. – Estimate IT risk. – Identify risk response options. – Review IT risk analysis. • RE3 <i>Maintain risk profile</i>, which has a goal of maintaining an up-to-date and complete inventory of known risks and attributes, including frequency and impact. • Risk IT elaborates on risk factors in chapter 6 of <i>The Risk IT Framework</i>. • <i>The Risk IT Practitioner Guide</i> provides an example of a risk analysis workflow (chapter 7). Section 4 of this guide deals with expressing and describing IT risk, amongst others, in terms of frequency and impact and guidance on qualitative and quantitative methods for risk analysis.
<p>Risk response</p>	<p>Having assessed relevant risks, management determines how it will respond. Responses include risk avoidance, reduction, sharing and acceptance. In considering its response, management assesses the effect on risk likelihood, impact, and costs and benefits, selecting a response that brings residual risk within desired risk tolerances. Management identifies any opportunities that might be available and takes an enterprise or portfolio view of risk, determining whether overall residual risk is within the entity's risk appetite.</p>	<ul style="list-style-type: none"> • An entire domain in Risk IT is dedicated to risk response (RR), providing fully developed processes for these activities. RR is fully aligned with this COSO ERM component. The RR domain covers the processes of RR1 <i>Articulate risk</i>, RR2 <i>Manage risk</i> and RR3 <i>React to events</i>. This process domain has a goal of ensuring that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities. • The Risk IT process RR2 <i>Manage risk</i> has a goal of ensuring that measures for seizing strategic opportunities and reducing risk to an acceptable level are managed as a portfolio. • In addition, chapter 6 of <i>The Risk IT Practitioner Guide</i> provides hands-on guidance to risk response and prioritisation.
<p>Control activities</p>	<p>Control activities are the policies and procedures that help ensure that management's risk responses are carried out. Control activities occur throughout the enterprise, at all levels and in all functions. They include a range of activities as diverse as approvals, authorisations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties. Important concepts in this context are type of activities, policies and procedures, and controls over information systems.</p>	<ul style="list-style-type: none"> • RR2 <i>Manage risk</i> covers activities for creating a risk and control baseline, as a basis for measurement. • Risk IT focuses less on providing extensive guidance on control activities since this is contained in the COBIT and Val IT frameworks. <i>The Risk IT Practitioner Guide</i> contains comprehensive links on mitigating IT risk using COBIT and Val IT. • <i>The Risk IT Framework</i>, chapter 8, covers risk and opportunity management using COBIT, Val IT and Risk IT.

Figure 54—Risk IT Coverage of COSO ERM Components (cont.)

COSO ERM Component	Important Concepts of the Component	Risk IT Coverage
Information and communication	<p>Pertinent information is identified, captured, and communicated in a form and time frame that enables people to carry out their responsibilities. Information systems use internally generated data, and information from external sources, providing information for managing risks and making informed decisions relative to objectives. Effective communication also occurs, flowing down, across and up the enterprise. There is also effective communication with external parties, such as customers, suppliers, regulators and shareholders.</p>	<ul style="list-style-type: none"> • Chapter 5 of <i>The Risk IT Framework</i> provides guidance on awareness and communication, including a table on communication flows with different stakeholders, both internal and external to the enterprise. This chapter also covers risk responsibility and accountability. • The Risk IT process RG1 <i>Establish and maintain a common risk</i> view covers promotion of an IT risk-aware culture and effective communication of IT risk. • The Risk IT process RE3 <i>Maintain risk profile</i>, amongst others, deals with designing and communicating IT risk indicators. • Throughout the process model, inputs and outputs have been defined for every process and related process details. These inputs and outputs illustrate the communication flows as well. • Chapter 3 of <i>The Risk IT Practitioner Guide</i> provides hands-on guidance on risk awareness, communication and reporting.
Monitoring	<p>In this section, COSO ERM deals with risk management being monitored, assessing the presence and functioning of its components over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. Ongoing monitoring occurs in the normal course of management activities. The scope and frequency of separate evaluations depends primarily on the assessment of risks and the effectiveness of ongoing monitoring procedures.</p>	<ul style="list-style-type: none"> • RR2.2 <i>Monitor operational alignment with risk tolerance thresholds</i> provides insight into the monitoring of control performance against a baseline and the application of KRIs • The review of the risk analysis exercise is included in RE2.4 'Perform a peer review of IT risk analysis'. • Risk IT includes practices in RG2.5 <i>Provide independent assurance over IT risk management</i>. • Risk IT includes management practices and information flows supporting process improvements based on lessons learned from risk events, policy exceptions, and data on risk-aware culture change. • The Risk IT process model includes goals and metrics that can be used to measure performance and a maturity model to set a road map for improving risk management processes.

Conclusion

Risk IT addresses all of the components defined in COSO ERM, sometimes extending the coverage of COSO ERM to the specifics of IT use in the enterprise. Although Risk IT focuses less on control, it provides linkages to control objectives in COBIT and management practices in the Val IT framework. The essentials with regard to both control and general risk management, as defined in COSO ERM, are present in Risk IT, either through the principles themselves, the framework's conceptual design, the process model or the additional guidance provided in *The Risk IT Framework* and *The Risk IT Practitioner Guide*.

APPENDIX 5. VOCABULARY COMPARISONS: RISK IT VS. ISO GUIDE 73 AND COSO ERM

APPENDIX 5. VOCABULARY COMPARISONS: RISK IT VS. ISO GUIDE 73 AND COSO ERM

Risk IT and ISO Guide 73 on Risk Management Vocabulary

ISO 27005 and ISO 31000 use the ISO/IEC Guide 73, Risk management—Vocabulary (the glossary publication overarching the risk management ISO publications) with regard to defining important concepts. Two exceptions exist: ‘impact’ and ‘information security risk’ as defined in the ISO 27005 document are not taken from Guide 73. A comparison of Guide 73 and Risk IT definitions is provided in **figure 55**.

This table comprises:

- Column 1—Guide 73 term
- Column 2—Guide 73 definition¹⁶
- Column 3—Explanation of the relevant Risk IT definition of the same term (labelled Identical, Implicit¹⁷, Absent or Equivalent)¹⁸
- Column 4—Risk IT definition
- Column 5—Comments (if relevant or required)

Figure 55—ISO Guide 73 and Risk IT Definition Comparisons

Guide 73 Concept	Definition in Guide 73	Disposition in Risk IT	Definition in Risk IT	Comment
Absolute risk	Level of risk without taking into account existing risk controls	Absent		This notion corresponds to the concept ‘inherent risk’. In general, Risk IT does not use this concept, except when the enterprise IT risk assessment is discussed.
Consequence	Outcome of an event affecting objectives	Implicit	N/A	Risk IT uses the concept ‘business impact’.
Control	Measures to modify risk	Implicit	N/A	Risk IT primarily links the IT risk of an organisation to the CoBIT and Val IT controls and management practices.
Event	Occurrence or change of a particular set of circumstances	Equivalent	Something that happens at a specific place and/or time	The term ‘scenario’ is used to describe ‘things happening’.
Exposure	Extent to which an organization is subject to an event	Implicit	N/A	The term ‘business impact’ is used instead.
External context	External environment in which the organization seeks to achieve its objective	Identical		The term is used as part of the risk factors.
Frequency	Measure of the likelihood of an event expressed as a number of events or outcomes per defined unit of time	Equivalent	A measure of the rate by which events occur over a certain period of time	
Heat map	Overview of the enterprise’s main risks plotted in its risk matrix	Equivalent		Risk IT uses the term ‘risk map’.
Impact	Adverse change to the level of business objectives achieved	Equivalent	Magnitude: A measure of the potential severity of loss or the potential gain from a realised IT-related event/scenario	Risk IT uses ‘magnitude’ instead of impact.
Incident	Event in which a loss occurred or could have occurred regardless of severity	Implicit	N/A	The term ‘materialisation of risk’ is used instead.
Information security risk (ISO 27005-specific)	Potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization	Equivalent	1. The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss of, or damage to, the assets 2. The potential of business objectives not being met	The ISO 27005 definition for information security risk is generally equivalent to the Risk IT definition for risk in general.

¹⁶ These definitions taken from Draft ISO Guide 73 are reproduced with the permission of the International Organization for Standardization (ISO). This draft guide can be obtained from any ISO member and from the web site of the ISO Central Secretariat at: www.iso.org. Copyright remains with ISO.

¹⁷ ‘Implicit’ means that the term does not exist explicitly in Risk IT, but the concept behind it exists and/or is in line with the Guide 73 definition.

¹⁸ ‘Equivalent’ means that the definitions are different, but the meaning is equivalent.

Figure 55—ISO Guide 73 and Risk IT Definition Comparisons (cont.)

Guide 73 Concept	Definition in Guide 73	Disposition in Risk IT	Definition in Risk IT	Comment
Internal context	Internal environment in which the organization seeks to achieve its objectives	Identical		The term is used as part of the risk factors.
Level of risk	Magnitude of a risk measured in terms of the combination of consequences and their likelihood	Implicit	N/A	The magnitude of risk is discussed in <i>The Risk IT Practitioner Guide</i> and in <i>The Risk IT Framework</i> , where risk appetite, risk response, etc., are discussed.
Likelihood	Chance of something happening	Absent	N/A	Risk IT uses the term 'frequency', which allows for a more accurate assessment of events occurring more than once in a given period.
Probability	Measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty	Equivalent		Instead, the term 'frequency' is used.
Residual risk	Risk remaining after risk treatment	Equivalent	The remaining risk after management has implemented risk response	The framework does not make use of inherent or absolute risk; rather, it works with residual risks, calling them 'risks'.
Risk	Effect of uncertainty on objectives	Equivalent	A probable situation with uncertain frequency and magnitude of loss (or gain)	Definitions are different but equivalent—both contain the concept 'uncertainty' and 'effect on business objectives'.
Risk aggregation	Process to combine individual risks to obtain a more complete understanding of risk	Equivalent	The process of integrating risk assessments at a corporate level to obtain a complete view on the overall risk for the enterprise	
Risk analysis	Process to comprehend the nature of risk and to determine the level of risk	Equivalent	A process by which frequency and magnitude of IT risk scenarios are estimated	
Risk appetite	The broad-based amount of risk a company or other entity is willing to accept in pursuit of its mission (or vision)	Equivalent	The amount of risk, on a broad level, that an entity is willing to accept in pursuit of its mission	
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation	Equivalent	Risk analysis plus its preliminary and ancillary activities	
Risk avoidance	Decision not to be involved in, or to withdraw from, an activity based on the level of risk	Identical		
Risk communication	Exchange or sharing of information about risk between the decision maker and other stakeholders	Implicit	N/A	Communication on risk is an important part of Risk IT.
Risk control	Measures to modify risk	Implicit	N/A	Risk IT primarily links the IT risks of an enterprise to the COBIT and Val IT controls and management practices.
Risk criteria	Terms of reference against which the significance of a risk is evaluated	Implicit	N/A	Several methods of describing and measuring risk are included in <i>The Risk IT Practitioner Guide</i> .
Risk estimation	Process to assign values to the probability and consequences of a risk	Equivalent	N/A	An equivalent process exists in Risk IT to describe the estimation of frequency and impact as mentioned previously (RE2.2).
Risk identification	Process of finding, recognizing and describing risk	Implicit	N/A	As mentioned in the mapping in appendix 2, Risk IT uses the scenario technique as a practical approach for risk identification.

APPENDIX 5. VOCABULARY COMPARISONS: RISK IT VS. ISO GUIDE 73 AND COSO ERM

Figure 55—ISO Guide 73 and Risk IT Definition Comparisons (cont.)

Guide 73 Concept	Definition in Guide 73	Disposition in Risk IT	Definition in Risk IT	Comment
Risk management	Co-ordinated activities to direct and control an organization with regard to risk	Implicit	N/A	The term 'risk management' is used holistically to cover all concepts and processes affiliated with managing risk. Therefore, there was a reluctance to use this term as specifically as ISO 31000 does.
Risk management process	Systematic application of management policies, procedures and practices to the tasks of communicating, consulting, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk	Implicit	N/A	
Risk matrix	Tool for ranking and displaying risks by defining ranges for consequence and likelihood	Identical		Risk IT uses the term 'risk map'.
Risk owner	Person or entity with the accountability and authority for managing the risk and any associated risk treatments	Implicit	N/A	RACI charts in the Risk IT process model assign risk owners.
Risk profile	Description of a set of risks	Identical		
Risk reduction	Actions taken to lessen the probability, negative consequences, or both, associated with a risk	Identical		Risk IT uses 'risk reduction' in combination with 'risk mitigation'. The terms can be used interchangeably.
Risk register	Record of information about identified risks	Identical		
Risk retention	Acceptance of the burden of loss or benefit of gain from a particular risk	Equivalent	N/A	Risk IT uses the term 'risk acceptance'.
Risk tolerance	Organization's readiness to bear the risk after risk treatments in order to achieve its objectives	Equivalent	The acceptable level of variation that management is willing to allow for any particular risk as it pursues objectives	
Risk transfer	Sharing with another party the burden of loss or benefit of gain, for a risk	Identical		Risk IT uses the term 'risk transfer' in combination with 'risk sharing'. The sharing of risk is a consequence of transferring risk to other parties.
Risk treatment	Process of developing, selecting and implementing controls	Equivalent		Risk IT uses the term 'risk mitigation'.
Uncertainty	State, even partial, of deficiency of information related to a future event, consequence or likelihood	Absent		The term as such is absent. The publication describes the different factors enabling or creating uncertainty.
Vulnerability	Intrinsic properties of something that create susceptibility to a source of risk that can lead to a consequence	Equivalent	A weakness in design, implementation, operation or internal control	

Risk IT and COSO ERM on Risk Management Vocabulary

Both COSO ERM and Risk IT have defined a number of terms. The exact definition or meaning of these terms can differ between the frameworks. For the reader interested in understanding these differences, see **figure 56**. The table includes:

- Column 1—COSO ERM concept
- Column 2—COSO ERM definition
- Column 3—Explanation of whether the Risk IT definition of the same term is identical, is present but implicit, is absent, or is different. (labelled Identical, Implicit¹⁹, Absent or Equivalent)²⁰
- Column 4—The Risk IT definition of the term
- Column 5—A comment, if required

¹⁹ 'Implicit' means that the term does not exist explicitly in Risk IT, but the concept behind it exists and/or is in line with the COSO ERM definition.

²⁰ 'Equivalent' means that the definitions are different, but the meaning is equivalent.

The purpose here is to provide readers knowledgeable about COSO ERM with a comparison that allows them to relate to Risk IT starting from a known basis. In addition, this table will help to prevent purely semantic discussions. Due to the control-focused character of COSO ERM, only the relevant risk-related concepts will be compared. The control-related concepts are linked to the other ISACA frameworks (COBIT and Val IT) and are, therefore, not included in this list.

Figure 56—COSO ERM and Risk IT Definition Comparisons (a)

COSO ERM Concept	Definition in COSO ERM	Disposition in Risk IT	Definition in Risk IT	Comment
Criteria	A set of standards against which enterprise risk management can be measured in determining effectiveness. The eight enterprise risk management components, taken in the context of inherent limitations of enterprise risk management, represent criteria for enterprise risk management effectiveness for each of the four objectives' categories.	Implicit	N/A	A more practical approach for measuring risk management effectiveness can be found in the metrics and maturity model of Risk IT.
Deficiency	A condition within enterprise risk management worthy of attention that may represent a perceived, potential or real shortcoming, or an opportunity to strengthen enterprise risk management to provide a greater likelihood that the entity's objectives will be achieved.	Implicit	Vulnerability event: Any event where a material increase in vulnerability results. Note that this increase in vulnerability can result from changes in control conditions or from changes in threat capability/force. Shortcomings to the Risk IT processes themselves can also be considered deficiencies.	Risk IT uses vulnerability as the outcome of a deficiency.
Design	1. Intent; as used in the definition, enterprise risk management is intended to identify potential events that may affect the entity and manage risk to be within its risk appetite, to provide reasonable assurance as to achievement of objectives. 2. Plan; the way a process is supposed to work, contrasted with how it actually works.	Implicit	N/A	
Effectuated	Used with enterprise risk management: devised and maintained	Absent		
Enterprise risk management process	A synonym for enterprise risk management applied in an entity	Equivalent	Enterprise risk management: The discipline by which an enterprise in any industry assesses, controls, exploits, finances and monitors risks from all sources for the purpose of increasing the enterprise's short- and long-term value to its stakeholders	The term 'enterprise risk management' is used holistically to cover all concepts and processes affiliated with managing risk.
Event	An incident or occurrence, from sources internal or external to an entity, that affects achievement of objectives	Equivalent	Something that happens at a specific place and/or time	
Impact	Result or effect of an event. There may be a range of possible impacts associated with an event. The impact of an event can be positive or negative relative to the entity's related objectives.	Equivalent	Magnitude: A measure of the potential severity of loss or the potential gain from a realised IT-related event/scenario	Risk IT uses both 'magnitude' and 'impact' to express this concept.

APPENDIX 5. VOCABULARY COMPARISONS: RISK IT VS. ISO GUIDE 73 AND COSO ERM

Figure 56—COSO ERM and Risk IT Definition Comparisons (cont.)

COSO ERM Concept	Definition in COSO ERM	Disposition in Risk IT	Definition in Risk IT	Comment
Inherent limitations	Those limitations of enterprise risk management. The limitations relate to the limits of human judgment; resource constraints; the need to consider the cost of controls in relation to expected benefits; the reality that breakdowns can occur; and the possibility of management override and collusion.	Implicit	N/A	
Inherent risk	The risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact	Equivalent	The risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls)	
Likelihood	The possibility that a given event will occur. Terms sometimes take on more specific connotations, with "likelihood" indicating the possibility that a given event will occur in qualitative terms such as high, medium and low, or other judgmental scales, and "probability" indicating a quantitative measure such as a percentage, frequency of occurrence or other numerical metric.	Absent	N/A	Risk IT uses the term 'frequency', which allows for more accurate assessment of events occurring more than once in a given period.
Management intervention	Management's actions to overrule prescribed policies or procedures for legitimate purposes; management intervention is usually necessary to deal with non-recurring and non-standard transactions or events that otherwise might be handled inappropriately by the system (contrast this term with "management override")	Absent	N/A	
Management override	Management's overruling of prescribed policies or procedures for illegitimate purposes with the intent of personal gain or an improperly enhanced presentation of an entity's financial condition or compliance status (contrast this term with "management intervention")	Absent	N/A	
Management process	The series of actions taken by management to run an entity. Enterprise risk management is a part of, and integrated with, the management process.	Implicit	N/A	Risk IT defines a process outlining the approach to integrate with the ERM management process.
Opportunity	The possibility that an event will occur and positively affect the achievement of objectives	Identical	N/A	The upside of risk is also acknowledged in Risk IT.
Policy	Management's dictate of what should be done to effect control. A policy serves as the basis for procedures for its implementation.	Implicit	N/A	The process model often mentions a general policy and how to align the tolerance with this existing policy. In addition, the maturity model includes a policies, standards and procedures dimension.

Figure 56—COSO ERM and Risk IT Definition Comparisons (cont.)

COSO ERM Concept	Definition in COSO ERM	Disposition in Risk IT	Definition in Risk IT	Comment
Procedure	An action that implements a policy	Implicit	N/A	In RG2.4 <i>Provide adequate resources for IT risk management</i> , procedures are defined as an important source for integrating the IT risk management process in ERM. In addition, the maturity model includes a policies, standards and procedures dimension.
Reporting	Used with “objectives”; having to do with the reliability of the entity’s reporting, including both internal and external reporting of financial and non-financial information	Implicit	N/A	Risk IT focuses extensively on monitoring and reporting with regard to risk, as described in chapter 3 of <i>The Risk IT Practitioner Guide</i> .
Residual risk	The remaining risk after management has taken action to alter the risk’s likelihood or impact	Equivalent	The remaining risk after management has implemented risk response	
Risk	The possibility that an event will occur and adversely affect the achievement of objectives	Equivalent	(Business) Risk: A probable situation with uncertain frequency and magnitude of loss (or gain)	Definitions are different but equivalent—both contain the concept of ‘uncertainty’ and ‘effect on business objectives’.
Risk appetite	The broad-based amount of risk a company or other entity is willing to accept in pursuit of its mission (or vision)	Equivalent	The amount of risk, on a broad level, that an entity is willing to accept in pursuit of its mission	
Risk tolerance	The acceptable variation relative to the achievement of an objective	Equivalent	The acceptable level of variation that management is willing to allow for any particular risk as it pursues objectives	
Stakeholders	Parties that are affected by the entity, such as shareholders, the communities in which the entity operates, employees, customers and suppliers	Implicit	N/A	Chapter 2 of <i>The Risk IT Framework</i> describes the stakeholders of IT risk management and chapter 3 of <i>The Risk IT Practitioner Guide</i> provides the information flows amongst the different stakeholders.
Uncertainty	Inability to know in advance the exact likelihood or impact of future events	Absent		The term as such is absent. The publication describes the different factors enabling or creating uncertainty.

APPENDIX 6. RISK IT GLOSSARY

Term	Explanation
Asset	Something of either tangible or intangible value worth protecting, including people, information, infrastructure, finances and reputation
Business goal	The translation of the enterprise's mission from a statement of intention into performance targets and results
Business impact	The net effect, positive or negative, on the achievement of business objectives
Business objective	A further development of the business goals into tactical targets and desired results and outcomes
Business risk	A probable situation with uncertain frequency and magnitude of loss (or gain)
Enterprise risk management	The discipline by which an enterprise in any industry assesses, controls, exploits, finances and monitors risks from all sources for the purpose of increasing the enterprise's short- and long-term value to its stakeholders
Event	Something that happens at a specific place and/or time
Event type	For the purpose of IT risk management ²¹ , one of three possible sorts of events: <ul style="list-style-type: none"> • Threat event • Loss event • Vulnerability event
Frequency	A measure of the rate by which events occur over a certain period of time
Inherent risk	The risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls)
IT risk	The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise
IT risk issue	1: An instance of an IT risk 2: A combination of control, value and threat conditions that impose a noteworthy level of IT risk
IT risk profile	A description of the overall (identified) IT risk to which the enterprise is exposed
IT risk register	A repository of the key attributes of potential and known IT risk issues. Attributes may include name, description, owner, expected/actual frequency, potential/actual magnitude, potential/actual business impact, disposition.
IT risk scenario	The description of an IT-related event that can lead to a business impact
IT-related incident	An IT-related event that causes an operational, developmental and/or strategic business impact
Loss event	Any event where a threat event results in loss ²²
Magnitude	A measure of the potential severity of loss or the potential gain from a realised IT-related event/scenario
Residual risk	The remaining risk after management has implemented risk response
Risk aggregation	The process of integrating risk assessments at a corporate level to obtain a complete view on the overall risk for the enterprise
Risk analysis	A process by which frequency and magnitude of IT risk scenarios are estimated
Risk appetite	The amount of risk, on a broad level, that an entity is willing to accept in pursuit of its mission
Risk culture	The set of shared values and beliefs that governs attitudes towards risk-taking, care and integrity, and determines how openly risks and losses are reported and discussed
Risk factor	Condition that can influence the frequency and/or magnitude and, ultimately, the business impact of IT-related events/scenarios
Risk indicator	A metric capable of showing that the enterprise is subject to, or has a high probability of being subject to, a risk that exceeds the defined risk tolerance
Risk management	Has been used in this publication as an overall generic term that covers both governance and management
Risk map	A (graphic) tool for ranking and displaying risks by defined ranges for frequency and magnitude
Risk portfolio view	1: A method to identify interdependencies and interconnections amongst risks, as well as the effect of risk responses on multiple risks 2: A method to estimate the aggregate impact of multiple risks (e.g., cascading and coincidental threat types/scenarios, risk concentration/correlation across silos) and the potential effect of risk response across multiple risks
Risk statement	A description of the current conditions that may lead to the loss, and a description of the loss. Source: Software Engineering Institute (SEI). For a risk to be understandable, it must be expressed clearly. Such a statement must include a description of the current conditions that may lead to the loss and a description of the loss.
Risk tolerance	The acceptable level of variation that management is willing to allow for any particular risk as it pursues objectives
Threat	Anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm
Threat event	Any event where a threat element/actor acts against an asset in a manner that has the potential to directly result in harm ²²
Vulnerability	A weakness in design, implementation, operation or internal control
Vulnerability event	Any event where a material increase in vulnerability results. Note that this increase in vulnerability can result from changes in control conditions or from changes in threat capability/force. ²²

²¹ Being able to consistently and effectively differentiate the different types of events that contribute to risk is a critical element in developing good risk-related metrics and well-informed decisions. Unless these categorical differences are recognised and applied, any resulting metrics lose meaning and, as a result, decisions based on those metrics are far more likely to be flawed.

²² Jones, J.; 'FAIR Taxonomy', Risk Management Insight, USA, 2008

Page intentionally left blank

LIST OF FIGURES

Listed in parentheses is the number of the same figure in *The Risk IT Framework*.

Figure 1—Risk IT Process Model Overview (17)	Foldout (after page 7)
Figure 2—Positioning COBIT, Val IT and Risk IT (1)	8
Figure 3— <i>The Risk IT Practitioner Guide</i> Overview (18)	8
Figure 4—Mapping Risk IT Processes With Risk IT Practitioner Guide Chapters	9
Figure 5—IT Risk in the Risk Hierarchy (3)	11
Figure 6—IT Risk Categories (2)	12
Figure 7—Enterprise IT Risk Assessment Form	13
Figure 8—Result of Enterprise IT Risk Assessment	14
Figure 9—IT Risk Management Scoping Based on Risk Assessment Results	14
Figure 10—Sample Risk Scenarios and Risk Appetite	16
Figure 11—Risk Map Indicating Risk Appetite Bands	17
Figure 12—Example Risk Map With Risk Appetite	17
Figure 13—IT Risk Communication Components (9)	20
Figure 14—Risk Communication Flows (10)	21
Figure 15—Example Key Risk Indicators	23
Figure 16—Risk Profile Components	24
Figure 17—Aggregation of Risk Maps: Disjointed Risks	27
Figure 18—Aggregation of Risk Maps: Shared Risks	27
Figure 19—Elements of Risk Culture (11)	29
Figure 20—Guidance to Improve Risk Culture Problems	30
Figure 21—Risk Analysis and Risk Response Overview	32
Figure 22—Inherent Risk, Current Risk and Residual Risk	32
Figure 23—Expressing IT Risk in Business Terms (12)	35
Figure 24—COBIT (BSC) Risk Description in Business Terms	35
Figure 25—Example Frequency Scales	38
Figure 26—Example Impact Scales	39
Figure 27—Example Impact Scales With Scoring	40
Figure 28—Changing Impact Scales to Indicate Importance of an Impact Criterion	41
Figure 29—Business Goals and Business Consequences	42
Figure 30—Relation COBIT Business Goals (Westerman/Hunter)	43
Figure 31—Mapping Between Business Goals/Consequences and COBIT Information Criteria	44
Figure 32—Mapping Between Business Goals/Consequences and Extended BSC Criteria	45
Figure 33—Example Risk Map	46
Figure 34—Example Risk Map With Risk Appetite	46
Figure 35—Example Risk Map With Indication of Special Attention Zone	47
Figure 36—Template Risk Register Entry	48
Figure 37—IT Risk Scenario Development (13)	52
Figure 38—Risk Factors in Detail	53
Figure 39—IT Risk Scenario Components (14)	55
Figure 40—Generic IT Risk Scenarios	59
Figure 41—Generic IT Risk Scenarios Mapped to COBIT and Val IT Processes	69
Figure 42—Generic IT Risk Scenarios and Environmental Risk Factors	73
Figure 43—Risk Response Options	76
Figure 44—Risk Response Options and Influencers	78
Figure 45—Risk Response Prioritisation Options	78
Figure 46—Complete Risk Response and Prioritisation Flow (15)	79
Figure 47—Risk Analysis Flowchart	82
Figure 48—COBIT Controls and Val IT Key Management Practices to Mitigate IT Risk	84
Figure 49—Risk Management Frameworks and Standards Compared (42)	111
Figure 50—Risk IT Coverage of ISO 31000 Risk Management Principles	113
Figure 51—Risk IT Coverage of ISO 31000 Framework Components	114
Figure 52—Risk IT Coverage of ISO 31000 Risk Management Processes	115
Figure 53—Risk IT Coverage of ISO 27005 Process Steps	117
Figure 54—Risk IT Coverage of COSO ERM Components	119
Figure 55—ISO Guide 73 and Risk IT Definition Comparisons	123
Figure 56—COSO ERM and Risk IT Definition Comparisons	126

Page intentionally left blank

OTHER ISACA PUBLICATIONS

Many ISACA publications contain detailed assessment questionnaires and work programmes, www.isaca.org/downloads. For more information, visit www.isaca.org/bookstore or e-mail research@isaca.org.

Frameworks and Models

- COBIT® 4.1, 2007, www.isaca.org/cobit—The COBIT framework, in versions 4.0 and higher, includes the:
 - Framework—Explains COBIT organisation of IT governance management and control objectives and good practices by IT domains and processes, and links them to business requirements
 - Process descriptions—Include 34 IT processes covering the IT responsibility areas from beginning to end
 - Control objectives—Provide generic best practice management objectives for IT processes
 - Management guidelines—Offer tools to help assign responsibility and measure performance
 - Maturity models—Provide profiles of IT processes describing possible current and future states
- *Enterprise Value: Governance of IT Investments: The Val IT™ Framework 2.0*, 2008, www.isaca.org/valit—Explains how to extract optimal value from IT-enabled investments; is based on the COBIT framework and organised into:
 - Three processes—Value Governance, Portfolio Management and Investment Management
 - IT key management practices—Essential management practices that positively influence the achievement of the desired result or purpose of a particular activity. They support the Val IT processes and play roughly the same role as do COBIT's control objectives.
- *An Introduction to the Business Model for Information Security (BMIS)*, 2009, www.isaca.org/bmis—Provides a view of information security programme activities within the context of the larger enterprise, to integrate the disparate security programme components into a holistic system of information protection. The *Business Model for Information Security* is scheduled to be issued early in 2010.
- *ITAF™: A Professional Practices Framework for IT Assurance*, 2008, www.isaca.org/itaf—Compliance and good practice setting guidance consisting of:
 - Guidance on the design, conduct and reporting of IT audit and assurance assignments
 - Definition of terms and concepts specific to IT assurance
 - Establishing standards that address IT audit and assurance professional roles and responsibilities, knowledge, skills and diligence, conduct and reporting requirements
- *The Risk IT Framework*, 2009, www.isaca.org/riskit—Fills the gap between generic risk management frameworks and detailed (primarily security-related) IT risk management frameworks:
 - Three domains—Risk Governance, Risk Evaluation and Risk Response
 - Provides an end-to-end, comprehensive view of all risks related to the use of IT and a similarly thorough treatment of risk management, from the tone and culture at the top, to operational issues
 - Enables enterprises to understand and manage all significant IT risk types, building upon the existing risk-related components within the current ISACA COBIT and Val IT frameworks

COBIT-related Publications

- *Aligning COBIT® 4.1, ITIL V3® and ISO/IEC 27002 for Business Benefit*, 2008
- *Building the Business Case for COBIT® and Val IT™: Executive Briefing*, 2009
- *COBIT® and Application Controls*, 2009—Provides guidance primarily for business executives, business management and IT management, as well as for IT developers and implementers, internal and external auditors and other professionals on application controls (expanding on the six application controls discussed in COBIT) and the relationships and dependencies that application controls have with other controls (such as IT general controls).
- *COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*, 2007—Provides guidance on the practices to be considered when improving processes and implementing solutions for control objectives. It also provides risk and value statements to help understand and justify the need to implement each control objective. Control practices are strongly recommended for use with *Implementing and Continually Improving IT Governance*. The control practices provide the more detailed guidance at the control objective level on why and what to implement as required by assurance professionals, management, service providers, end users and IT professionals.
- COBIT® Mappings:
 - *COBIT® Mapping: Mapping of CMMI® for Development V1.2 With COBIT® 4.0*, 2007
 - *COBIT® Mapping: Mapping of ISO/IEC 17799:2000 With COBIT®, 2nd Edition*, 2006
 - *COBIT® Mapping: Mapping of ISO/IEC 17799:2005 With COBIT® 4.0*, 2006
 - *COBIT® Mapping: Mapping of ITIL With COBIT® 4.0*, 2007
 - *COBIT® Mapping: Mapping of ITIL V3 With COBIT® 4.1*, 2008
 - *COBIT® Mapping: Mapping of NIST SP 800-53 With COBIT® 4.1*, 2007
 - *COBIT® Mapping: Mapping of PMBOK With COBIT® 4.0*, 2006
 - *COBIT® Mapping: Mapping of PRINCE2 With COBIT®, 0*, 2007
 - *COBIT® Mapping: Mapping of SEI's CMM for Software With COBIT® 4.0*, 2006
 - *COBIT® Mapping: Mapping of TOGAF 8.1 With COBIT® 4.0*, 2007
 - *COBIT® Mapping: Overview of International IT Guidance, 2nd Edition*, 2006

COBIT-related Publications (cont.)

- COBIT Online®—Although not a publication, this product is also available through the ISACA bookstore. It allows users to customise a version of COBIT for their own enterprise, then store and manipulate that version as desired. It offers online, real-time surveys, frequently asked questions, benchmarking and a discussion facility for sharing experiences and questions.
- *COBIT® Quickstart™, 2nd Edition*, 2007—Provides a baseline of control for the smaller enterprise and a possible first step for the larger enterprise
- *COBIT® Security Baseline™, 2nd Edition*, 2007—Focuses on essential steps for implementing information security within the enterprise. It also provides easy-to-understand guidance for addressing security aspects of IT governance.
- *COBIT® User Guide for Service Managers*, 2009—Focuses on service managers, providing them a better understanding of the need for IT governance and how to apply good practices in their specific roles and responsibilities. It facilitates easier use and adoption of COBIT and ITIL concepts and approaches, and encourages integration of COBIT with ITIL. It provides easy-to-understand guidance for addressing service manager aspects of IT governance.
- *Implementing and Continually Improving IT Governance*, 2009
- *IT Assurance Guide: Using COBIT®*, 2007—Provides guidance on how to use COBIT to support a variety of assurance tasks, supported by suggested testing steps aligned with the control practices. The guide can support audit teams that need to provide independent assurance that IT governance practices have been implemented effectively.
- *IT Control Objectives for Basel II*, 2007—Provides easy-to-understand guidance for addressing Basel II aspects of IT governance
- *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition*, 2006—Provides guidance on how to assure compliance for the IT environment based on the COBIT control objectives. It also provides easy-to-understand guidance for addressing Sarbanes-Oxley aspects of IT governance.
- *ITGI Enables ISO/IEC 38500:2008 Adoption*, 2009

Risk IT-related Publication

- *The Risk IT Practitioner Guide*, 2009—Contains practical and more detailed guidance on how to accomplish some of the activities described in the process model

Val IT-related Publications

- *Enterprise Value: Getting Started With Value Management*, 2008—Provides an easy-to-follow guide on getting a value management initiative started for business and IT executives and organisational leaders
- *Enterprise Value: Governance of IT Investments: The Business Case*, 2005—Focuses on one key element of the investment management process
- *Val IT™ Mapping: Mapping of Val IT™ to MSP™, PRINCE2™ and ITIL V3®*, 2009—Focuses on *Managing Successful Programmes (MSP)*, *Projects in Controlled Environments (PRINCE2)* and *IT Infrastructure Library (ITIL) V3*, but there are other relevant frameworks, such as *Gateway Reviews*, the newly released *Portfolio, Programme and Project Office Guidance (P3O)* and *The Standard for Portfolio Management*. These and others may be referenced in future publications.

Additional Executive and Management Guidance

- *An Executive View of IT Governance*, 2008
- *Board Briefing on IT Governance, 2nd Edition*, 2003—Helps executives better understand IT governance concepts, what the issues are and how best to make it happen
- *Building the Business Case for COBIT® and Val IT™: Executive Briefing*—Explores and demonstrates the business value of COBIT and Val IT
- *Defining Information Security Management Position Requirements: Guidance for Executives and Managers*, 2008
- *Identifying and Aligning Business Goals and IT Goals: Full Research Report*, 2008
- *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*, 2006—Presents information security in business terms and contains tools and techniques to help uncover security-related problems.
- *Information Security Governance: Guidance for Information Security Managers*, 2008
- *Information Security Governance—Top Actions for Security Managers*, 2005
- *IT Governance and Process Maturity*, 2008
- IT Governance Domain Practices and Competencies:
 - *Governance of Outsourcing*, 2005
 - *Information Risks: Whose Business Are They?*, 2005
 - *IT Alignment: Who Is in Charge?*, 2005
 - *Measuring and Demonstrating the Value of IT*, 2005
 - *Optimising Value Creation From IT Investments*, 2005
- IT Governance Roundtables:
 - *Defining IT Governance*, 2008
 - *IT Staffing Challenges*, 2008
 - *Unlocking Value*, 2009
 - *Value Delivery*, 2008
- *Managing Information Integrity: Security, Control and Audit Issues*, 2004
- *Understanding How Business Goals Drive IT Goals*, 2008
- *Unlocking Value: An Executive Primer on the Critical Role of IT Governance*, 2008—Provides executives with an insight into why IT governance is important and how it can add value to the enterprise

Additional Practitioner Guidance

- Audit/Assurance Programs:
 - *Change Management Audit/Assurance Program*, 2009
 - *Generic Application Audit/Assurance Program*, 2009
 - *Identity Management Audit/Assurance Program*, 2009
 - *IT Continuity Planning Audit/Assurance Program*, 2009
 - *Network Perimeter Security Audit/Assurance Program*, 2009
 - *Outsourced IT Environments Audit/Assurance Program*, 2009
 - *Security Incident Management Audit/Assurance Program*, 2009
 - *Systems Development and Project Management Audit/Assurance Program*, 2009
 - *UNIX/LINUX Operating System Security Audit/Assurance Program*, 2009
 - *z/OS Security Audit/Assurance Program*, 2009
- *Cybercrime: Incident Response and Digital Forensics*, 2005
- *Enterprise Identity Management: Managing Secure and Controllable Access in the Extended Enterprise Environment*, 2004
- *Information Security Career Progression Survey Results*, 2008
- *Information Security Harmonisation—Classification of Global Guidance*, 2005
- *OS/390—z/OS: Security, Control and Audit Features*, 2003
- *Peer-to-peer Networking Security and Control*, 2003
- *Risks of Customer Relationship Management: A Security, Control and Audit Approach*, 2003
- *Security Awareness: Best Practices to Serve Your Enterprise*, 2005
- *Security Critical Issues*, 2005
- *Security Provisioning: Managing Access in Extended Enterprises*, 2002
- *Stepping Through the IS Audit*, 2nd Edition, 2004
- *Stepping Through the InfoSec Program*, 2007
- Technical and Risk Management Reference Series:
 - *Security, Audit and Control Features Oracle® Database*, 3rd Edition, 2009
 - *Security, Audit and Control Features Oracle® E-Business Suite*, 2nd Edition, 2006
 - *Security, Audit and Control Features PeopleSoft®*, 2nd Edition, 2006
 - *Security, Audit and Control Features SAP® ERP*, 3rd Edition, 2009
- *Top Business/Technology Survey Results*, 2008

Page intentionally left blank