The Risk IT Framework

Principles

Process Details

Management Guidelines

Maturity Models

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 Framework* (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

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 978-1-60420-111-6
The Risk IT Framework
Printed in the United States of America

ACKNOWLEDGEMENTS

ISACA wishes to recognise:

Development Team
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
Dirk Steuperaert, CISA, CGEIT, IT In Balance BVBA, Belgium

IT Risk Task Force (2008-2009)
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland, Chair
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 and 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, India
Philip De Picker, CISA, MCA, Nationale Bank van Belgie, 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
Monica Jain, CGEIT, CSQA, CSSBB, USA
Jack Jones, CISA, CISM, CISSP, Risk Management Insight LLC, USA
Dharmesh Joshi, CISA, CGEIT, CA, CIA, CISSP, CIBC, 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 Corp., 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
Bjarne Lonberg, CISSP, A.P. Moller—Maersk, Denmark
Jo Lusk, CISA, Federal Government, USA
Charles Mansour, CISA, Charles Mansour Audit and Risk Service, UK
Mario Micallef, CGEIT, CPAA, FIA, Ganado & Associates, Malta
Jack Musgrove, CGEIT, CMC, BI International, USA
Paul Phillips, Barclays Bank Plc, UK
Andre Pitkowski, CGEIT, OCTAVE, APIT Informatica, Brazil
Jack M. Pullara, CISA, PricewaterhouseCoopers LLP, USA

ACKNOWLEDGEMENTS *(cont.)*

Expert Reviewers *(cont.)*
Felix Ramirez, CISA, CGEIT, Riebeeck Associates, USA
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
Gustavo Adolfo Solis Montes, Grupo Cynthus SA de CV, Mexico
John Spangenberg, SeaQuation, The Netherlands
Robert E. Stroud, CGEIT, CA Inc., 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 & Associes 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 Eurl, 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

1. Executive Summary 7

2. Risk IT Framework—Purpose and Target Audience 11
IT Risk 11
Purpose of the Risk IT Framework 11
Intended Audiences and Stakeholders 12
Benefits and Outcomes 12

3. Risk IT Principles 13

4. The Risk IT Framework 15

5. Essentials of Risk Governance 17
Risk Appetite and Tolerance 17
Responsibilities and Accountability for IT Risk Management 18
Awareness and Communication 18
Risk Culture 22

6. Essentials of Risk Evaluation 23
Describing Business Impact 23
IT Risk Scenarios 24

7. Essentials of Risk Response 27
Key Risk Indicators 27
Risk Response Selection and Prioritisation 29

8. Risk and Opportunity Management Using COBIT, Val IT and Risk IT 31

9. The Risk IT Framework Process Model Overview 33

10. Managing Risk in Practice—The Practitioner Guide Overview 35

11. Overview of the Risk IT Framework Process Model 37
Detailed Process Descriptions 37

12. The Risk IT Framework 43
RG1 Establish and maintain a common risk view. 45
RG2 Integrate with ERM. 51
RG3 Make risk-aware business decisions. 57
RE1 Collect data. 65
RE2 Analyse risk. 69
RE3 Maintain risk profile. 73
RR1 Articulate risk. 81
RR2 Manage risk. 85
RR3 React to events. 90

Appendix 1. Overview of Reference Materials 97

Appendix 2. High-level Comparison of Risk IT With Other Risk Management Frameworks and Standards 99

Appendix 3. Risk IT Glossary 101

List of Figures 103

Other ISACA Publications 104

Page intentionally left blank

1. EXECUTIVE SUMMARY

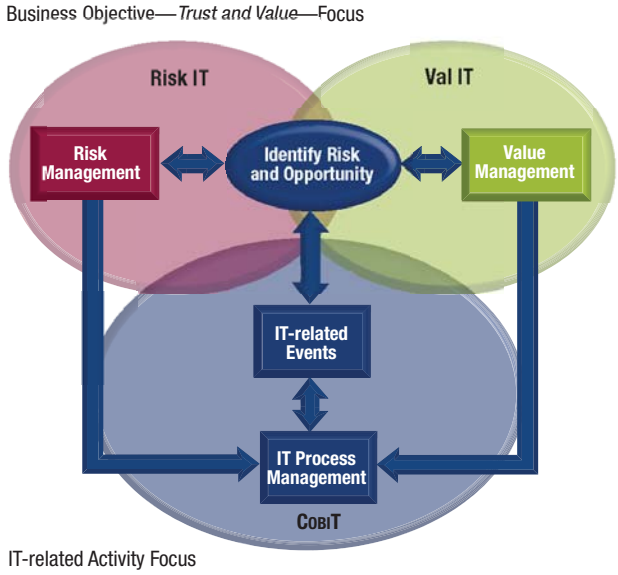
This document forms part of ISACA's Risk IT initiative, which is dedicated to helping enterprises manage IT-related risk. The collective experience of a global team of practitioners and experts, and existing and emerging practices and methodologies for effective IT risk management, have been consulted in the development of the Risk IT framework. Risk IT is a framework based on a set of guiding principles and featuring business processes and management guidelines that conform to these principles.

The Risk IT framework complements ISACA's COBIT[1], which provides a comprehensive framework for the control and governance of business-driven information-technology-based (IT-based) solutions and services. While COBIT sets good practices for the *means* of risk management by providing a set of controls to mitigate IT risk, Risk IT sets good practices for the *ends* by providing a framework for enterprises to identify, govern and manage IT risk.

The Risk IT framework is to be used to help implement IT governance, and enterprises that have adopted (or are planning to adopt) COBIT as their IT governance framework can use Risk IT to enhance risk management.

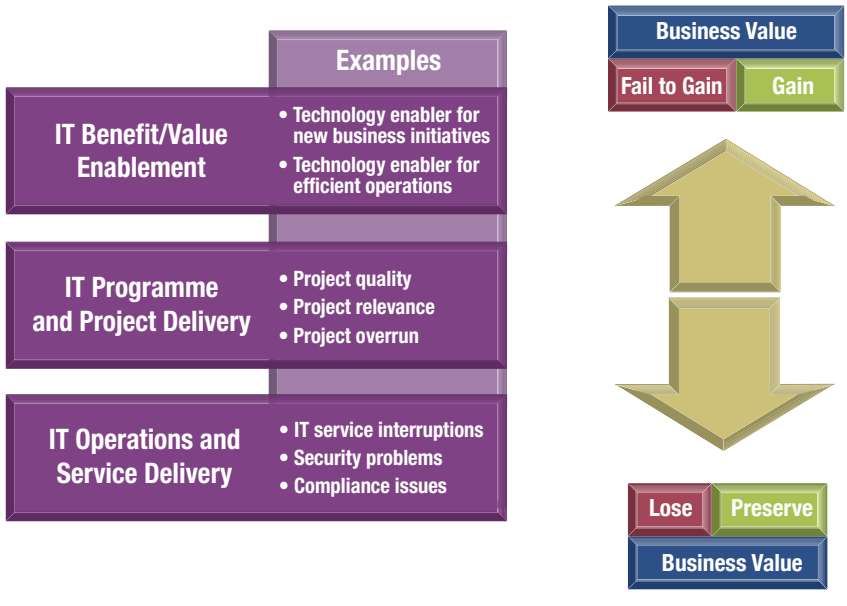
The COBIT processes manage all IT-related activities within the enterprise. These processes have to deal with events internal or external to the enterprise. Internal events can include operational IT incidents, project failures, full (IT) strategy switches and mergers. External events can include changes 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 the 'Risk Management' and 'Value Management' boxes are directed back to the 'IT Process Management' area in **figure 1**.

Figure 1—Positioning COBIT, Val IT and Risk IT



IT risk is business risk—specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. It consists of IT-related events that could potentially impact the business. It can occur with both uncertain frequency and magnitude, and it creates challenges in meeting strategic goals and objectives. IT risk can be categorised in different ways (see **figure 2**).

Figure 2—IT Risk Categories



[1] ISACA, COBIT 4.1, 2008, *www.isaca.org*

- IT benefit/value enablement risk—Associated with (missed) opportunities to use technology to improve efficiency or effectiveness of business processes, or as an enabler for new business initiatives
- IT programme and project delivery risk—Associated with the contribution of IT to new or improved business solutions, usually in the form of projects and programmes. This ties to investment portfolio management (as described in the Val IT framework).
- IT operations and service delivery risk—Associated with all aspects of the performance of IT systems and services, which can bring destruction or reduction of value to the enterprise

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

Figure 2 shows that for all categories of IT risk there is an equivalent upside. For example:
- Service delivery—If service delivery practices are strengthened, the enterprise can benefit, e.g., by being ready to absorb additional transaction volumes or market share.
- Project delivery—Successful project delivery brings new business functionality.

It is important to keep this risk/benefit duality in mind during all risk-related decisions. For example, decisions should consider the exposure that may result if a risk is not treated vs. the benefit if it is addressed, or the potential benefit that may accrue if opportunities are taken vs. missed benefits if opportunities are foregone.

The Risk IT framework is aimed at a wide audience, as risk management is an all-encompassing and strategic requirement in any enterprise. The target audience includes:
- Top executives and board members who need to set direction and monitor risk at the enterprise level
- Managers of IT and business departments who need to define risk management processes
- Risk management professionals who need specific IT risk guidance
- External stakeholders

Additional guidance is available in *The Risk IT Practitioner Guide* (summarised in this publication, with a more complete volume issued separately), including more practical examples and suggested methodologies, as well as detailed linking amongst Risk IT, COBIT and Val IT.

The Risk IT framework is based on the principles of enterprise risk management (ERM) standards/frameworks such as COSO ERM[2] and AS/NZS 4360[3] (soon to be complemented or replaced by ISO 31000) and provides insight on how to apply this guidance to IT. Risk IT applies the proven and generally accepted concepts from these major standards/frameworks, as well as the main concepts from other IT risk management related standards. However, the terminology used in Risk IT may sometimes differ from the one used in other standards, so for those professionals who are more familiar with other risk management standards or frameworks we have provided extensive comparisons between Risk IT and a number of existing major risk management standards in *The Risk IT Practitioner Guide*. Risk IT differs from existing IT risk guidance documents that focus solely on IT security in that Risk IT covers all aspects of IT risk.

Although Risk IT aligns with major ERM frameworks, the presence and implementation of these frameworks is not a prerequisite for adopting Risk IT. By adopting Risk IT enterprises will automatically apply all ERM principles. In cases where ERM is present in some form, it is important to build on the strengths of the existing ERM programme—this will increase business buy-in and adoption of IT risk management, save time and money, and avoid misunderstandings about specific IT risks that may be part of a bigger business risk.

Risk IT defines, and is founded on, a number of guiding principles for effective management of IT risk. The principles are based on commonly accepted ERM principles, which have been applied to the domain of IT. The Risk IT process model is designed and structured to enable enterprises to apply the principles in practice and to benchmark their performance.

The Risk IT framework is about IT risk—in other words, business risk related to the use of IT. The connection to business is founded in the principles on which the framework is built, i.e., effective enterprise governance and management of IT risk, as shown in **figure 5**:
- Always connect to business objectives
- Align the management of IT-related business risk with overall ERM
- Balance the costs and benefits of managing IT 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 activities

[2] Committee of Sponsoring Organizations (COSO) of the Treadway Commission, *Enterprise Risk Management—Integrated Framework*, USA, 2004, *www.coso.org*
[3] Standards Australia, AS/NZS 4360:2004, *Australian/New Zealand Standard for Risk Management*, Australia, 2004, *www.saiglobal.com*
[4] ISACA, *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0*, USA, 2008, *www.isaca.org*

Around these building blocks a comprehensive process model is built for IT risk management that will look familiar to users of COBIT and Val IT[4]. Substantial guidance is provided on the key activities within each process, responsibilities for the process, and information flows between processes and performance management of the process. The process model is divided into three domains—Risk Governance, Risk Evaluation and Risk Response—each containing three processes:

- Risk Governance (RG)
  - RG1 Establish and maintain a common risk view
  - RG2 Integrate with ERM
  - RG3 Make risk-aware business decisions
- Risk Evaluation (RE)
  - RE1 Collect data
  - RE2 Analyse risk
  - RE3 Maintain risk profile
- Risk Response (RR)
  - RR1 Articulate risk
  - RR2 Manage risk
  - RR3 React to events

Applying good IT risk management practices as described in Risk IT will provide tangible business benefits, e.g., fewer operational surprises and failures, increased information quality, greater stakeholder confidence, reduced regulatory concerns, and innovative applications supporting new business initiatives.

The Risk IT framework is part of the ISACA product portfolio on IT governance. Although this document provides a complete and stand-alone framework, it does include references to COBIT. The practitioner guide issued in support of this framework makes extensive reference to COBIT and Val IT, and it is recommended that managers and practitioners acquaint themselves with the major principles and contents of those two frameworks.

Like COBIT and Val IT, Risk IT is not a standard but a framework, including a process model and good practice guidance. This means that enterprises can and should customise the components provided in the framework to suit their particular organisation and context.

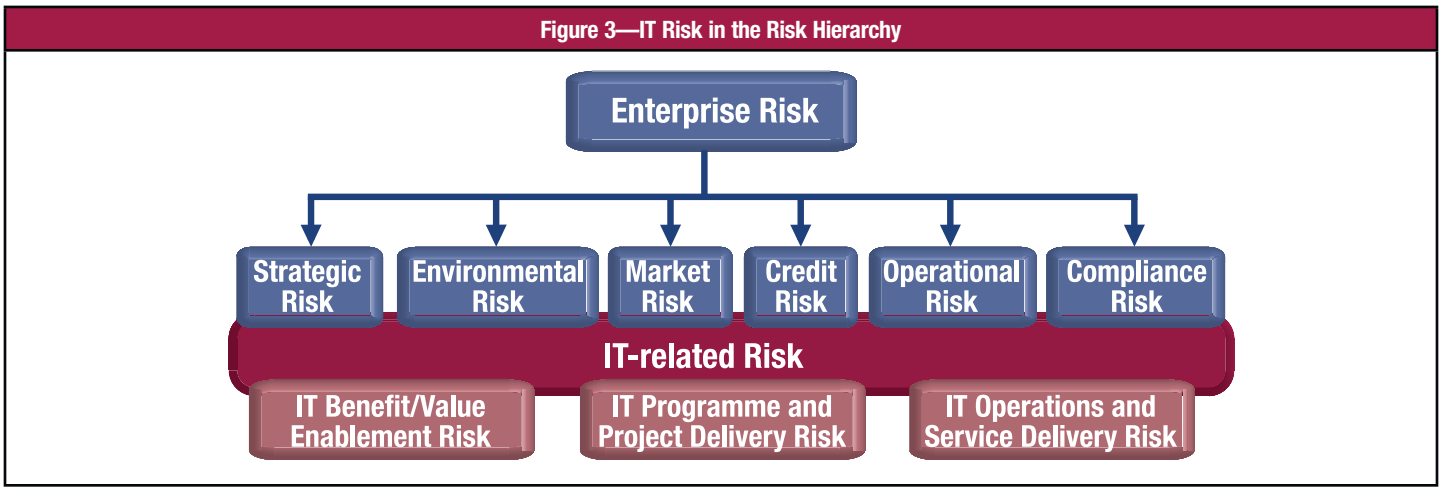
Page intentionally left blank

2. RISK IT FRAMEWORK—PURPOSE AND TARGET AUDIENCE

IT Risk

IT risk is a component of the overall risk universe of the enterprise, as shown in **figure 3**. Other risks 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 3**.

Figure 3—IT Risk in the Risk Hierarchy



IT risk is business risk—specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. It consists of IT-related events and conditions that could potentially impact the business. It can occur with both uncertain frequency and magnitude, and it creates challenges in meeting strategic goals and objectives. IT risk can be categorised in different ways:

- IT benefit/value enablement risk—Associated with (missed) opportunities to use technology to improve efficiency or effectiveness of business processes, or as an enabler for new business initiatives
- IT programme and project delivery risk—Associated with the contribution of IT to new or improved business solutions, usually in the form of projects and programmes. This ties to investment portfolio management (as described in the Val IT framework).
- IT operations and service delivery risk—Associated with all aspects of the performance of IT systems and services, which can bring destruction or reduction of value to the enterprise

Many IT risk issues can occur because of third-party problems (service delivery as well as solution development)—both IT third parties and business partners (e.g., supply chain IT risk caused at a major supplier can have a large business impact). Therefore, good IT risk management requires significant dependencies to be known and well understood.

IT risk always exists, whether or not it is detected or recognised by an enterprise. In this context, it is important to identify and manage potentially significant IT risk issues, as opposed to every risk issue, as the latter may not be cost effective.

Purpose of the Risk IT Framework

Management of business risk is an essential component of the responsible administration of any enterprise. Almost every business decision requires the executive or manager to balance risk and reward.

The all-encompassing use of IT can provide significant benefits to an enterprise, but it also involves risk. Due to IT's importance to the overall business, IT risk should be treated like other key business risks, such as strategic risk, environmental risk, market risk, credit risk, operational risks and compliance risk, all of which fall under the highest 'umbrella' risk category: failure to achieve strategic objectives. While these other risks have long been incorporated into corporate decision-making processes, too many executives tend to relegate IT risk to technical specialists outside the boardroom.

The Risk IT framework explains IT risk and enables users to:

- Integrate the management of IT risk into the overall ERM of the enterprise, thus allowing the enterprise to make risk-return-aware decisions
- Make well-informed decisions about the extent of the risk, and the risk appetite and the risk tolerance of the enterprise
- Understand how to respond to the risk

In brief, this framework allows the enterprise to make appropriate risk-aware decisions.

Practice has shown that the IT function and IT risk are often not well understood by an enterprise's key stakeholders, including board members and executive management. Yet, these are the people who depend on IT to achieve the strategic and operational objectives of the enterprise and, by consequence, should be accountable for risk management. Without a clear understanding of the IT function and IT risk, senior executives have no frame of reference for prioritising and managing IT risk.

IT risk is not purely a technical issue. Although IT subject matter experts are needed to understand and manage aspects of IT risk, business management is the most important stakeholder. Business managers determine what IT needs to do to support their business; they set the targets for IT and consequently are accountable for managing the associated risks. In Risk IT, business management includes enterprise/corporate roles, business-line leaders and support functions (chief financial officer [CFO], chief information officer [CIO], human resources [HR], etc.).

The Risk IT framework fills the gap between generic risk management frameworks such as COSO ERM, AS/NZS 4360, ISO 31000, the UK-based ARMS[5] and domain-specific (such as security-related or project-management-related) frameworks. It 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. In summary, the framework will enable enterprises to understand and manage all significant IT risk types.

The framework provides:
- An end-to-end process framework for successful IT risk management
- Guidance for practitioners, including tools and techniques to understand and manage concrete risks to business operations. This includes a generic list of common, potentially adverse IT-related risk scenarios that could impact the realisation of business objectives.

Intended Audiences and Stakeholders

The intended audience for the Risk IT framework is extensive, as are the reasons for adopting and using the framework, and the benefits each group can find in it (**figure 4**). All of the roles listed in **figure 4** can be considered stakeholders for the management of IT risk.

Figure 4—Audiences and Benefits

Role	Benefits of/Reasons for Adopting and Adapting the Risk IT Framework
Boards and executive management	Better understanding of their responsibilities and roles with regard to IT risk management, the implications of risk in IT to strategy objectives, and how to better use IT to reduce risk in strategic moves
Corporate risk managers (for ERM)	Assistance with managing IT risk, in line with generally accepted ERM principles
Operational risk managers	Linkage of their framework to Risk IT; identification of operational losses or development of key risk indicators (KRIs)
IT management	Better understanding of how to identify and manage IT risk and how to communicate IT risk to business decision makers
IT service managers	Enhancement of their view of operational IT-related risks, which should fit into an overall IT risk management framework
Business continuity managers	Alignment with ERM (since assessment of risk is a key aspect of their responsibility)
IT security managers	Positioning of security risk amongst other categories of IT risk
CFOs	Gaining a better view of IT-related risk and its financial implications for investment and portfolio management purposes
Enterprise governance officers	Assistance with their review and monitoring of governance responsibilities and other IT governance roles
Business managers	Understanding and management of IT risk—one of many business risks, all of which should be aligned
IT auditors	Better analysis of risk in support of audit plans and reports
Regulators	Support of their assessment of regulated enterprises' IT risk management approach
External auditors	Additional guidance on IT-related risk levels when establishing an opinion over the quality of internal control
Insurers	Support in establishing adequate IT insurance coverage and seeking agreement on risk levels
Rating agencies	In collaboration with insurers, a reference to assess and rate objectively how an enterprise is dealing with IT risk

Benefits and Outcomes

The Risk IT framework addresses many issues that enterprises face today, notably their need for:
- An accurate view of significant current and near-future IT-related risks throughout the extended enterprise, and the success with which the enterprise is addressing them
- End-to-end guidance on how to manage IT-related risks, beyond both purely technical control measures and security
- Understanding how to capitalise on an investment made in an IT internal control system already in place to manage IT-related risk
- Understanding how effective IT risk management enables business process efficiency, improves quality, and reduces waste and costs
- When assessing and managing IT risk, integration with the overall risk and compliance structures within the enterprise
- A common framework/language to help communication and understanding amongst business, IT, risk and audit management
- Promotion of risk responsibility and its acceptance throughout the enterprise
- A complete risk profile to better understand the enterprise's full exposure, so as to better utilise company resources

[5] AIRMIC, ALARM, IRM, 'A Risk Management Standard', 2002, *www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf*

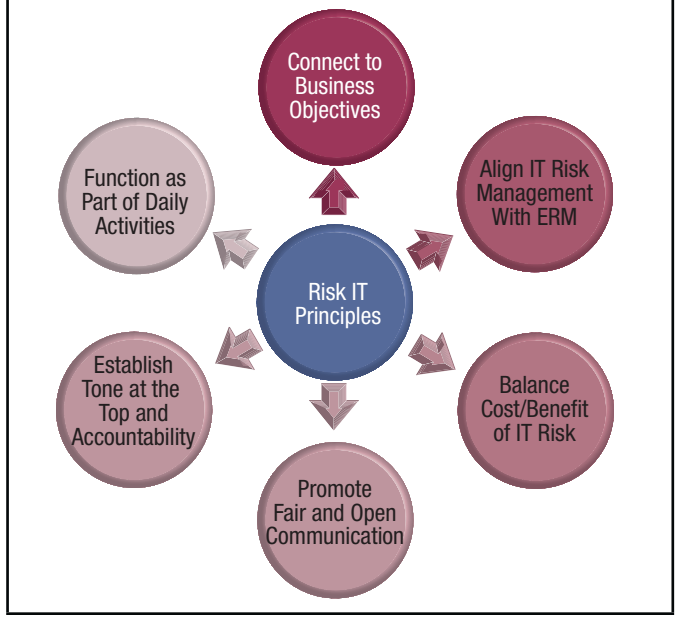
3. RISK IT PRINCIPLES

Risk IT defines, and is founded on, a number of guiding principles for effective management of IT risk. The principles are based on commonly accepted ERM principles, which have been applied to the domain of IT. The Risk IT process model is designed and structured to enable enterprises to apply the principles in practice and to benchmark their performance.

The Risk IT framework is about IT risk—in other words, business risk related to the use of IT. The connection to business is founded in the principles on which the framework is built, i.e., effective enterprise governance and management of IT risk, as shown in **figure 5**:

- Always connect to business objectives
- Align the management of IT-related business risk with overall ERM, if applicable, i.e., if ERM is implemented in the enterprise
- Balance the costs and benefits of managing IT 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 activities

Figure 5—Risk IT Principles



Each of these principles is examined below in more detail.

Effective enterprise governance of IT risk always connects to business objectives:

- IT risk is treated as a business risk, as opposed to a separate type of risk, and the approach is comprehensive and cross-functional.
- The focus is on business outcome. IT supports the achievement of business objectives, and IT risks are expressed as the impact they can have on the achievement of business objectives or strategy.
- Every analysis of IT risk contains a dependency analysis of how the business process depends on IT-related resources, such as people, applications and infrastructure.
- IT risk management is a business enabler, not an inhibitor. IT-related business risk is viewed from both angles: protection against value destruction and enabling of value generation.

Effective enterprise governance of IT risk aligns the management of IT-related business risk with overall ERM:

- Business objectives and the amount of risk that the enterprise is prepared to take are clearly defined.
- Enterprise decision-making processes consider the full range of potential consequences and opportunities from IT risk.
- The entity's risk appetite reflects its risk management philosophy and influences the culture and operating style (as stated in *COSO Enterprise Risk Management—Integrated Framework*).
- Risk issues are integrated for each business organisation, i.e., the risk view is consolidated across the overall enterprise.
- Attestation of/sign-off on control environment is provided.

Effective enterprise governance of IT risk balances the costs and benefits of managing IT risk:

- Risk is prioritised and addressed in line with risk appetite and tolerance.
- Controls are implemented to address a risk and based on a cost-benefit analysis. In other words, controls are not implemented simply for the sake of implementing controls.
- Existing controls are leveraged to address multiple risks or to address risk more efficiently.

Effective management of IT risk promotes fair and open communication of IT risk:

- Open, accurate, timely and transparent information on IT risk is exchanged and serves as the basis for all risk-related decisions.
- Risk issues, principles and risk management methods are integrated across the enterprise.
- Technical findings are translated into relevant and understandable business terms.

Effective management 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:

- Key people, i.e., influencers, business owners and the board of directors, are engaged in IT risk management.
- There is a clear assignment and acceptance of risk ownership, including assuming accountability, doing performance measurement and integrating risk management in the (performance) reward system. Direction is demonstrated from the top by means of policies, procedures and the right level of enforcement.
- A risk-aware culture is actively promoted, starting with the tone from the top. This helps ensure that those involved with operational risk management are operating on consistent risk assumptions.
- Risk decisions are made by authorised individuals, with a focus on business management, e.g., for IT investment decisions, project funding, major IT environment changes, risk assessments, and monitoring and testing controls.

Effective management of IT risk promotes continuous improvement and is part of daily activities:

- Because of the dynamic nature of risk, management of IT risk is an iterative, perpetual, ongoing process. Every change brings risk and/or opportunity, and the enterprise prepares for this by giving advance consideration to changes in the organisation itself (mergers and acquisitions), in regulations, in IT, in the business, etc.
- Attention is paid to consistent risk assessment methods, roles and responsibilities, tools, techniques, and criteria across the enterprise, noting especially:
  - Identification of key processes and associated risks
  - Understanding of impacts on achieving objectives
  - Identification of triggers that indicate when an update of the framework or components in the framework is required
- Risk management practices are appropriately prioritised and embedded in enterprise decision-making processes.
- Risk management practices are straightforward and easy to use, and contain practices to detect threat and potential risk, as well as prevent and mitigate it.

4. The Risk IT Framework

The Risk IT framework is built on the principles laid out in chapter 3 and further developed into a comprehensive process model (**figure 6**).

The risk management process model groups key activities into a number of processes. These processes are grouped into three domains. The process model will appear familiar to users of CobiT and Val IT: substantial guidance is provided on the key activities within each process, responsibilities for the process, information flows between processes and performance management of the process.

The three domains of the Risk IT framework—Risk Governance, Risk Evaluation and Risk Response—each contain three processes, as shown in **figure 6**.

Figure 6—Risk IT Framework

The following chapters contain a number of essential practices and techniques for each of the three domains of the Risk IT framework.

The model is explained in full detail in chapter 11.

Page intentionally left blank

5. ESSENTIALS OF RISK GOVERNANCE

This chapter discusses a few essential components of the Risk Governance domain. They are discussed briefly, and more information and practical guidance can be found in *The Risk IT Practitioner Guide*. The topics discussed here include:
- Risk appetite and risk tolerance
- Responsibilities and accountability for IT risk management
- Awareness and communication
- Risk culture

Risk Appetite and Tolerance

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 definitions (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)

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*.

Risk Appetite

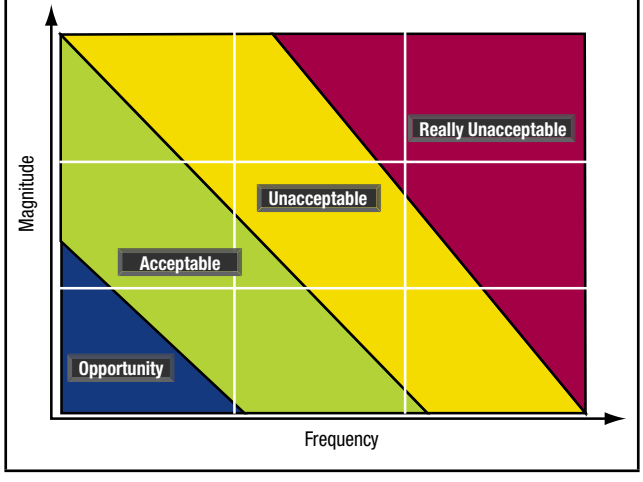
Risk appetite is the amount of risk an entity is prepared to accept when trying to achieve its objectives. When considering the risk appetite levels for the enterprise, two major factors are important:
- The enterprise's objective capacity to absorb loss, e.g., financial loss, reputation damage
- The (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?

Risk appetite can be defined in practice 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.

Risk appetite can be defined using risk maps. Different bands of risk significance can be defined, indicated by coloured bands on the risk map shown in **figure 7**.

In this example, 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 an immediate risk response.
- Yellow—Indicates elevated risk, i.e., also above 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 a 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

Figure 7—Risk Map Indicating Risk Appetite Bands



This risk appetite scheme is an example. Every enterprise has to 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. Risk appetite and risk tolerance should be applied not only to risk assessments but also to all IT risk decision making.

Risk Tolerance

Risk tolerance is the tolerable deviation from the level set by the risk appetite and business objectives, e.g., 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.

On risk appetite and risk tolerance, the following guidance applies:
- 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, or in some entities 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 of risk. Enterprises at which 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 tolerance is defined at the enterprise level by the board and clearly communicated to all stakeholders (see process RG1 of the Risk IT process model). A process should be in place to review and approve any exceptions to such standards.
- 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 better risk management it has in place, the more risk can be taken in pursuit of return.
- The cost of mitigation options can affect risk tolerance; indeed, 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 a large negative impact, the enterprise may choose to accept the risk associated with regulatory non-compliance, which is a risk trade-off.

Chapter 2 of *The Risk IT Practitioner Guide* discusses risk appetite and risk tolerance in more detail.

Responsibilities and Accountability for IT Risk Management

The table in **figure 8** defines a number of roles for risk management and indicates where these roles carry responsibility or accountability for one or more activities within a process:
- Responsibility belongs to those who must ensure that the activities are completed successfully.
- Accountability applies to those who own the required resources and have the authority to approve the execution and/or accept the outcome of an activity within specific Risk IT processes. This table is a summary of the detailed tables within the process model.

The roles described in the table are implemented differently in every enterprise and, hence, do not necessarily correspond to organisational units or functions. For that purpose, each role has been briefly described in the table.

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.

Risk communication is a key part in this process; it 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

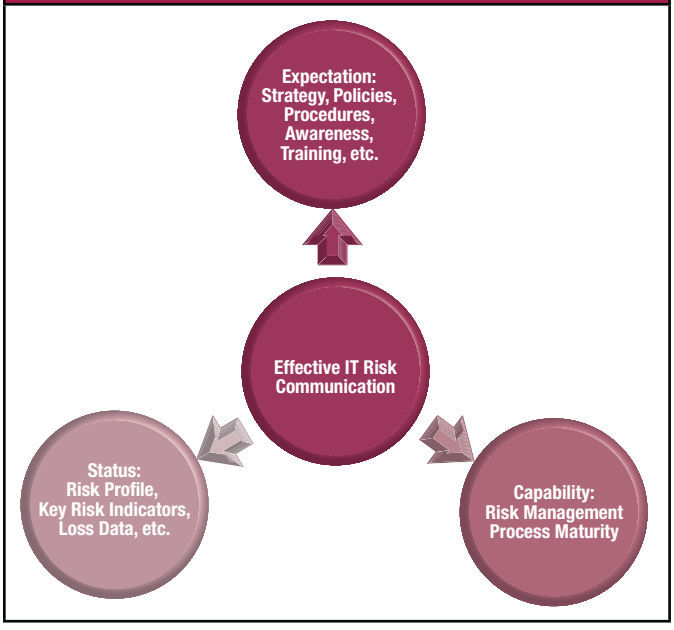
The consequences of poor communication include:
- A false sense of confidence at the top on the degree of actual exposure related to IT, and lack of a well-understood direction for risk management from the top down
- Unbalanced communication to the external world on risk, especially in cases of high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

Figure 8—Responsibilities and Accountability for IT Risk Management

Role Definitions		Risk Governance			Risk Evaluation			Risk Response		
Role	Suggested Definition	Common Risk View	Integrate With ERM	Risk-aware Decisions	Collect Data	Analyse Risk	Maintain Risk Profile	Articulate Risk	Manage Risk	React to Events
Board	The most senior executives and/or non-executives of the enterprise who are accountable for the governance of the enterprise and have overall control of its resources	●	●							
Chief executive officer (CEO)	The highest-ranking officer who is in charge of the total management of the enterprise	○	○						●	
Chief risk officer (CRO)	The individual who oversees all aspects of risk management across the enterprise. An IT risk officer function may be established to oversee IT-related risk.	○	○	○	●	○	○	●	○	○
Chief information officer (CIO)	The most senior official of the enterprise who is accountable for IT advocacy; aligning IT and business strategies; and planning, resourcing and managing the delivery of IT services and information and the deployment of associated human resources. The CIO typically chairs the governance council that manages the portfolio.	○	○	○	○	○	○	○	○	○
CFO	The most senior official of the enterprise who is accountable for financial planning, record keeping, investor relations and financial risks	○								
Enterprise risk committee	The executives who are accountable for the enterprise-level collaboration and consensus required to support enterprise risk management (ERM) activities and decisions. An IT risk council may be established to consider IT risk in more detail and advise the enterprise risk committee.	○		○		○		○		
Business management	Business individuals with roles relating to managing a programme(s)	○	○	●		●	●	○	○	○
Business process owner	The individual responsible for identifying process requirements, approving process design and managing process performance. In general, a business process owner must be at an appropriately high level in the enterprise and have authority to commit resources to process-specific risk management activities.	○	○	○	○	○	○	○	○	●
Risk control functions	The functions in the enterprise responsible for managing certain risk focus areas (e.g., chief information security officer, business continuity plan/disaster recovery, supply chain, project management office)	○	○	○	○	○	○	○	○	○
Human resources (HR)	The most senior official of an enterprise who is accountable for planning and policies with respect to all human resources in that enterprise	○								
Compliance and audit	The function(s) in the enterprise responsible for compliance and audit	○								○

Legend of the table:
- ○ Blue cell—The role carries responsibility and/or partial accountability for the process.
- ● Red cell—The role carries main accountability for this process. Only one role can be the main one accountable for a given process.

Figure 9—IT Risk Communication Components



Risk Communication—What to Communicate?

IT risk communication covers a broad array of information flows. Risk IT distinguishes amongst the following major types of IT risk communication, as shown in **figure 9**:

- Information on expectations from risk management: risk strategy, policies, procedures, awareness training, continuous reinforcement of principles, etc. This is essential communication on the enterprise's 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
  - KRIs to support management reporting on risk
  - Event/loss data
  - 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 a 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 between stakeholders are just an important a communication means for IT-risk-related information.

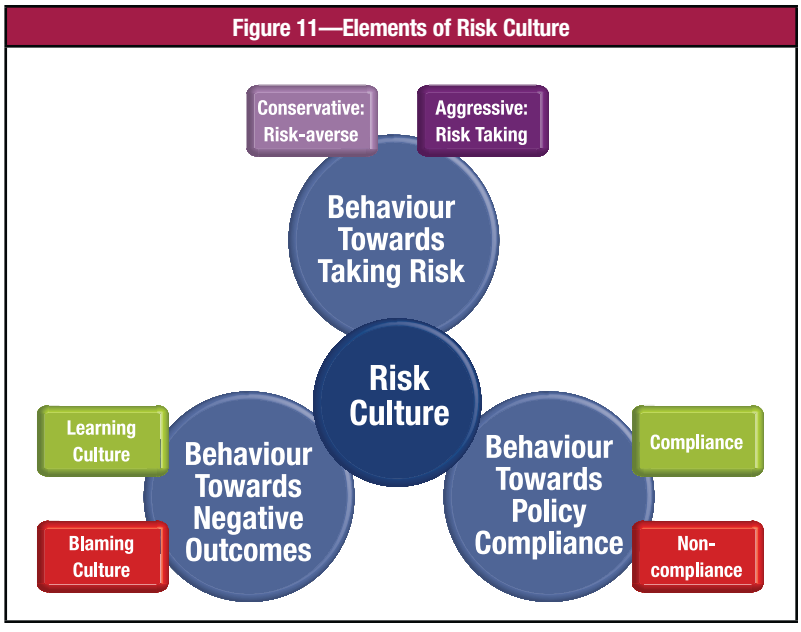
Risk Communication—Stakeholders

The table in **figure 10** provides a quick overview of the most important communication channels for effective and efficient risk management. 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. More detailed information, e.g., source and destination of information, can be found in the Risk IT process descriptions, in the input and output tables. This table is focused on the most important information that each stakeholder needs to process.

Figure 10—Risk Communication Flows		
Input	**Stakeholders**	**Output**
• Executive summary IT risk reports • Current IT risk exposure/profile • KRIs	Executive management and board	• 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
• 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	• Enterprise appetite for IT risk • Residual IT risk exposures • IT risk action plan
• 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)	• Residual IT risk exposures • Operational IT risk information • Business impact of the IT risk and impacted business units • Ongoing changes to risk factors
• Key performance objectives	Chief financial officer (CFO)	• Financial information with regard to IT and IT programmes/projects (budget, actual, trends, etc.)
• 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	• Control and compliance monitoring • Risk analysis request
• Key performance objectives • IT risk action plan • IT risk assessment methodology • IT risk register • Risk culture	IT management (including security and service management)	• IT risk mitigation strategy and plan, including assignment of responsibility and development of metrics
• Key performance objectives • IT risk RACI charts • IT risk action plan • Control and compliance monitoring	Compliance and audit	• Audit findings
• Key performance objectives • IT risk action plan • IT risk assessment methodology • IT risk register • Audit findings	Risk control functions	• Residual IT risk exposures • IT risk reports
• Risk awareness expectations • Risk culture	Human resources (HR)	• Potential IT risk • Support on risk awareness initiatives
• Control and compliance monitoring	External auditors	• Audit findings
• Public opinion, legislation • IT risk executive summary report • In general, all communications intended for the board and executive management	Regulators	• Requirements for controls and reporting • Summary findings on risk
• Executive summary risk reports	Investors	• Risk tolerance levels for their portfolio of investments
• Summary IT risk reports, including residual risk, controls maturity levels and audit findings	Insurers	• Insurance coverage (property, business interruption, directors and officers)
• Risk awareness expectations • Risk culture	All employees	• Potential IT risk issues

Risk Culture

Figure 11—Elements of Risk Culture



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 and business executives 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 11**.

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?
- Behaviour towards following policy—To what extent will people embrace and/or comply with policy?
- Behaviour towards negative outcomes—How does the enterprise 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 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.

6. Essentials of Risk Evaluation

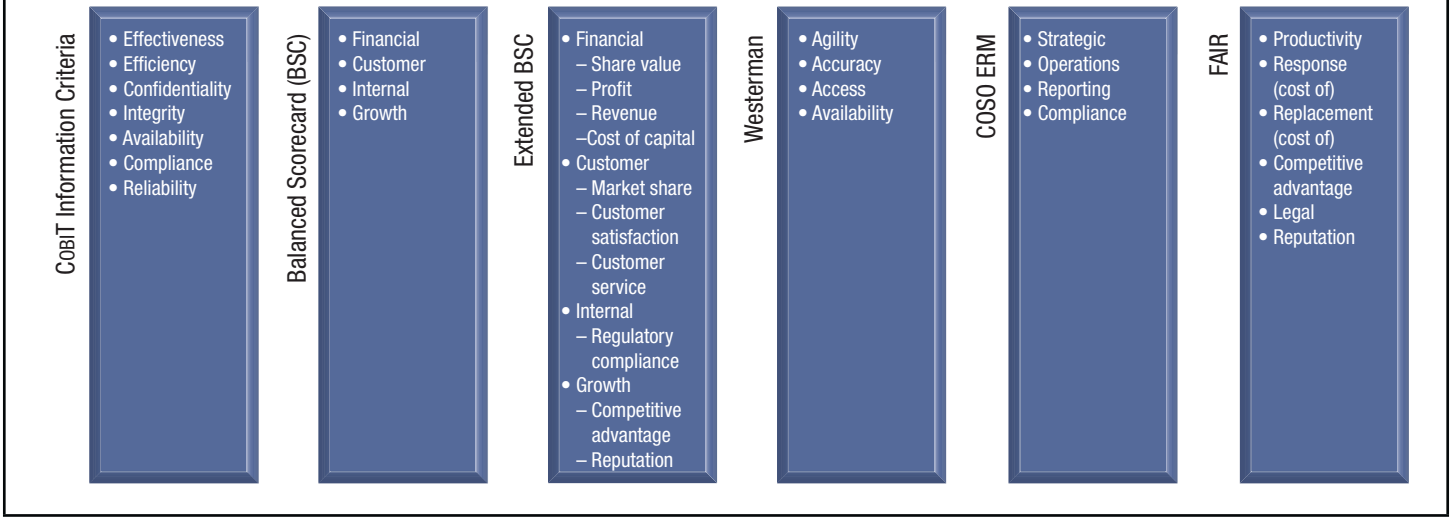
In this chapter a few essential components of the Risk Evaluation domain are discussed briefly. More information and practical guidance can be found in *The Risk IT Practitioner Guide*. The topics discussed here include:
- Describing business impact
- Risk scenarios

Describing Business Impact

Meaningful IT risk assessments and risk-based decisions require IT risk to be expressed in unambiguous and clear, business-relevant terms. Effective risk management requires mutual understanding between IT and the business over which risk needs 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 IT risks to be translated/expressed in business-relevant terms, but does not prescribe any single method. Some available methods are shown in **figure 12** and they are briefly discussed in the remainder of this section. More detail on the methods outlined in **figure 12** and guidance on how to apply them in practice are included in *The Risk IT Practitioner Guide*.

Figure 12—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 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 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.

Extended BSC Criteria

A variant of the approach described in the previous section, COBIT Business Goals and Balanced Scorecard, goes one step further, linking the BSC dimensions to a limited set of more tangible criteria. The set of criteria described in **figure 12** 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

A fourth means of expressing IT risk in business terms is based on the 4A framework[6], which 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 Enterprise Risk Management—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.

IT Risk Scenarios

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's dependence on it. One of the techniques to overcome this challenge is the development and use of risk scenarios. It is a core approach to bring realism, insight, organisational engagement, improved analysis and structure to the complex matter of IT risk.

Once these scenarios are developed, they are used during the risk analysis, where frequency of the scenario actually happening and business impacts are estimated.

Figure 13 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 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

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 over IT risk.

Once the set of risk scenarios is defined, it can be used for risk analysis, where frequency and impact of the scenario are assessed. An important component of this assessment is the risk factors, as shown in **figure 13**.

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—These can be divided into internal and external factors, the difference between them being the degree of control that 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—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 is the enterprise mature in performing the risk management processes defined in the Risk IT framework?
  - IT capabilities—How good is the enterprise at performing the IT processes defined in COBIT?

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

– IT-related business capabilities (or value management)—How closely do the enterprise's value management activities align with those expressed in the Val IT processes?

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.

Figure 13—IT Risk Scenario Development

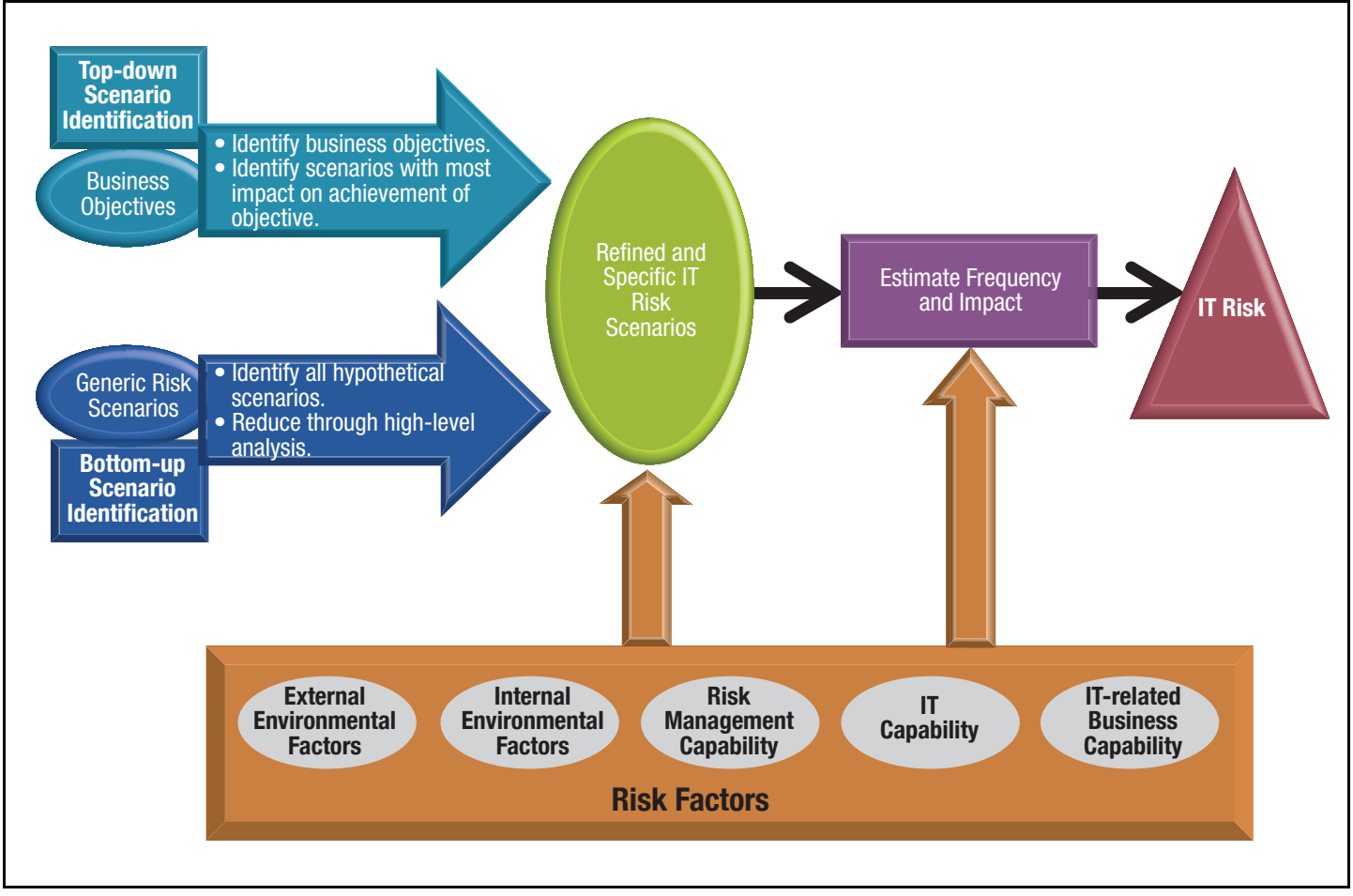
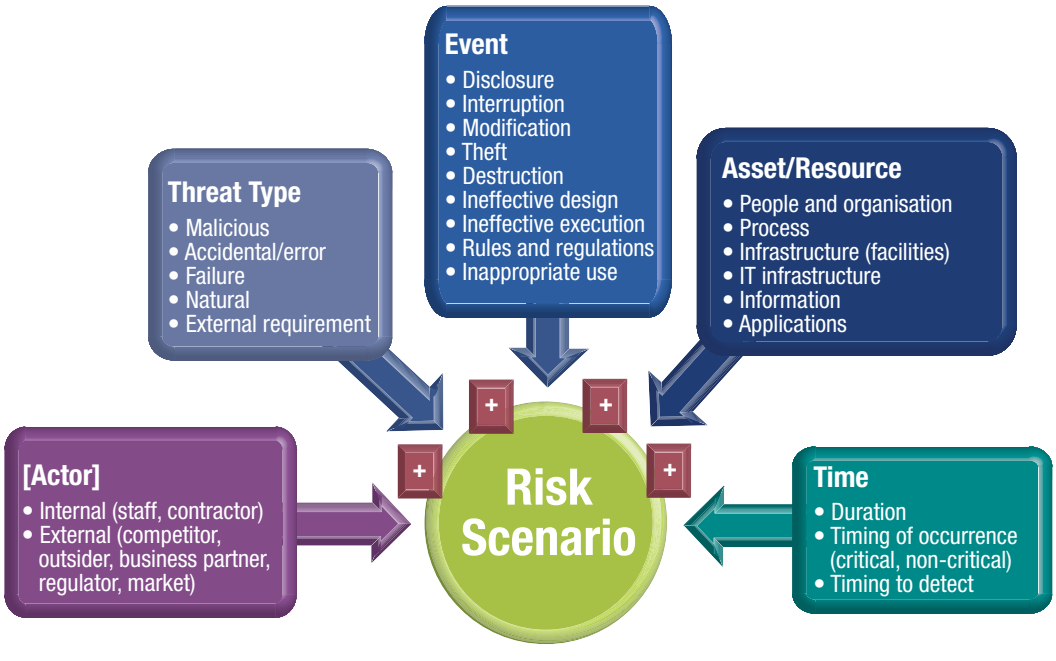


Figure 14—IT Risk Scenario Components



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, shown in **figure 14**:

- 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 (*force majeure*)?
- Event—A scenario always has to contain an event. Is it disclosure (of confidential information), interruption (of a system, a project), modification, theft, destruction, etc.? Event also includes ineffective design (of systems, processes, etc.), ineffective execution of processes (e.g., change management procedures, acquisition procedures, project prioritisation processes), regulation (impact of) and inappropriate use.
- 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 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, e.g., facilities, equipment
  - 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 the 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?)

The risk scenario structure differentiates between loss events (events generating the negative impact), vulnerabilities or vulnerability events (events contributing to the magnitude or frequency of loss events occurring), and threat events (circumstances or events that can trigger loss events). It is important not to confuse these risks or throw them into one large risk list.

The Risk IT Practitioner Guide contains extensive guidance on how to construct relevant and manageable sets of IT risk scenarios, and includes a comprehensive list of example risk scenarios.

7. Essentials of Risk Response

In this chapter, a few essential components of the Risk Response domain are discussed briefly. More information and practical guidance can be found in *The Risk IT Practitioner Guide*. The topics discussed here include:
- KRIs
- Risk response definition and prioritisation

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 steps (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.
- 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 that trigger levels can be defined that will enable stakeholders to take appropriate action in a timely manner.

Risk Response Definition and Prioritisation

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

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, or declining to engage in a very large project when the business case shows a notable risk of failure.

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., implementing sufficiently mature IT risk management processes as defined by the Risk IT framework
- Introducing a number of control measures 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.

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.

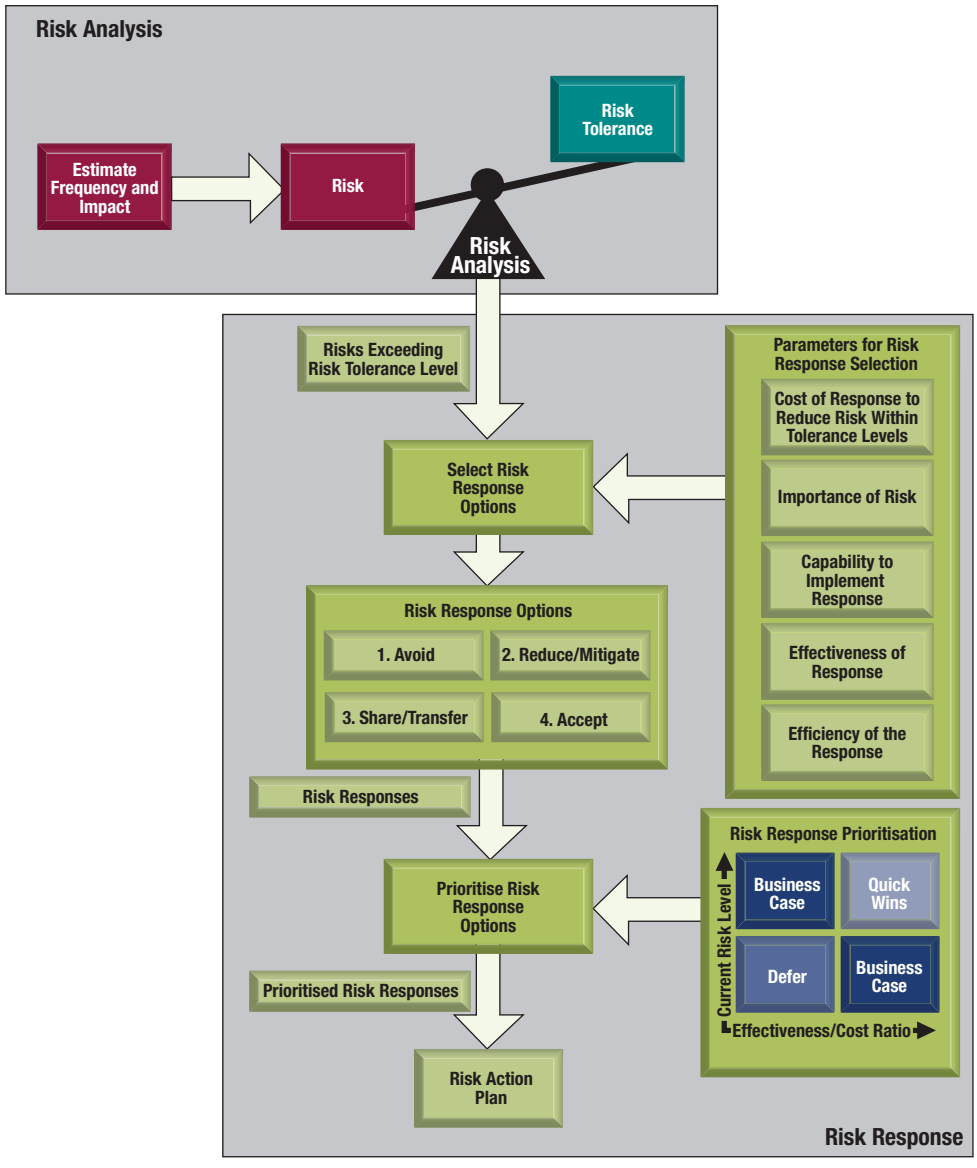
Risk Acceptance

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. If a particular risk is assessed to be extremely rare but very important (catastrophic) and approaches to reduce it are prohibitive, management can decide to accept it.

The Risk IT Practitioner Guide (chapter 6) includes examples of risk response and offers more detailed guidance on how to select and prioritise risk response. Specific to risk reduction, the COBIT and Val IT frameworks contain a comprehensive set of control measures, and *The Risk IT Practitioner Guide* offers guidance on how different risks can be reduced using these frameworks (chapter 8).

The risk response and prioritisation processes are depicted in **figure 15**.

Figure 15—Risk IT Response Options and Prioritisation



Risk Response Selection and Prioritisation

The four previous sections listed the available risk response options. Next is a brief discussion on 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. The following parameters need to be taken into account in this process:

- 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)
- The enterprise's capability to implement the response. 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

It is likely that the aggregate required effort for the mitigation share/transfer responses, e.g., 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:

- 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

For that reason, the enterprise has to select and prioritise risk responses, using the following criteria:

- 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 impact and frequency values)
- The enterprise's capability to implement the response
- Effectiveness of the response, i.e., the extent to which the response will reduce the impact and frequency of adverse events
- 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)

8. Risk and Opportunity Management Using CobiT, Val IT and Risk IT

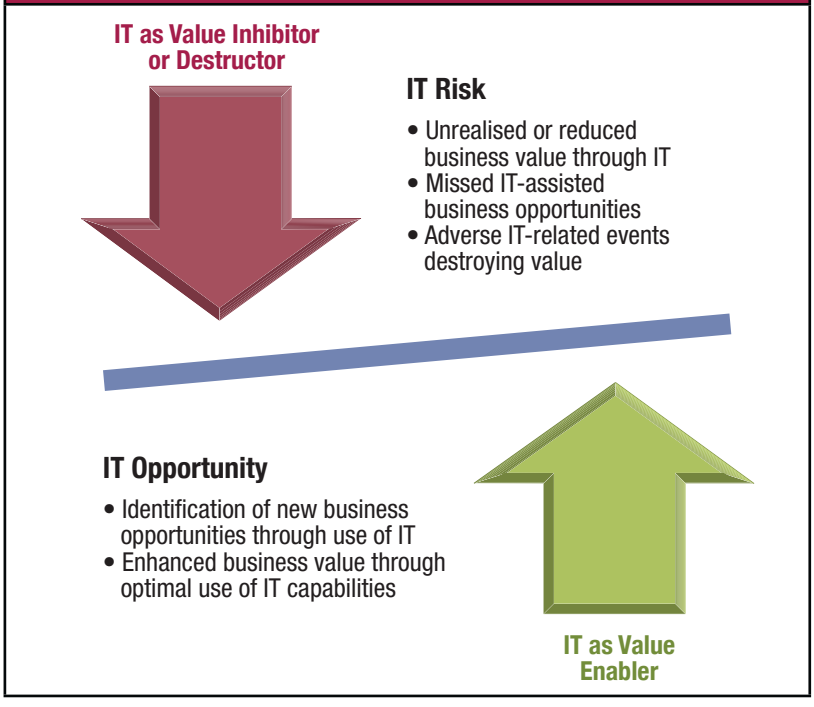
In a typical enterprise on a typical day, IT activities, organised in IT processes, are deployed. Events occur on a non-stop basis: important technology choices must be made, repairs for operational incidents must be applied, software problems need to be addressed and applications must be built. Each of these events carries both risk and opportunity.

Risk reflects the combination of the frequency of events occurring and the impact those events have on the enterprise. Risk—the potential for events and their consequences—contains opportunities for benefit (upside) or threats to success (downside). Risk and opportunity go together; indeed, to provide business value to stakeholders, enterprises must engage in various activities and initiatives (opportunities), all of which carry degrees of uncertainty and, therefore, risk. Managing risk and opportunity is a key strategic activity for enterprise success.

IT can play several roles in the risk-opportunity relationship (**figure 16**):

- Value enabler—New business initiatives almost always depend on some involvement of IT:
  - Enabling successful IT projects that support the new initiatives and, thus, the creation of value
  - Applying new technology or using new technology in innovative ways to enable new business initiatives and the creation of value
- Value inhibitor—The reverse side of the above statements applies as well:
  - IT-enabled business projects or investments often fail to deliver the expected results, so value is not delivered.
  - The enterprise may fail to identify or capture opportunities for new business initiatives arising from new technology.
- Value destruction—Some IT events, especially in IT operations, can cause mild to serious operational disruption to the enterprise, e.g., system or network outages for short or extended durations; loss, disclosure or corruption of information.

Figure 16—Risk and Opportunity



Reversing the previous statement, a capability to make a business change and implement enhanced business processes driven by IT programme and project solutions coupled with reliable, flexible and responsive IT (operational) capabilities can enable the enterprise to grow faster or take on new business initiatives. This equates to the fastest and best-performing cars needing the best brakes. Effective capabilities and controls enable enterprises to avoid risks (protect value) and take risks (value creation).

How can an enterprise deal with this in practice? Ideally, it embeds both risk-aware and opportunity-aware thinking in the evaluation and monitoring of all initiatives requiring IT involvement. For example:

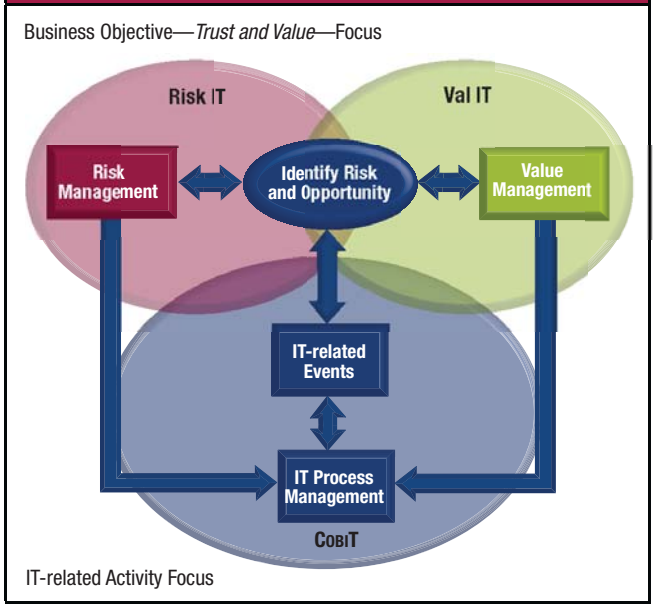
- When an important investment in IT infrastructure is proposed, either as a proactive initiative or in reaction to confirmed weaknesses, the enterprise should consider all of the following in its decision making:
  - Benefits in risk reduction of the new initiative
  - Risks associated with the investment (e.g., project risk)
  - Business benefits of possessing the resulting new IT infrastructure and opportunities
- When a new technology emerges, the enterprise should consider the following when determining whether or not to adopt the technology:
  - Impact of adopting the technology (support, reliability, ease of integration)
  - Risks associated with operating the new technology (e.g., security, reliability)
  - Consequences (e.g., obsolescence, lagging behind competitors) of not adopting the new technology
  - Business benefits of the new technology (e.g., enablement of new business initiatives, accomplishment of effectiveness and efficiency gains)

After the enterprise completes its initial assessment of the risks and/or opportunities, it needs to determine how to deal with them. Here, the three ISACA frameworks—CobiT, Val IT and Risk IT—complement each other and provide practical guidance (**figure 1**).

The COBIT processes manage all IT-related activities within the enterprise. These processes have to 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 the 'Risk Management' and 'Value Management' boxes are directed back to the 'IT Process Management' area in **figure 1**.

Some people view the risk-opportunity dichotomy as 'taking on more risk and grabbing potential opportunities'. This may be an apt description of the overall risk appetite that the enterprise has defined for itself; however, it should be noted that although taking on more risk, e.g., going forward without a full business continuity plan, may save money in the short run, it may also prohibit enterprise growth at a later stage. A good risk analysis method includes the components described previously and identifies the choices to be made. Then, sound risk management and value management practices can be applied, enabling informed decisions to be made.

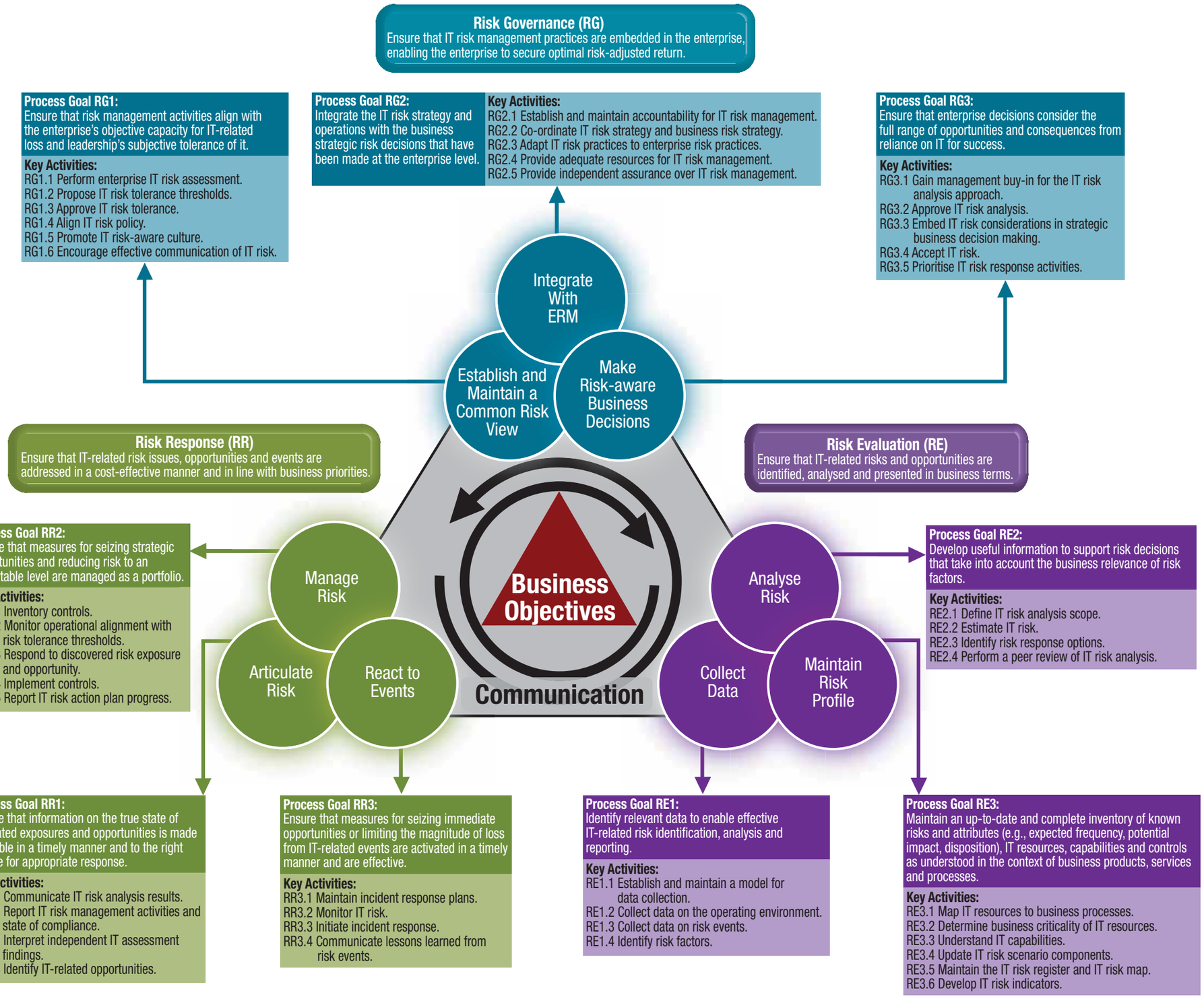
Figure 1—Positioning COBIT, Val IT and Risk IT



9. THE RISK IT FRAMEWORK PROCESS MODEL OVERVIEW

Figure 17 depicts an overview of the Risk IT process model. For each of the three domains, the domain goal and its three processes are highlighted. For each of the nine processes, the process goal and key activities are listed.

Figure 17—Risk IT Process Model Overview



Page intentionally left blank

10. Managing Risk in Practice—The Practitioner Guide Overview

The Risk IT Practitioner Guide complements *The Risk IT Framework*. The practitioner guide provides examples of possible techniques and more detailed guidance on how to approach—from a practical basis—the concepts covered in the previous chapters and in the detailed process model.

Some of the concepts and techniques treated in more detail in the practitioner guide include:
- Building scenarios, based on a set of generic IT risk scenarios
- Building a risk map, using techniques to describe the impact and frequency of scenarios
- Building impact criteria with business relevance
- Defining KRIs
- Using CobiT and Val IT to mitigate risk; the link between risk and CobiT and Val IT control objectives and key management practices

Figure 18 depicts an overview of *The Risk IT Practitioner Guide* and maps the domains and processes of the Risk IT process model to which it can be applied:
- RG1 Establish and maintain a common 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

Figure 18—*The Risk IT Practitioner Guide* Overview

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

Page intentionally left blank

11. Overview of the Risk IT Framework Process Model

This section provides an overview of the nine business processes across the three Risk IT domains: Risk Governance, Risk Evaluation and Risk Response. Management guidelines include goals and metrics at different levels and Responsible, Accountable, Consulted and Informed (RACI) charts. To enable comparisons and benchmarks, a maturity model is presented for each domain, providing an incremental measurement scale from zero through five. At level 0, 'non-existent', the enterprise has not yet adopted even the most basic IT risk management practices. At level 5, 'optimised', the enterprise is able to quantify the value from mature risk governance, risk evaluation and risk response capabilities and has the means to improve.

Detailed Process Descriptions

Process Components

An effective process is a reliable and repetitive collection of activities and controls to perform a certain task. Processes take input from one or more sources (including other processes), manipulate the input, utilise resources according to the policies, and produce output (including output to other processes). Processes should have clear business reasons for existing, accountable owners, clear roles and responsibilities around the execution of each key activity, and the means to undertake and measure performance.

Management Practices

Management practices are characteristics needed for processes to be successful. In Risk IT, management practices directly support key activities. The process detail sections provide a grouping of management practices for each key activity. (This approach is different from CobiT and Val IT, which specify activities that are related but distinct from the management practices.) The Risk IT management practices should not be considered a methodology. However, they provide a framework that enterprises can use to assess their current practices, determine where there are areas for improvement and guide initiatives to make that improvement. Each enterprise needs to consider its own policies, risk appetite and environment when selecting the management practices that best apply to that enterprise.

Inputs and Outputs

The nine Risk IT processes, although listed sequentially, are interrelated in a complex way. To illustrate how the processes share information and depend on each other, inputs and outputs are defined at the management practice/activity level (**figure 19**). (This approach is different from CobiT and Val IT, which model inputs and outputs at the process level.) Inputs suggest what information a Risk IT activity needs from other activities and processes to be successful. Concurrently, Risk IT activities generate information (outputs) to support other IT governance and enterprise risk management activities and processes (e.g., CobiT, Val IT and external business processes). Processes that exist outside CobiT, Val IT and Risk IT are indicated with an asterisk (*). The illustrative Risk IT inputs and outputs should not be regarded as an exhaustive list since additional information flows could be defined depending on a particular enterprise's environment and process framework.

The major links between the Risk IT business processes and CobiT are through the following CobiT IT processes:
- PO1 Define a strategic IT plan.
- PO2 Define the information architecture.
- PO4 Define the IT processes, organisation and relationships.
- PO5 Manage the IT investment.
- PO6 Communicate management aims and directions.
- PO9 Assess and manage IT risks.
- DS2 Manage third-party services.
- DS8 Manage service desk and incidents.
- DS10 Manage problems.
- ME1 Monitor and evaluate IT performance.
- ME2 Monitor and evaluate internal control.
- ME3 Ensure compliance with external requirements.
- ME4 Provide IT governance.

The major links between Val IT and Risk IT are through the following Val IT business processes:
- VG1 Establish informed and committed leadership.
- VG3 Define portfolio characteristics.
- VG5 Establish effective governance monitoring.
- PM4 Evaluate and select programmes to fund.
- IM1 Develop and evaluate the initial programme concept business case.
- IM2 Understand the programme candidate and implementation options.
- IM5 Develop the detailed candidate programme business case.
- IM9 Monitor and report on the programme.

In addition, *The Risk IT Practitioner Guide* makes the link amongst generic risk scenarios and management practices and controls within the CobiT and Val IT processes.

Figure 19—Example Inputs and Outputs (RE2.3)

From	Inputs
RG1.3	IT risk tolerance thresholds
RG3.4, RR3.4	Risk response requirements
RE2.1	Risk analysis scope
RE2.2	Scenario analysis results
RE3.5	IT risk profile
RR1.1, RR1.4, RR2.2	IT risk issues and opportunities
RR1.2, RR2.2	Control gaps and policy exceptions
RR2.1	Risk and control baseline
Val IT PM4	Approved investment programmes
CobiT PO5	IT budgets
CobiT PO10	Project management guidelines
CobiT ME2	Report on effectiveness of IT controls
*	Operating budget

To	Outputs
RE2.4, RR1.1	Risk analysis results

* Input from/output to outside Risk IT, Val IT and CobiT

Management Guidelines

The Risk IT management guidelines provide tools to help enterprises set up and manage risk management processes and practices in their environment. The guidelines can help with answers to typical management questions such as:

- How do the IT risk management processes and activities interrelate?
- What are the key activities that need to be undertaken or improved?
- What roles and responsibilities should be defined for successful IT risk management processes?
- How does the enterprise measure and compare IT risk management processes?
- What are the indicators of good performance?

For each Risk IT process, the guidelines provide:

- Inputs and outputs (embedded within the process detail, as described previously)
- Roles and responsibilities
- Goals and metrics

Roles and Responsibilities—RACI Chart

A RACI chart (**figure 20**) indicates which role(s) is responsible, accountable, consulted and/or informed for each key activity—defined as a group of management practices supporting the chart's associated Risk IT process. The following definitions apply to the RACI designations:

- Responsible (R)—Those who must ensure that the activities are completed successfully
- Accountable (A)—Those who own the required resources and have the authority to approve the execution and/or accept the outcome of an activity
- Consulted (C)—Those whose opinions are sought on an activity (two-way communication)
- Informed (I)—Those who are kept up to date on the progress of an activity (one-way communication)

A chart is provided for each Risk IT process.

Figure 20—Example of RACI Chart (RE2)

RACI Chart

Roles

Key Activities	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RE2.1 Define IT risk analysis scope.		I	R	C	I	C	A	R	C		C
RE2.2 Estimate IT risk.		I	R	C	C	I	A/R	R	R		C
RE2.3 Identify risk response options.			C	C	C	R	A	R	R		I
RE2.4 Perform a peer review of IT risk analysis.			A/R				I		I		I

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

Suggested definitions for the RACI roles are listed in figure 21 (these also appear in **figure 8**).

Figure 21—Role Definitions

Role	Suggested Definition
Board	The most senior executives and/or non-executives of the enterprise who are accountable for the governance of the enterprise and have overall control of its resources
Chief executive officer (CEO)	The highest-ranking officer who is in charge of the total management of the enterprise
Chief risk officer (CRO)	The individual who oversees all aspects of risk management across the enterprise. An IT risk officer function may be established to oversee IT-related risk.
Chief information officer (CIO)	The most senior official of the enterprise who is accountable for IT advocacy; aligning IT and business strategies; and planning, resourcing and managing the delivery of IT services and information and the deployment of associated human resources. The CIO typically chairs the governance council that manages the portfolio.
CFO	The most senior official of the enterprise who is accountable for financial planning, record keeping, investor relations and financial risks
Enterprise risk committee	The executives who are accountable for the enterprise-level collaboration and consensus required to support enterprise risk management (ERM) activities and decisions. An IT risk council may be established to consider IT risk in more detail and advise the enterprise risk committee.
Business management	Business individuals with roles relating to managing a programme(s)
Business process owner	The individual responsible for identifying process requirements, approving process design and managing process performance. In general, a business process owner must be at an appropriately high level in the enterprise and have authority to commit resources to process-specific risk management activities.
Risk control functions	The functions in the enterprise responsible for managing certain risk focus areas (e.g., chief information security officer, business continuity plan/disaster recovery, supply chain, project management office)
Human resources (HR)	The most senior official of an enterprise who is accountable for planning and policies with respect to all human resources in that enterprise
Compliance and audit	The function(s) in the enterprise responsible for compliance and audit

Figures 8 and **21**, while not intended to represent an organisational chart or structure, show the interrelationships amongst the suggested roles.

The actual assignment of R, A, C and I will vary amongst enterprises depending on their organisational model and other factors. Certain regulatory requirements may assign responsibilities to specific roles. For example, banking regulations assign accountability to boards for certain activities that otherwise might not receive that high a level of attention, or financial market regulations may assign certain activities to a business continuity leader. For each key activity, ideally only one person is accountable (i.e., assigned an A). Those who are assigned an A should have the appropriate authority and sufficient resources to sponsor the activity. One or more people may be made responsible (i.e., assigned an R) depending on the activity's scope. Roles not assigned an R, A, C or I for a given activity are typically not directly involved with or affected by the activity's performance. The assignments in Risk IT are meant to be generic and constitute suggested examples only.

The following assumptions were made when developing the RACI charts in Risk IT:

- 'Effective governance across all risk management disciplines (including credit risk, interest rate risk, liquidity risk and operational risk) is highly dependent on the capability maturity of the three lines of defence model … The three lines of defence model distinguishes amongst functions owning and managing risks, functions overseeing risks, and functions providing independent assurance …'[7]. As such, Risk IT segregates the role of audit from the CRO and the risk control functions. (This approach is different from CobiT and Val IT, which represent compliance, audit, risk and security as a group of roles.)
- The CIO does not report through any other CxO, such as the CFO or chief operating officer (COO), but instead reports directly to the CEO.
- The CIO has all subordinate IT management roles reporting to him/her and can, therefore, control and answer for all of them.
- The CRO has all subordinate IT risk roles, e.g., an IT risk and compliance group or a business risk analysis group, reporting to him/her and can, therefore, control and answer for all of them.
- Due to staffing and budget, in actual practice some roles may need to be multifunctional.

Goals and Metrics

Risk IT presents a top-down cascade of goals and metrics across the domain, process and activity levels. Goals define what the business expects. Domain goals are achieved by the interaction of processes, each of which has distinct process goals that, in turn, rely on activity goals. Metrics can be lag indicators, which provide a measure of what has actually been done or achieved, or lead indicators, which provide a measure of what potentially may be achieved. Taken together, goals and metrics can provide building blocks for a business scorecard. (It is important to note that in Risk IT the activity goal and the activity name are the same.)

Figure 22 contains an example of a goals and metrics table.

[7] ISACA, *IT Control Objectives for Basel II, The Importance of Governance and Risk Management for Compliance*, USA, 2007, p. 56-57, *www.isaca.org*

Figure 22—Example of Goals and Metrics Table (RE2)

Activity Goals	Process Goal	Domain Goal
• Define IT risk analysis scope. • Estimate IT risk. • Identify risk response options. • Perform a peer review of IT risk analysis.	• Develop useful information to support risk decisions that take into account the business relevance of risk factors.	• Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.

Activity Metrics	Process Metrics	Domain Metric
• Percentage of time analyses are substantiated by later experience or testing (accuracy) • Percentage of time that peer review finds no significant logical, calculation or incompleteness errors (defensibility) • Percentage of time that parallel assessments on the same scenarios performed by different analysts get the same results (consistency) • Percentage of time that analyses are performed by trained analysts (higher-level metric related to accuracy, defensibility and consistency) • A 'satisfaction index', derived over risk analysis reporting (e.g., the percentage of favourable satisfaction survey responses from business executives regarding the readability, usefulness and accuracy of risk analysis reports)	• Percentage of risks for which the probable frequency of occurrence and the probable magnitude of the business impact are measured within the scope • Percentage of critical assets, targets and resources reviewed for the effect of known operational controls • Percentage of risk analysis undergoing peer review before being sent to management • Ratio of cumulative actual losses to expected loss magnitude	• The cumulative business impact from IT-related incidents and events not identified by risk evaluation processes

Maturity Models

Boards and executive management need to consider how effective their enterprises are at managing IT risk and should be able to answer these related questions:
- What are the enterprise's peers doing to manage IT risk, and how does the enterprise compare to them?
- What are the proven good practices in IT risk management, and how does the enterprise compare to them?
- Based on these comparisons, is the enterprise doing enough?
- How does the enterprise identify what it needs to do to reach the level of IT risk management that is sought?

It can be difficult to obtain meaningful answers to these questions. Management is constantly looking for benchmarking and self-assessment tools in response to the need to know what to do to achieve the best results. One such tool is maturity modelling, which can enable the enterprise to rate itself from the least mature level (having non-existent or unstructured processes) to the most mature (having adopted and optimised the use of good practices).

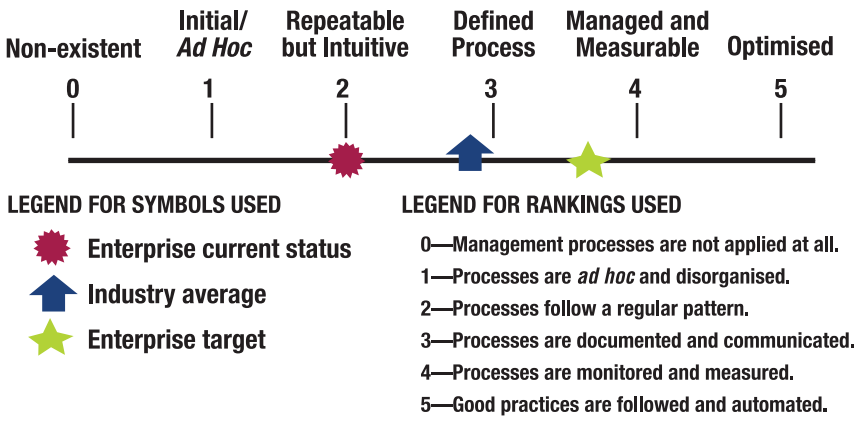
When modelling maturity, it is useful to identify a limited number of levels. A larger number would render the system difficult to use and suggest a precision that is not justifiable. In general, the purpose is to identify where enterprises are for certain activities and suggest how to set priorities for improvements.

The Risk IT maturity levels are designed as profiles in which an enterprise can identify symptoms or descriptions of its current and possible future states. Each enterprise will recognise that many of its processes are at different maturity levels; for example, some processes may be at level 1, some at level 3 and others at level 4. In this way, the maturity models are designed to enable management to focus on key areas needing attention, rather than on trying to get all processes stabilised at one level before moving to the next.

Using the Risk IT maturity models, management can identify:
- The actual performance of the enterprise—Where the enterprise is today
- The enterprise's target for improvement—Where the enterprise wants to be

To make the results easily usable in management briefings—where they should be presented as a means to support the case for future plans to improve risk governance, evaluation and response—a graphic presentation method might need to be provided (**figure 23**).

Figure 23—Maturity Model



For each Risk IT domain, both high-level and detailed versions of the maturity model are provided. The detailed versions are built around the following attributes, each of which evolves through the categories:

- Awareness and communication
- Responsibility and accountability
- Goal setting and measurement
- Policies, standards and procedures
- Skills and expertise
- Tools and automation

The maturity model scales can help management understand where shortcomings exist and set targets for where they need to be. The most appropriate maturity level for an enterprise will be influenced by the enterprise's business objectives, the operating environment and industry practices. Specifically, the level of IT risk management maturity will depend on the enterprise's dependence on IT, its technological sophistication and, most important, the future role its executives and management foresee for information technology.

Page intentionally left blank

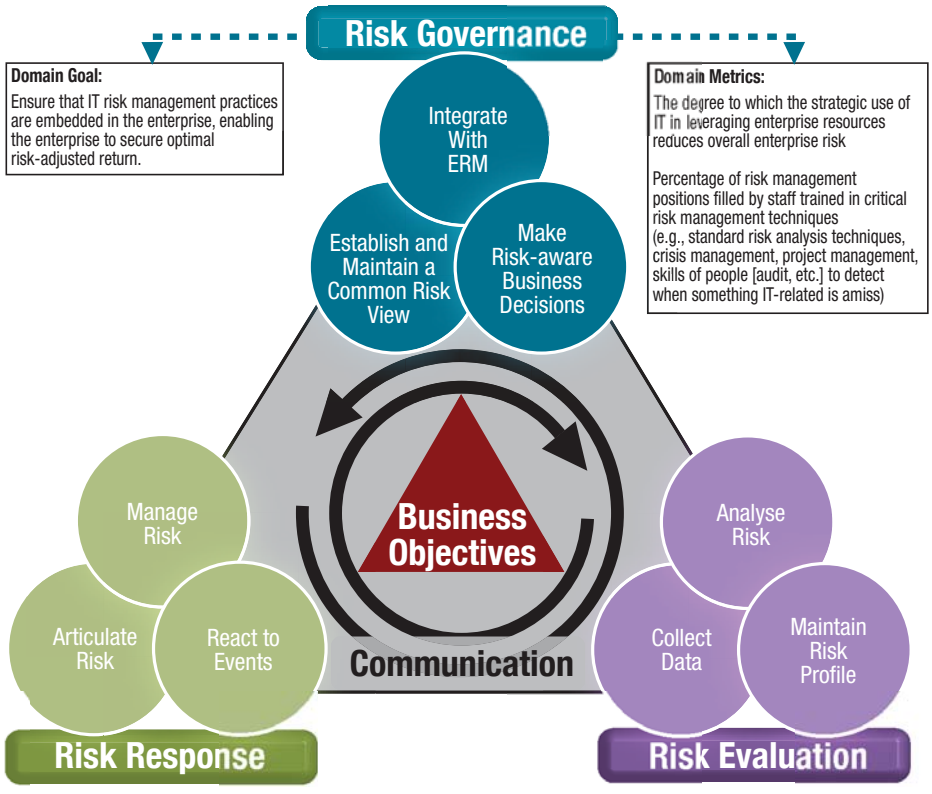
12. THE RISK IT FRAMEWORK

This chapter presents the framework itself and contains the following:
- Domain-level information:
  - Domain overview—A graphic overview of the domain within the framework, highlighting the domain goal(s) and metric(s) (**figures 24**, **30** and **36**)
  - Maturity model—High-level and detailed views (**figures 28, 29, 34, 35, 40** and **41**)
- Process-level information:
  - Process overview—A graphic overview of the process within the framework, highlighting the process goal and key activities (**figures 25, 26, 27, 31, 32, 33, 37, 38** and **39**)
  - Process detail—Key management practices, with inputs and outputs
  - Management guidelines—RACI charts, goals and metrics

The Risk IT framework consists of:
- Domain—Risk Governance (RG)
  - RG1 Establish and maintain a common risk view
  - RG2 Integrate with ERM
  - RG3 Make risk-aware business decisions
- Domain—Risk Evaluation (RE)
  - RE1 Collect data
  - RE2 Analyse risk
  - RE3 Maintain risk profile
- Domain—Risk Response (RR)
  - RR1 Articulate risk
  - RR2 Manage risk
  - RR3 React to events

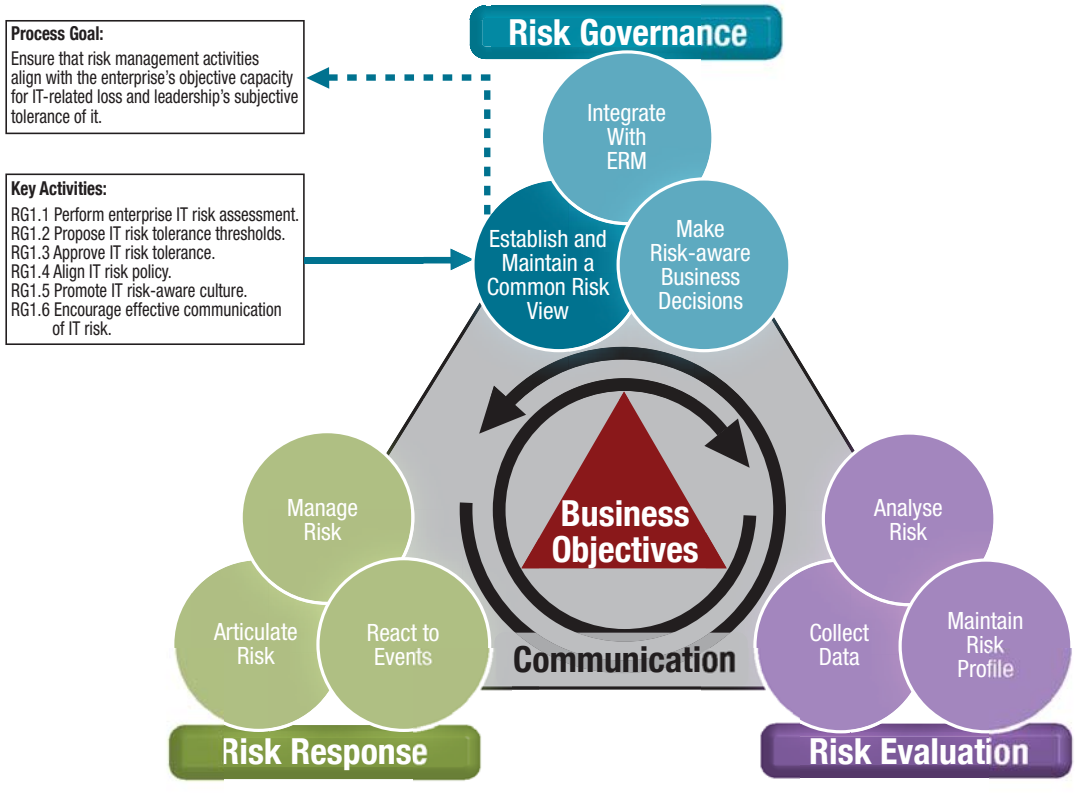
DOMAIN OVERVIEW—RISK GOVERNANCE (RG)

Figure 24—Risk Governance Domain



PROCESS OVERVIEW

Figure 25—Process RG1 Establish and Maintain a Common Risk View



PROCESS DETAIL

RG1 Establish and maintain a common risk view.

Ensure that risk management activities align with the enterprise's objective capacity for IT-related loss and leadership's subjective tolerance of it.

RG1.1 Perform enterprise IT risk assessment.

Sponsor workshops with business management to discuss the broad amount of risk that the enterprise is willing to accept in pursuit of its objectives (risk appetite). Help business managers understand IT risk in the context of scenarios that affect their business and the objectives that matter most in their daily lives (e.g., sales, cost, customer satisfaction, cash). Take a top-down, end-to-end look at business services and processes and identify the major points of IT support. Identify where value is generated and needs to be protected and sustained. Identify IT-related events and conditions that may jeopardise value, affect enterprise performance and execution of critical business activities within acceptable bounds, or otherwise affect enterprise objectives (e.g., business, regulatory, legal, contracts, technology, trading partner, human resources, other operational aspects). Map them to a business-driven hierarchy of risk categories (e.g., IT benefit/value enablement, IT programme and project delivery, IT operations and service delivery) and subcategories (IT risk domains) derived from high-level IT risk scenarios. Break up IT risk by lines of business, product, service and process. Identify potential cascading and coincidental threat types and the probable effect of risk concentration and correlation across silos. Understand how IT capabilities contribute to the enterprise's ability to add value and withstand loss. Compare management's perception of the importance of IT capabilities to their current state. Consider how IT strategies, change initiatives and external requirements (e.g., regulation, contracts, industry standards) may affect the risk profile. Identify risk focus areas, scenarios, dependencies, risk factors and measurements of risk that require management attention and further examination and development.

From	Inputs
RG2.2	Integrated risk management strategy
RG2.3	Integrated risk management methods
RE1.4	Risk factors
RE3.3	IT capability assessment
RE3.4	IT risk scenario components
RE3.5	IT risk profile
RR1.3	Independent IT assessment findings in context
Val IT PM1	IT strategy and goals feedback
Val IT IM7	Service portfolios
CobiT PO1	Strategic IT plan, tactical IT plans, IT project portfolio, IT service portfolio, IT sourcing strategy, IT acquisition strategy
CobiT PO4	Documented system owners, IT organisation and relationships
CobiT ME3	Catalogue of legal and regulatory requirements related to IT service delivery, report on compliance of IT activities with external legal and regulatory requirements
CobiT ME4	Enterprise appetite for IT risk, enterprise strategic direction for IT
*	Enterprise strategy, objectives, goals, risk universe, risk appetite, risk management framework, legal and regulatory requirements mappings

* Input from/output to outside Risk IT, Val IT and CobiT

To	Outputs
RG1.2, RG1.3, RG1.4, RE2.1, *	Key business and IT objectives, major risk factors
RG1.2, RG1.3, RG1.4, RG1.5, RG2.1, RG2.2, RE2.1, RR2.1	Risk focus areas
RG1.2, RG1.3, RG1.4, RG1.5, RG2.2, RG3.3, RE2.1, RE3.1, RE3.4	High-level risk scenarios
RG1.2, RG1.3, RG1.4, RG2.2, RG3.3, RE2.1, RE3.1, RE3.4; Val IT VG1; CobiT PO1, PO9, DS1	Key services and supporting business processes and systems
RG1.2, RG1.3, RG1.4, RG1.5, RE2.1, RE3.2, RE3.4	Prioritised inventories of risk and impact categories
RE2.1	Risk analysis request
RE3.2	Asset/resource criticality (macro level)

* Input from/output to outside Risk IT, Val IT and CobiT

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 the context of risk-return balance. Propose limits and measures in the context of IT benefit/value enablement, IT programme and project delivery, and IT operations and service delivery, and over multiple time horizons (e.g., immediate, short-term, long-term).

From	Inputs
RG1.1	Key business and IT objectives, major risk factors, risk focus areas, high-level risk scenarios, key services and supporting business processes and systems, prioritised inventories of risk and impact categories
RG1.3	IT risk tolerance thresholds (approved)
COBIT ME4	Enterprise appetite for IT risk, enterprise strategic direction for IT
*	Business risk tolerance thresholds

To	Outputs
RG1.3	IT risk tolerance thresholds (proposed)

* Input from/output to outside Risk IT, Val IT and COBIT

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 objectives 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.

From	Inputs
RG1.1	Key business and IT objectives, major risk factors, risk focus areas, high-level risk scenarios, key services and supporting business processes and systems, prioritised inventories of risk and impact categories
RG1.2	IT risk tolerance thresholds (proposed)
COBIT ME4	Enterprise appetite for IT risk, enterprise strategic direction for IT
*	Business risk tolerance thresholds

To	Outputs
RG1.2, RG1.4, RG1.5, RG1.6, RG2.4, RG2.5, RG3.3, RG3.4, RG3.5, RE2.2, RE2.3, RE3.2, RE3.5, RE3.6, RR1.3, RR2.1, RR2.2, RR3.2, RR3.4; Val IT VG3; COBIT PO9; *	IT risk tolerance thresholds

* Input from/output to outside Risk IT, Val IT and COBIT

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.

From	Inputs
RG1.1	Key business and IT objectives, major risk factors, risk focus areas, key services and supporting business processes and systems, prioritised inventories of risk and impact categories, high-level risk scenarios
RG1.3	IT risk tolerance thresholds
RG2.1	IT risk domain owners, performance targets, incentives and rewards, integrated roles and responsibilities for risk management and oversight
RG2.2	Integrated risk management strategy
RE1.4	Risk factors, emerging threats
RE3.5	IT risk profile
RR1.1, RR1.4, RR2.2	IT risk issues and opportunities
RR1.2	State of compliance reports
CobiT PO3	Technology standards
CobiT PO6	IT policies
CobiT ME4	Enterprise appetite for IT risk, enterprise strategic direction for IT
*	Enterprise policies and standards (IT-related)

* Input from/output to outside Risk IT, Val IT and CobiT

To	Outputs
RG1.5, RG1.6, RG2.1, RG2.2, RG2.4, RG2.5, RG3.1, RR1.3, RR2.1; Val IT VG5; CobiT PO6; *	IT risk policy
RG1.5, RG1.6; CobiT PO3, PO4, PO6, PO7; *	IT-related policies and standards (updates)

* Input from/output to outside Risk IT, Val IT and CobiT

RG1.5 Promote IT risk-aware culture.

Based on an understanding of the current risk culture, empower the enterprise to proactively identify IT risk, opportunity and potential business impacts. Encourage employees to address IT risk issues before serious escalation is required. Train business and IT staff on threats, impacts and the enterprise's planned responses to specific risk events. Communicate the 'why you should care' message for risk focus areas, and explain how to take risk-aware actions for situations not specified in policies. Walk through scenarios for areas not directly covered by policy, and reinforce expectations for understanding general policy direction and using good judgement. Demonstrate an attitude that encourages discussion and acceptance of the appropriate amount of risk. Be positive about promoting a risk culture appropriate for IT and aligned with enterprise risk-aware culture.

From	Inputs
RG1.1	Risk focus areas, high-level risk scenarios
RG1.3	IT risk tolerance thresholds
RG1.4	IT risk policy, IT-related policy and standards (updates)
RG2.1	Performance targets, incentives and rewards, integrated roles and responsibilities for risk management and oversight
RG2.3	Integrated risk management methods
RE3.4	IT risk scenario components
RR1.2	State of compliance reports
*	Risk culture survey results, data on adherence to policy and standards, data on risk tolerance thresholds vs. policy vs. operations

* Input from/output to outside Risk IT, Val IT and CobiT

To	Outputs
RE1.2	Performance metrics on cultural shift towards risk awareness
CobiT PO6	IT risk management guidelines
CobiT DS7	Specific training requirements for IT risk management

* Input from/output to outside Risk IT, Val IT and CobiT

RG1.6 Encourage effective communication of IT risk.

Establish and maintain a risk communication plan that covers IT risk policy, responsibilities, accountabilities and the risk landscape (e.g., threats, controls, impacts, root causes, business decisions). Feature filters in the plan so it is clear, concise, useful and directed to the right audience. Perform frequent and regular communication between IT management and business leadership regarding IT risk issue status, concerns and exposures. Base business and IT management communications on a predefined approach with the following objectives:

- Align IT risk communication with enterprise risk terms.
- Consistently prioritise IT risk issues in a manner that aligns with the enterprise definition of business risk.
- Express IT risk in business strategic and operational terms.
- Clearly communicate how adverse IT-related events may affect business objectives (e.g., business goals/balanced scorecard, the 4 'A's[8], COSO ERM objective categories).
- Enable senior managers and IT executives to understand the actual amount of IT risk to help steer the right resources to respond to IT risk in line with appetite and tolerance.

From	Inputs
RG1.3	IT risk tolerance thresholds
RG1.4	IT risk policy, IT-related policy and standards (updates)
RG2.1	Performance targets, incentives and rewards, integrated roles and responsibilities for risk management and oversight
RG2.3	Integrated risk management methods
RR1.1, RR1.4, RR2.2	IT risk issues and opportunities
RR2.5	IT risk action plan progress/deviations
RR3.4	Root cause of incidents
COBIT PO4	Documented system owners, IT organisation and relationships

To	Outputs
All, COBIT PO6	IT risk communication plan
All, *	Communication of IT risk

* Input from/output to outside Risk IT, Val IT and COBIT

MANAGEMENT GUIDELINES—RG1

RACI Chart **Roles**

Key Activities	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RG1.1 Perform enterprise IT risk assessment.	I	A	R	R	C	I	R	C	R	C	C
RG1.2 Propose IT risk tolerance thresholds.	I	I	C	R	C	I	A	C	C		C
RG1.3 Approve IT risk tolerance.	A	C	C	C	C	R	C	C	C	C	C
RG1.4 Align IT risk policy.	C	A	R	R	R	C	R	R	R	R	C
RG1.5 Promote IT risk-aware culture.	A	R	R	R	R	R	R	R	R	R	R
RG1.6 Encourage effective communication of IT risk.	R	R	R	R	R	R	A	R	R	R	R

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

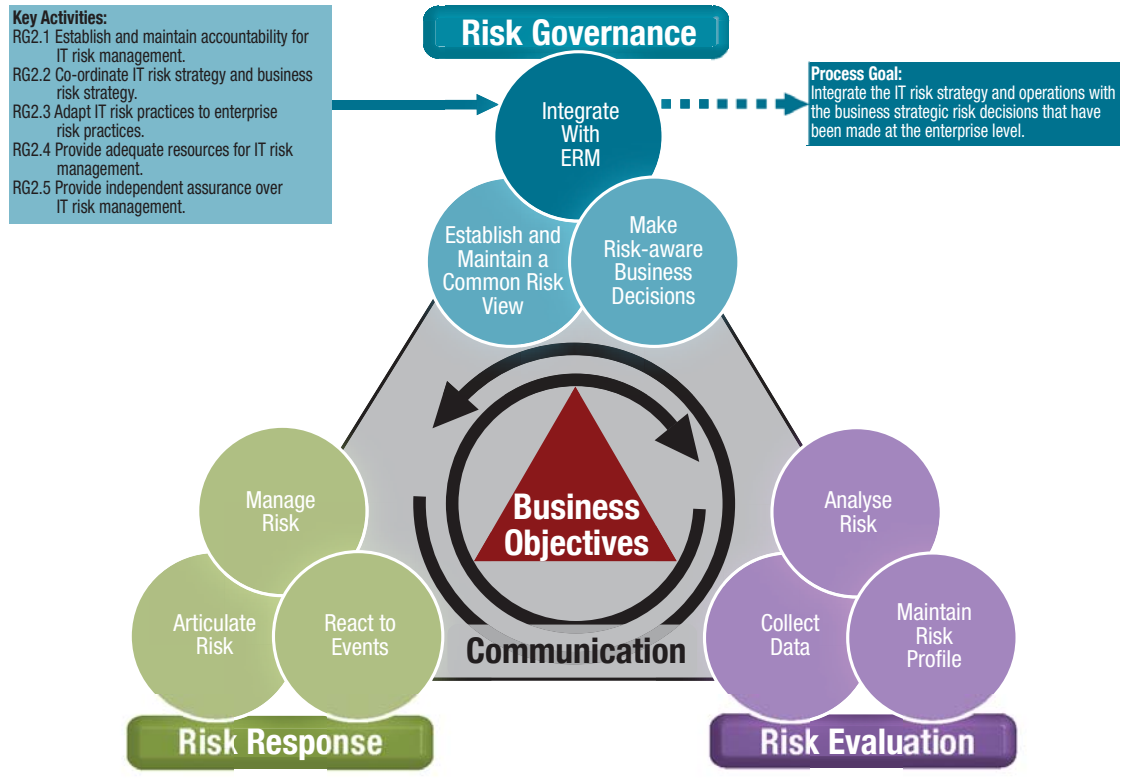
[8] Westerman, *op cit*

Goals and Metrics—RG1

Activity Goals	Process Goal	RG Goal
• Perform enterprise IT risk assessment. • Propose IT risk tolerance thresholds. • Approve IT risk tolerance. • Align IT risk policy. • Promote IT risk-aware culture. • Encourage effective communication of IT risk.	• Ensure that risk management activities align with the enterprise's objective capacity for IT-related loss and leadership's subjective tolerance of it.	• Ensure that IT risk management practices are embedded in the enterprise, enabling the enterprise to secure optimal risk-adjusted return.
Activity Metrics	**Process Metrics**	**RG Metrics**
• Frequency of enterprise IT risk assessment • Number of out-of-cycle enterprise IT risk assessments • Level of executive participation in enterprise IT risk assessment (e.g., attend in person, send a subordinate, receive report) • Existence of an IT risk policy • Number of aligned policies to which intended audience has signed adherence • Percentage of employees trained on IT risk management responsibilities • Number of communications that establish and reinforce IT risk policy and management expectations • Coverage of enterprise by communication on IT risk policy	• Number of known executive-level risk tolerance violations not subjected to disciplinary action (enforcement of policy) • Number of IT-related events with business impact in which a failure to escalate was a factor in event occurrence and/or the loss magnitude (e.g., the risk manager did not know or there was an impaired cultural ability to escalate) • Number of policies in force with one or more statements contradicting a related risk tolerance (alignment of IT policies with tolerance) • Number of IT risk issues that exceed risk tolerance	• The degree to which the strategic use of IT in leveraging enterprise resources reduces overall enterprise risk • Percentage of risk management positions filled by staff trained in critical risk management techniques (e.g., standard risk analysis techniques, crisis management, project management, skills of people [audit, etc.] to detect when something IT-related is amiss)

PROCESS OVERVIEW

Figure 26—Process RG2 Integrate With ERM



PROCESS DETAIL

RG2 Integrate with ERM.

Integrate the IT risk strategy and operations with the business strategic risk decisions that have been made at the enterprise level.

RG2.1 Establish and maintain accountability for IT risk management.
Specify those accountable and responsible for the management of IT risk across the enterprise. For the top-level executive with overall accountability for IT risk, set a performance expectation to incorporate risk awareness in the culture. Establish performance measurements and reporting processes with appropriate levels of recognition, approval, incentives and sanctions. Ensure that there are structures in place (e.g., enterprise risk committee, IT risk council, IT risk officer) to involve the business with risk-return-aware decisions and day-to-day operations. Create a distinction amongst the roles of business units (who own and manage the risk on a day-to-day basis), risk control functions (who offer subject matter expert evaluation and advice) and internal audit (who provide independent assurance). Identify business managers with authority to address IT risk issues across IT benefit/value enablement, IT programme and project delivery, and IT operations and service delivery. Set expectations for these managers to champion policies, standards, controls and compliance monitoring activities (e.g., establishment and monitoring of KRIs). Set and evaluate performance targets based on risk-return-aware decision making (e.g., the ability of managers to integrate and balance performance management with risk management across their scope of authority). Assign roles for managing specific IT risk domains (e.g., system capacity, IT staffing, IT programme selection). Assign each domain a level of criticality based on risk/reward. As required, assign additional risk management responsibilities (e.g., system-specific) at lower levels.

From	Inputs
RG1.1	Risk focus areas
RG1.4	IT risk policy
RG2.2	IT risk management scope
RG3.4, RR3.4	Risk response requirements
RR1.1, RR1.4, RR2.2	IT risk issues and opportunities
Val IT VG1	Leadership commitment
Val IT VG2	Business roles, responsibilities, accountabilities
CobiT PO4	Documented system owners, IT organisation and relationships
CobiT PO7	Roles and responsibilities

To	Outputs
RG1.4, RR2.1	IT risk domain owners
RG1.4, RG1.5, RG1.6, RG2.5; CobiT PO4, PO7; *	Performance targets, incentives and rewards, integrated roles and responsibilities for risk management and oversight
RG2.2, RG2.5, RG3.3, RR2.4, RR2.5, RR3.1; Val IT PM4; CobiT PO4, PO9, AI6, ME1, ME2	IT risk action plans
RG2.4, RE3.1; CobiT PO4, PO7; *	Roles and responsibilities

* Input from/output to outside Risk IT, Val IT and CobiT

RG2.2 Co-ordinate IT risk strategy and business risk strategy.
Determine how IT-related risk management is to be defined in the context of protecting and sustaining a given business process or business activity. Adopt and align with the existing enterprise framework for business risk. Integrate any IT specifics into one enterprise approach. Understand the enterprise's risk goals and objectives and the mix of competing business risk issues and resource limitations. Determine how IT risk management is to be approached in the context of the enterprise's risk universe and other enterprise risk types. Define the IT department's role in operational risk management activities based on the extent of the business's dependency on IT and related physical infrastructure in achieving financial, operational and customer-satisfaction objectives. Co-ordinate risk assessment activities and perform integrated reporting. Co-ordinate risk and issue classification; risk rating scales (e.g., frequency, magnitude, business impact); control categories (e.g., predictive, detective, corrective); and hierarchies for risk-based policies, standards and operating procedures. Where available, employ existing ERM principles and views of risk (e.g., actuarial view, portfolio view, predictive systems view). Determine when and how certain enterprise risk views are to be used for IT risk. Accommodate the enterprise's unique performance needs and external requirements.

From	Inputs
RG1.1	Risk focus areas, key services and supporting business processes and systems, high-level risk scenarios
RG1.4	IT risk policy
RG2.1, RG2.3, RR2.3, RR3.4	IT risk action plans
RR1.2	Inputs to integrated enterprise risk reporting
RR1.1, RR1.4, RR2.2	IT risk issues and opportunities
RR2.2	Monitoring requirements
RR3.1	Incident response plans
RR3.4	Process improvements
CobiT PO9	IT-related risk management guidelines
CobiT ME4	Enterprise appetite for IT risk, enterprise strategic direction for IT
*	Enterprise strategy, objectives, goals, risk universe, risk appetite and risk management framework

* Input from/output to outside Risk IT, Val IT and CobiT

To	Outputs
RG1.1, RG1.4, RG2.3, RG3.4, RE1.1, RE2.1, RR1.1, RR2.1, RR2.2, RR3.2, CobiT PO9	Integrated risk management strategy
RG2.1, RG2.3, RG2.4, RG2.5, CobiT PO6	IT risk management scope
RG2.5, RG3.3, RR2.4, RR2.5, RR3.1; Val IT PM4; CobiT PO4, PO9, AI6, ME1, ME2	IT risk action plans
RE3.2, RE3.4	Prioritised inventories of risk and impact categories
RR1.2	Integrated risk reporting requirements
CobiT PO1; *	Integrated business strategy and priorities
*	Updates to enterprise risk strategy

* Input from/output to outside Risk IT, Val IT and CobiT

RG2.3 Adapt IT risk practices to enterprise risk practices.

Organise existing IT risk management methods—those required to: 1) understand the business context for IT (e.g., business activity IT dependency analysis, scenario analysis); 2) identify IT risk (e.g., data model, escalation pathways); 3) govern IT risk (e.g., enterprise IT risk assessment procedures, risk-based decision models); and 4) manage IT risk (e.g., select the right KRIs for the right business performance targets and define escalation procedures). Understand enterprise risk management expectations, activities and methods that are relevant to IT risk management (e.g., issue management, communication and training, how risk is identified and measured, how controls are evaluated, what information is provided to whom, how risk appetite is established and agreed upon). Identify gaps and specific IT risk management practices that should be updated or created to meet ERM expectations. Likewise, identify enterprise risk activities that should be added or updated to fully consider IT risk. Identity what other functions do, or need to do, in support of the enterprise's objectives and management of IT risk. Prioritise and track efforts to close the gaps between IT risk and ERM, and improve effectiveness and efficiency (e.g., optimise controls, streamline risk assessment, co-ordinate KRIs and escalation triggers, integrate reporting).

From	Inputs
RG2.2	Integrated risk management strategy, IT risk management scope
RG3.1	IT risk analysis approach issues
RR2.2	Key IT risk indicators and escalation triggers
RR3.4	Process improvements
CobiT PO9	IT-related risk management guidelines

To	Outputs
RG1.1, RG1.5, RG1.6, RG3.1, RE2.1, RE2.2, RE3.2, RR3.2, RR3.4	Integrated risk management methods
RG2.2, RG2.5, RG3.3, RR2.4, RR2.5, RR3.1; Val IT PM4; CobiT PO4, PO9, AI6, ME1, ME2	IT risk action plans
*	Updates to ERM activities, integrated issue management process and platform shared by the various functions

* Input from/output to outside Risk IT, Val IT and CobiT

RG2.4 Provide adequate resources for IT risk management.

Identify resource requirements for IT risk management at both the business and IT levels and in the context of competing business risk issues, resource limitations and objectives. Allocate appropriate funds to fill gaps and position the enterprise to take advantage of opportunities. Make risk/reward trade-offs in relation to organisational objectives (e.g., allocate more or fewer resources based on criticality of data within a tiered approach to information security). Consider:

- People and skills (specify how the risk management skills of managers and staff will be developed and maintained)
- Documented processes and procedures for IT risk management
- Information systems and databases for managing IT risk issues
- Budget and other resources for specific risk response activities
- Expectations from regulators and external auditors

From	Inputs
RG1.3	IT risk tolerance thresholds
RG1.4	IT risk policy
RG2.1	Roles and responsibilities
RG2.2	IT risk management scope

To	Outputs
CobiT PO4, PO7; *	IT risk management resource requirements, roles and responsibilities, job descriptions, skills matrix, relationships

* Input from/output to outside Risk IT, Val IT and CobiT

RG2.5 Provide independent assurance over IT risk management.
Monitor IT risk action plans and obtain assurance on the performance of key IT risk management practices and whether IT risk is being managed in line with risk appetite and tolerance.

From	Inputs
RG1.3	IT risk tolerance thresholds
RG1.4	IT risk policy
RG2.1, RG2.2, RG2.3, RR2.3, RR3.4	IT risk action plans
RG2.1	Performance targets, incentives and rewards, integrated roles and responsibilities for risk management and oversight
RG2.2	IT risk management scope
RG3.4	Documented acceptance of risk
RR1.2	State of compliance reports, inputs to integrated enterprise risk reporting
RR2.1	Risk and control baseline
RR2.5	IT risk action plan progress/deviations
RR3.4	Process improvements
COBIT ME4	Enterprise appetite for IT risk, enterprise strategic direction for IT

To	Outputs
*	Board reporting

* Input from/output to outside Risk IT, Val IT and COBIT

MANAGEMENT GUIDELINES—RG2

RACI Chart

Key Activities	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RG2.1 Establish and maintain accountability for IT risk management.	A	R	R	R	R	I	I	I	C	C	C
RG2.2 Co-ordinate IT risk strategy and business risk strategy.	A	R	C	R	C	C	R	C	C	C	I
RG2.3 Adapt IT risk practices to enterprise risk practices.			C	A/R	C	I	C	C	R	C	C
RG2.4 Provide adequate resources for IT risk management.	A	R	C	R		I	C	R	C	C	
RG2.5 Provide independent assurance over IT risk management.	A/R	C	C	C	C	C	C	C	C	C	C

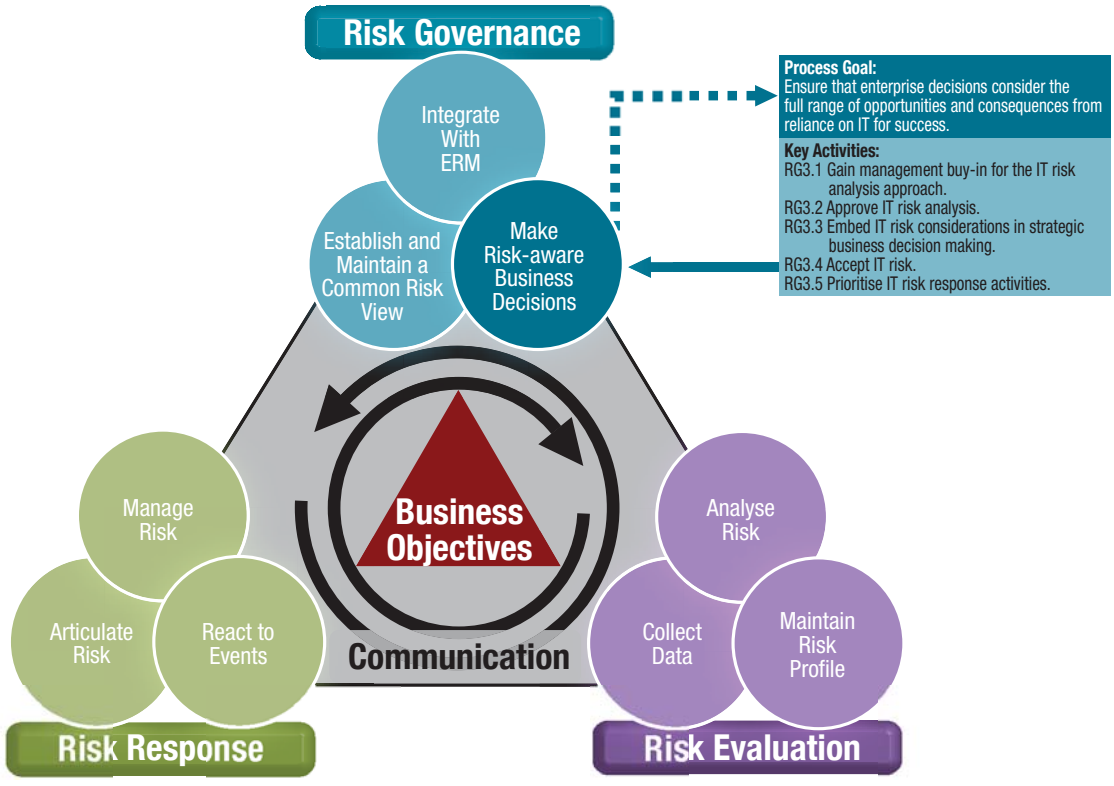
A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics—RG2

Activity Goals	Process Goal	RG Goal
• Establish and maintain accountability for IT risk management. • Co-ordinate IT risk strategy and business risk strategy. • Adapt IT risk practices to enterprise risk practices. • Provide adequate resources for IT risk management. • Provide independent assurance over IT risk management.	• Integrate the IT risk strategy and operations with the business strategic risk decisions that have been made at the enterprise level.	• Ensure that IT risk management practices are embedded in the enterprise, enabling the enterprise to secure optimal risk-adjusted return.
Activity Metrics	**Process Metrics**	**RG Metrics**
• Percentage of employees whose performance metrics and rewards reflect risk management objectives • An alignment score related to RACI regarding the ranking of actions to take (e.g., percentage of key IT risk-related accountabilities accepted by business and IT personnel) • Number of different risk reports provided to the board; extent of integration of reporting on IT risk • Degree of completeness of the integrated risk management strategy • Percentage of the integrated risk management strategy supported by defined methods applicable to IT risk • Percentage of IT risk management structures and activities set up vs. planned • Percentage of IT risk practices adapted to ERM organisational expectations • Percentage of IT risk management action plans approved for implementation • Percentage of core ERM activities with embedded IT risk considerations • Number of different issue management processes and platforms • Percentage of business lines with budgets allocated based on risk significance (e.g., per risk assessment results) • Number of open positions in the risk management staff	• Percentage of business executives and managers who have received training on the enterprise's reliance on and usage of IT, the related risk and the integrated risk strategy • Percentage of IT risk management operational expenditures that have direct traceability to business risk strategy • Percentage of business projects that consider IT risk • Percentage of core ERM activities that consider IT risk • Frequency of IT risk as an agenda item for the executive committee • Extent of alignment of common objectives across ERM and IT risk management • Percentage of controls that are tested multiple times (e.g., by business units then risk and control functions then internal audit) • Number of separate risk assessments within an entity that cannot aggregate results	• The degree to which the strategic use of IT in leveraging enterprise resources reduces overall enterprise risk • Percentage of risk management positions filled by staff trained in critical risk management techniques (e.g., standard risk analysis techniques, crisis management, project management, skills of people [audit, etc.] to detect when something IT-related is amiss)

PROCESS OVERVIEW

Figure 27—Process RG3 Make Risk-aware Business Decisions



PROCESS DETAIL

RG3 Make risk-aware business decisions.

Ensure that enterprise decisions consider the full range of opportunities and consequences from reliance on IT for success.

RG3.1 Gain management buy-in for the IT risk analysis approach.

Coach management decision makers on the proposed IT risk analysis approach. Illustrate how risk analysis results can benefit major decisions. Describe what level of quality decision makers should expect, how to interpret risk analysis reports, definitions of key terms (e.g., risk probabilities, degree of error, risk factors), and the limitations of measurements and estimates based on incomplete data. Identify gaps with enterprise risk expectations.

From	Inputs
RG1.4	IT risk policy
RG2.3	Integrated risk management methods

To	Outputs
RG2.3	IT risk analysis approach issues

RG3.2 Approve IT risk analysis.

Determine whether the risk analysis report provides sufficient information to understand the risk issues and, if needed, to evaluate risk response options. Note its limitations for the decision(s) at hand. Approve or reject the risk analysis report.

From	Inputs
RR1.1	Risk analysis report

To	Outputs
RG3.3, RG3.4, RG3.5	Approved risk analysis report, risk analysis limitations
RR1.1	Risk analysis deficiencies

RG3.3 Embed IT risk considerations in strategic business decision making.

Be proactive in looking at IT risk factors in advance of pending business decisions and then bring useful information to the table where the decisions are being made. Examples of useful information include the risk and performance levels within the portfolio of IT applications as compared to the value of the business processes they enable, or opportunities to rebalance the enterprise portfolio based on risk, return and anticipated changes to the IT environment. Help business management consider the effect that IT risk and existing risk management capacity (controls, capabilities, resources) will have on business decisions and the effect business decisions may have on existing IT risk exposure and IT risk management capacity going forward. Help business management understand IT risk based on various portfolio views (e.g., business unit, product, process) and weigh the impact that proposed IT investments will have on the overall risk profile of the enterprise (increase or reduce risk). Stress that as a condition of approval of business decisions, cost and opportunity must be weighed against an estimated net change of the IT risk exposure.

From	Inputs
RG1.1	Key services and supporting business processes and systems, high-level risk scenarios
RG1.3	IT risk tolerance thresholds
RG2.1, RG2.2, RG2.3, RR2.3, RR3.4	IT risk action plans
RG3.2	Approved risk analysis report, risk analysis limitations
RE3.3	IT capability assessment
RE3.5	IT risk profile
RR1.1	Loss/gain probabilities and ranges, risk response options, cost/benefit expectations
RR1.1, RR1.4, RR2.2	IT risk issues and opportunities
RR1.3	Independent IT assessment findings in context
CobiT PO1	Strategic IT plan, tactical IT plans, IT project portfolio, IT service portfolio, IT sourcing strategy, IT acquisition strategy
*	Pending business decisions

To	Outputs
RE2.1	Risk analysis request
RE3.5	IT risk profile changes
RR2.3, Val IT IM5	Full economic life cycle cost and benefits
Val IT VG1	Risk elements to be included in the value management process
Val IT IM1	IT risk-related opportunities

* Input from/output to outside Risk IT, Val IT and CobiT

RG3.4 Accept IT risk.

Using the established IT risk tolerance thresholds as a guide, decide whether to accept the remaining risk exposure level. Consider relevant information from risk analysis reports such as loss probabilities and ranges, risk response options, cost/benefit expectations, and the potential effects of risk aggregation. Discuss with impacted business process owners and together examine the risk-return ratios, and determine where to spend the risk budget on 'known' risks to allow acceptance of the unknown risk. Obtain business agreement on risk acceptance or, if no acceptance, the appropriate risk response requirements. Document how risk was considered in the decision and the rationale for any exceptions to risk tolerance (e.g., significant strategic business opportunity). Ensure that risk acceptance decisions and risk response requirements are communicated across organisational lines in accordance with established enterprise risk and corporate governance policies and procedures.

From	Inputs
RG1.3	IT risk tolerance thresholds
RG2.2	Integrated risk management strategy
RG3.2	Approved risk analysis report, risk analysis limitations
RE3.5	IT risk profile
RR1.1	Loss/gain probabilities and ranges, risk response options, cost/benefit expectations
RR1.1, RR1.4, RR2.2	IT risk issues and opportunities
RR1.2, RR2.2	Control gaps and policy exceptions
RR1.3	Independent IT assessment findings in context, vulnerability events
RR2.2	Risk aggregation data

To	Outputs
RG2.1, RE2.3, RR2.1, RR2.3, RR2.4	Risk response requirements
RG2.5, RE3.5, RE3.6	Documented acceptance of risk
RE2.1	Risk analysis request
RE3.5	IT risk profile changes

RG3.5 Prioritise IT risk response activities.

Examine the portfolio of risk response activities to identify those with a greater probable impact on overall risk reduction. Quantify the overall expected effect on the probable frequency and magnitude of related risk scenarios through the planned application of controls, capability and resources. Based on dimensions such as current risk level and effectiveness/cost ratio, classify and balance responses (e.g., quick wins, opportunities, deferred efforts) with those that may need a business case. Emphasise specific projects with relatively greater odds to:

- Reduce risk concentrations (e.g., improvements to architecture, separation of operational units and systems)
- Implement controls that directly address multiple risk types and are cost effective
- Implement controls that improve process effectiveness and prevent excessive risk taking

Record the rationale, constraints and how the decision is driving changes to published policy, operational controls, capabilities, resource deployments and communication plans. When applicable, record the rationale for exceeding or falling below risk appetite and tolerance.

From	Inputs
RG1.3	IT risk tolerance thresholds
RG3.2	Approved risk analysis report, risk analysis limitations
RE3.5	IT risk profile
RR1.1	Loss/gain probabilities and ranges, risk response options, cost/benefit expectations
RR1.1, RR1.4, RR2.2	IT risk issues and opportunities
RR1.3	Independent IT assessment findings in context, vulnerability events
Val IT VG3	Investment evaluation criteria
Val IT IM2	Complete understanding of candidate programmes including alternative courses of action
CobiT PO5	IT budgets
*	Operating budget

* Input from/output to outside Risk IT, Val IT and CobiT

To	Outputs
RE2.1	Risk analysis request
RE3.5	IT risk profile changes
RE3.5, RR2.3	Risk response priority (risk disposition)
RR2.3; Val IT PM4 (if a full business case is already made), IM1 (if a business case still needs to be made)	Risk management benefits assigned to IT portfolio

MANAGEMENT GUIDELINES—RG3

RACI Chart

Roles

Key Activities	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RG3.1 Gain management buy-in for the IT risk analysis approach.		C	A/R	R	C	C	C	C	R	C	C
RG3.2 Approve IT risk analysis.		I	R	C	C	A	I	R	I	I	I
RG3.3 Embed IT risk considerations in strategic business decision making.	I	C	C	A/R	C	C	C	C	R	C	I
RG3.4 Accept IT risk.	I	I	C	R	C	R	A	R	C		I
RG3.5 Prioritise IT risk response activities.		I	A	R	I	C	C	R	R		I

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

Goals and Metrics

Activity Goals	Process Goal	RG Goal
• Gain management buy-in for the IT risk analysis approach. • Approve IT risk analysis. • Embed IT risk considerations in strategic business decision making. • Accept IT risk. • Prioritise IT risk response activities.	• Ensure that enterprise decisions consider the full range of opportunities and consequences from reliance on IT for success.	• Ensure that IT risk management practices are embedded in the enterprise, enabling the enterprise to secure optimal risk-adjusted return.
Activity Metrics	**Process Metrics**	**RG Metrics**
• Percentage of business decisions that should have considered IT risk but did not • Number and size of adverse events/losses arising out of risk acceptance decision, including opportunity losses • Percentage of IT risk acceptance decisions with a complete set of supporting documentation • Number of prioritised risk response activities • Percentage of IT risk issues for which the expected reduction in frequency and magnitude is tracked	• Value of failed projects due to issues not identified during the decision-making process (e.g., Was the risk presented on the risk log? Was it estimated properly? Was there follow-through on it?) • Number of key management decisions made without the availability of a relevant risk analysis report • Percentage of decisions (or indecision) leading to IT-related loss that are revisited for lessons learned • Cycle time from the discovery of a control deficiency (e.g., vulnerability event) to a risk acceptance decision • Cycle time from reported policy exceptions to a decision on their disposition	• The degree to which the strategic use of IT in leveraging enterprise resources reduces overall enterprise risk • Percentage of risk management positions filled by staff trained in critical risk management techniques (e.g., standard risk analysis techniques, crisis management, project management, skills of people [audit, etc.] to detect when something IT-related is amiss)

DOMAIN MATURITY MODEL (RG)
HIGH LEVEL

0 Non-existent when
The enterprise does not recognise the need to consider the business impact from IT risk. Decisions involving IT risk taking lack credible information. There is no awareness of external requirements for IT risk management and integration with enterprise risk management.

1 Initial when
There is an emerging understanding that IT risk is important and needs to be managed, but it is viewed as a technical issue and the business primarily considers the downside of IT risk. Any IT risk identification criteria vary widely across the enterprise and the IT organisation. By default, IT is accountable for problem management, availability, system access, etc. Risk appetite and tolerance are applied only during episodic risk assessments. Enterprise risk policies and standards, which are minimal at best, may be incomplete and/or reflect only external requirements and lack defensible rationale and enforcement mechanisms. IT risk management skills may exist on an *ad hoc* basis, but they are not actively developed. *Ad hoc* inventories of controls, which are unrelated to risk, are dispersed across desktop applications.

2 Repeatable when
There is an awareness of the need to actively manage IT risk, but the focus is on technical compliance with no anticipation of value added. There are emerging leaders for IT risk management within silos who assume responsibility and are usually held accountable, even if this is not formally agreed. Risk tolerance is set locally and may be difficult to aggregate. Investments are focused on specific risk issues within functional and business silos (e.g., security, business continuity, operations). There is board-issued guidance for risk management. Minimum skill requirements, which include an awareness of IT risk, are identified for critical enterprise risk areas. Functional and IT silo-specific inventories of risk issues exist.

3 Defined when
IT risk management is viewed as a business issue, and both the downside and upside of IT risk are recognised. There is a designated leader for IT risk across the enterprise; this leader is engaged with the enterprise risk committee, where IT risk is in scope and discussed. The business understands how IT fits in the enterprise risk universe and the risk portfolio view. Enterprise risk tolerance is derived from local tolerances and IT risk management activities are being aligned across the enterprise. Formal risk categories have been identified and described in clear terms. Risk awareness training includes situations and scenarios beyond specific policy and structures and promotes a common language for communicating risk. Defined requirements exist for a centralised inventory of risk issues. Workflow tools are used to escalate risk issues and track decisions.

4 Managed when
IT risk management is viewed as a business enabler, and both the downside and upside of IT risk are understood. The designated leader for IT risk across the enterprise is fully engaged with the enterprise risk committee, which expects value from including IT in decisions. The IT department's role in operational risk management and the broader ERM is well understood. The board defines risk appetite and tolerance across the risk universe, including IT risk. Enterprise policies and standards reflect business risk tolerance. Far-sighted risk scenarios consider IT risk across the enterprise. Major business decisions fully consider the probability of loss and the probability of reward. Skill requirements are routinely updated for all areas, proficiency is ensured for all risk management areas and certification is encouraged. Tools enable enterprise risk portfolio management, automation of IT risk management workflows, and monitoring of critical activities and controls.

5 Optimised when
Senior executives make a point of considering all aspects of IT risk in their decisions. The IT risk leader is considered a trusted advisor during design, implementation and steady-state operations. The IT department is a major player in business-line operational risk efforts and enterprise risk efforts. Strategic objectives are based on an executive-level understanding of IT-related business threats, risk scenarios and competitive opportunities. Enterprise policies and standards continue to reflect business risk tolerance while increasing efficiency. The enterprise formally requires continuous improvement of IT risk management skills, based on clearly defined personal and enterprise goals. Real-time monitoring of risk events/incidents and control exceptions exists, as does automation of policy management.

Figure 28—RG Detailed Maturity Model Par			
	Awareness and Communication	**Responsibility and Accountability**	**Goal Setting and Measurement**
0	The enterprise does not recognise the need to consider the business impact from IT risk. Decisions involving IT risk taking lack credible information. There is no awareness of external requirements for IT risk management and integration with ERM.		
1	There is an emerging understanding that IT risk is important and needs to be managed, but it is viewed as a technical issue and the business primarily considers the downside of IT risk. Any IT risk identification criteria vary widely across the enterprise and the IT organisation. IT risk issues are primarily communicated by assurance groups (e.g., internal audit). Minimal structure and basis for discussion of IT risk concepts exist. Senior managers and IT executives struggle with IT risk language.	By default, IT is accountable for problem management, availability, system access, etc. Ownership of IT risk in the context of business services and processes is not defined. There is no consideration of business accountability and responsibility for proactive IT risk management. No linkage to an individual performance measurement and reward programme exists. There is no business expectation of value from including the IT executive view of risk during decision making.	Risk appetite and tolerance are applied only during episodic risk assessments. Investments are focused on externally imposed requirements and expectations. Reporting is compliance-driven and focused on remediation of issues identified by assurance groups and external parties.
2	There is an awareness of the need to actively manage IT risk, but the focus is on technical compliance with no anticipation of value added. Some localised IT understanding of risk/reward exists. Senior managers and IT executives are developing a common language for IT risk, but IT risk discussions across silos may be impaired by competing business unit- and function-specific risk language.	There are emerging leaders for IT risk management within silos who assume responsibility and are usually held accountable, even if this is not formally agreed. The enterprise risk committee charter covers IT risk, but IT has minimal representation. Performance targets are tied to meeting external reporting requirements and minimising negative findings. Roles are only partially defined and contain overlaps (e.g., risk evaluation overlaps with risk response, IT implementers are empowered to both prescribe local IT solutions and express opinions). There is confusion about responsibility for integrating IT risk management with operations and ERM. When problems occur, a culture of blame tends to exist.	Risk tolerance is set locally and may be difficult to aggregate. Investments are focused on specific risk issues within functional and business silos (e.g., security, business continuity, operations). Regular manual reporting of IT risk management activities is directed to local IT management.
3	IT people generally understand how IT-related failures or events impact enterprise objectives and cause direct or indirect loss to the enterprise, while business people generally understand how IT-related failures or events can affect key services and processes. IT risk management is viewed as a business issue, and both the downside and upside of IT risk are recognised. IT risk strategies and plans are communicated by management. IT risk discussions are based on a defined language/taxonomy. Enterprise-level information on risk and opportunity is shared.	There is a designated leader for IT risk across the enterprise who is engaged with the enterprise risk committee, where IT risk is in scope and discussed. The business understands how IT fits in the enterprise risk universe and the risk portfolio view. The IT risk leader has a strong relationship with the CFO and is regularly consulted during portfolio management and budgeting activities. The IT risk leader has sufficient stature to effectively challenge business decisions involving IT risk. IT risk roles are clearly defined and contain minimal overlap. Process responsibility and accountability are defined and process owners have been identified. Performance measures are tied to providing business value in addition to meeting external requirements.	Enterprise risk tolerance is derived from local tolerances, and IT risk management activities are being aligned across the enterprise. Investments are being made against common risk issues, although they may not address the root cause in all cases. Risk appetite and tolerance are applied during system design, implementation, steady state and major organisational changes. Regular reporting of IT risk management process outcomes is directed to IT management.

Figure 28—RG Detailed Maturity Model Part 1 *(cont.)*

	Awareness and Communication	Responsibility and Accountability	Goal Setting and Measurement
4	Risk culture is analysed and reported. The business understands IT risk/reward. IT risk management is viewed as a business enabler, and both the downside and upside of IT risk are understood. The IT risk language spoken by senior executives is blending and aligning with corporate risk language. IT risk discussions are a normal part of executive decision making.	The designated leader for IT risk across the enterprise is fully engaged with the enterprise risk committee, which expects value from including IT in decisions. The IT department's role in operational risk management and the broader ERM is well understood. Integrated risk management is embedded in strategic planning and business operations. All IT risk domains have a nominated owner, and responsibility and accountability are accepted. Senior business management and IT management together determine the acceptable level of risk that the enterprise will tolerate. A reward culture that motivates positive action is in place.	The board defines risk appetite and tolerance across the risk universe, including IT risk. Risk tolerance may be refined by the enterprise risk committee or an IT risk council. Risk portfolio views are dynamic, and risk tolerance is evaluated based on different views. Better investment decisions result from enterprise visibility into costs, IT risk issues and benefits/rewards. Opportunities associated with risk are part of the risk plan's expected outcomes. Investments are balanced against a portfolio view of risk and address the root cause. Regular reporting of business outcomes related to IT risk management is made to business management.
5	Senior executives make a point of considering all aspects of IT risk in their decisions. The enterprise views integrated risk management as a source of business value.	The IT risk leader is considered a trusted advisor during design, implementation and steady-state operations. Executive sponsorship is strong, and the tone from the top has embedded integrated risk management into the enterprise culture. Roles and responsibilities are process-driven, with cross-functional teams collaborating. Accountability for risk management to help achieve objectives is embedded in all processes, support functions, business lines and geographic locations. The IT department is a major player in business-line operational risk efforts and enterprise risk efforts.	Strategic objectives are based on an executive-level understanding of IT-related business threats, risk scenarios and competitive opportunities. The enterprise employs robust business analytics to measure the effectiveness of managing uncertainties and seizing risky opportunities.

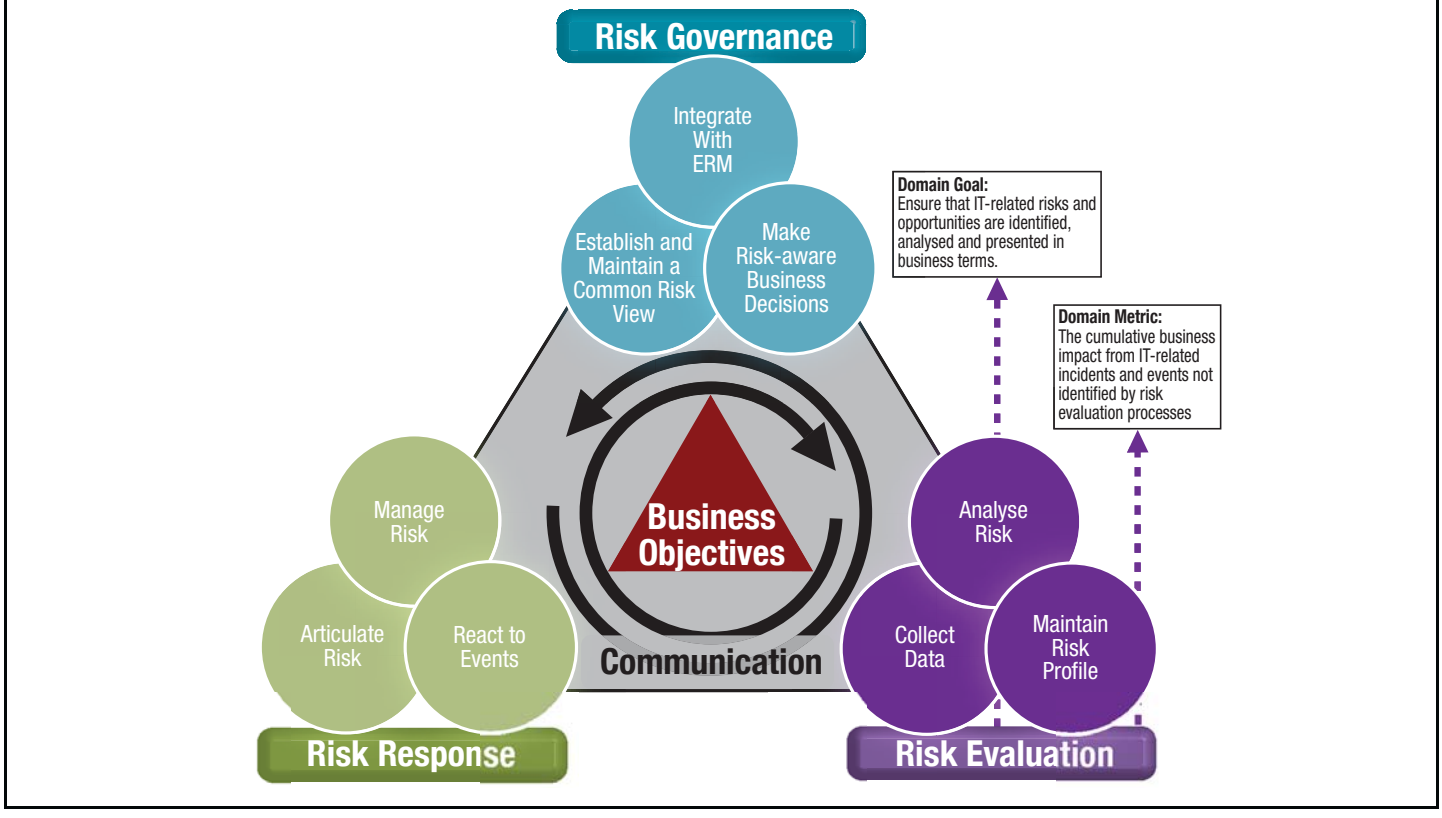
Figure 29—RG Detailed Maturity Model Part 2 *(c*

	Policies, Standards and Procedures	Skills and Expertise	Tools and Automation
0			
1	Enterprise policies and standards, which are minimal at best, may be incomplete and/or reflect only external requirements and lack defensible rationale and enforcement mechanisms. Minimal procedures for IT risk management exist. Policies and standards are not kept up to date relative to evolving business, technology or threat landscapes.	IT risk management skills may exist on an *ad hoc* basis, but they are not actively developed. Enterprise risk managers and business process owners lack IT risk understanding. IT personnel lack an understanding of the business impact of IT risk.	*Ad hoc* inventories of controls that are unrelated to risk are dispersed across desktop applications. Policies and standards exist in multiple formats. There is no workflow around incidents and risk decisions.
2	There is board-issued guidance for risk management. Policies and standards are established for functional and business silos and may not align with the board guidance and overall business risk appetite.	Minimum skill requirements, which include an awareness of IT risk, are identified for critical enterprise risk areas. Risk awareness training focuses on policy and some risk language. IT risk management training is provided in response to needs, rather than on the basis of an agreed-upon plan, and informal training on the job occurs.	Functional and IT silo-specific inventories of risk issues exist. Key elements of risk decisions are recorded in desktop applications. Some desktop-based risk management tools may exist, but a co-ordinated approach and expected benefits from tools are lacking.

Figure 29—RG Detailed Maturity Model Part 2 *(cont.)*			
	Policies, Standards and Procedures	**Skills and Expertise**	**Tools and Automation**
3	Formal risk categories have been identified and described in clear terms. Enterprise policies and standards reflect overall business risk appetite. Established risk policy is based on board guidance. Important issues are directed to senior management. The process, policies and procedures are defined and documented for all key IT risk management activities. Exceptions are resolved in a formal manner.	Skill requirements are defined and documented for all enterprise risk areas and include IT risk concepts. Risk awareness training includes situations and scenarios beyond specific policy and structures and promotes a common language for communicating risk. Enterprise risk managers and business process owners receive targeted IT training, e.g., IT for finance executives. IT personnel receive training on business activities, products, general business risk, competing risk issues and business dependency on IT. A formal training plan has been developed.	Requirements are defined for a centralised inventory of risk issues. Workflow tools are used to escalate risk issues and track decisions. Data collection tools can distinguish amongst multiple event types.
4	Enterprise policies and standards reflect business risk tolerance. Far-sighted risk scenarios consider IT risk across the enterprise. Major business decisions fully consider the probability of loss and the probability of reward. Standards for developing and maintaining the integrated risk management processes and procedures are adopted and followed.	Skill requirements are routinely updated for all areas, proficiency is ensured for all risk management areas and certification is encouraged. Risk awareness training is comprehensive and includes role playing and cascading and coincidental threat types and scenarios. Mature training techniques are applied according to the training plan and knowledge sharing is encouraged. All internal IT risk management experts are involved, and the effectiveness of the training plan is evaluated.	Tools enable enterprise risk portfolio management, automation of IT risk management workflows and monitoring of critical activities and controls. Standard tools are deployed that integrate IT risk management with ERM.
5	Enterprise policies and standards continue to reflect business risk tolerance while increasing efficiency (e.g., they are dynamically updated, they contain details for high-risk situations and flexibility for lower-risk situations). IT risk management is fully integrated into ERM processes and structures, business activities, business lines, products, and initiatives (e.g., new partnerships, service providers, mergers, acquisitions). All risk decisions are consistently based on probabilities of loss and reward. IT, internal audit, compliance, control and risk management are highly integrated and co-ordinate and report risk issues.	The enterprise formally requires continuous improvement of IT risk management skills, based on clearly defined personal and enterprise goals. Training and education for IT risk management support external best practices and use of leading-edge concepts and techniques. Knowledge sharing is an enterprise culture and knowledge-based systems are being deployed. External experts and industry leaders are used for guidance.	Real-time monitoring of risk events/incidents and control exceptions occurs. Policy management is automated. Automated tools enable end-to-end support of the risk management processes. Tools are being used to support improvement of the risk management process.

DOMAIN OVERVIEW

Figure 30—Risk Evaluation Domain



PROCESS OVERVIEW

Figure 31—Process RE1 Collect Data

PROCESS DETAIL

RE1 Collect data.

Identify relevant data to enable effective IT-related risk identification, analysis and reporting.

RE1.1 Establish and maintain a model for data collection.

Establish and maintain a model for the collection, classification and analysis of IT risk data. Accommodate multiple types of events (e.g., threat event, vulnerability event, loss event) and multiple categories of IT risk (e.g., IT benefit/value enablement, IT programme and project delivery, IT operations and service delivery). Include filters and views to help determine how specific risk factors may affect risk (e.g., frequency, magnitude, business impact). The model should support the measurement and assessment of risk attributes (e.g., availability) across IT risk domains and provide useful data for setting incentives for a risk-aware culture.

From	Inputs
RG2.2	Integrated risk management strategy
*	Technical and operational risk policies, loss reporting and escalation policies, enterprise obligations around loss and event reporting

To	Outputs
RE1.2, RE1.3, Val IT VG5	Model for data collection

* Input from/output to outside Risk IT, Val IT and CobiT

RE1.2 Collect data on the operating environment.

Per the data collection model, record data on the enterprise's operating environment that could play a significant role in the management of IT risk. Consult sources within the business, legal department, audit, compliance and office of the CIO. Cover major revenue streams, external IT systems, product liability, the regulatory landscape, competition within the industry, IT trends, competitor alignment with key benchmarks, relative maturity in key business and IT capabilities, and geopolitical issues. Survey and organise the historical IT risk data and loss experience of industry peers through industry-based event logs, databases and industry agreements for common event disclosure (e.g., banking industry agreements regarding disclosure of widespread fraud events).

From	Inputs
RG1.5	Performance metrics on cultural shift towards risk awareness
RE1.1	Model for data collection
RE3.3	IT capability assessment
CobiT DS10	Problem records, known problems, known errors and workarounds
CobiT ME1	Historical risk trends and events
*	Business capability assessment, business intelligence, external entity risk event and loss data, legal and regulatory mappings

To	Outputs
RE1.4, RE2.2, RE3.4, RE3.5, RE3.6, RR3.1, RR3.4	Operating environment data, historical IT risk and loss data

* Input from/output to outside Risk IT, Val IT and CobiT

RE1.3 Collect data on risk events.

Per the data collection model, record data on risk events that have caused or may cause impacts to IT benefit/value enablement, IT programme and project delivery, and/or IT operations and service delivery. Capture relevant data from related issues, incidents, problems and investigations.

From	Inputs
RE1.1	Model for data collection
RR3.3	Incident response actions taken
RR3.4	Root cause of incidents
CobiT PO10	Project performance reports
CobiT DS2	Process performance reports, supplier risks
CobiT DS4	Contingency test results, process performance reports
CobiT DS5	Security threats and vulnerabilities
CobiT DS8	Incident reports
CobiT DS9	Process performance reports
CobiT DS10	Problem records, known problems, known errors and workarounds
CobiT ME1	Historical risk trends and events

To	Outputs
RE1.4, RE2.2, RE3.4, RE3.5, RE3.6, RR3.1, RR3.4; Val IT IM6, IM9	Real-time problem and loss data, root-cause analysis and loss trends

RE1.4 Identify risk factors.

For business-relevant analogous events, organise the collected data and highlight contributing factors (e.g., drivers of the frequency and magnitude of risk events). Determine what specific conditions existed or did not exist when risk events were experienced and how the conditions may have affected event frequency and magnitude of loss. Determine common contributing factors across multiple events. Perform periodic event and risk-factor analysis to identify new or emerging risk issues and to gain an understanding of the associated internal and external risk factors.

From	Inputs
RE1.2	Operating environment data, historical IT risk and loss data
RE1.3	Real-time problem and loss data, root-cause analysis and loss trends

To	Outputs
RG1.1, RG1.4, RE2.1, RE2.2, RE3.4, RE3.5, RE3.6, RR3.4	Risk factors
RG1.4, RE2.1, RE2.2, RE3.4, RE3.5, RE3.6, RR1.4, RR3.1, RR3.4	Emerging threats

MANAGEMENT GUIDELINES—RE1

RACI Chart **Roles**

Key Activities	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RE1.1 Establish and maintain a model for data collection.	I	I	A/R	C	C	C	C	C	C		C
RE1.2 Collect data on the operating environment.		I	A/R	C	I	I	C	I	I	I	C
RE1.3 Collect data on risk events.		I	A	R	C	I		C	C		I
RE1.4 Identify risk factors.			A	R	I	I	C	C	R	C	C

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

Goals and Metrics—RE1

Activity Goals	Process Goal	RE Goal
• Establish and maintain a model for data collection. • Collect data on the operating environment. • Collect data on risk events. • Identify risk factors.	• Identify relevant data to enable effective IT-related risk identification, analysis and reporting.	• Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.
Activity Metrics	**Process Metrics**	**RE Metric**
• Existence of a defined and documented risk-related data collection model • Number of sources used for data collection • Completeness of risk event data against established standards (e.g., affected assets, impact data, threat community, actions). This includes both discrete event data (e.g., control 'yes' or 'no') and continuous data (e.g., ongoing stream data on server response time). • Number of data items for which the contributing factors have been identified • Completeness of historical data across the top categories and domains of IT risk	• Number of loss events with key characteristics not captured in some form of repository • Degree to which collected data support reporting of trends and scenario analysis • The degree of visibility and recognition into the control state provided by data collection • The degree of visibility and recognition into the threat landscape provided by data collection	• The cumulative business impact from IT-related incidents and events not identified by risk evaluation processes

PROCESS OVERVIEW

Figure 32—Process RE2 Analyse Risk

PROCESS DETAIL

RE2 Analyse risk.

Develop useful information to support risk decisions that take into account the business relevance of risk factors.

RE2.1 Define IT risk analysis scope.

Decide on the expected breadth and depth of risk analysis efforts. Consider a wide range of scope options, to include:
- Requirements of strategic decision makers (e.g., new products and services, new operating environments, outsourcing, new compliance requirements)
- Enterprise IT risk assessment results
- Response to indicators, triggers or events (e.g., new or emerging threat populations)
- Areas of residual risk outside of tolerance thresholds
- Management's need for further examination of ongoing operations (e.g., line of business, product, service and process—individually or in combinations)

Map in relevant risk factors and the business criticality of in-scope assets/resources and triggers. Aim for optimal value from risk analysis efforts by favouring scope based on productive processes and products of the business (e.g., revenue generation, customer service, quality) over internal structures not directly related to business outcomes (e.g., types of hardware, physical locations, functional organisations). Set the risk analysis scope after a consideration of business criticality, the cost of measurement vs. the expected value of information and reduction in uncertainty, and any overarching regulatory requirements.

From	Inputs
RG1.1	Key business and IT objectives, major risk factors, risk focus areas, high-level risk scenarios, key services and supporting business processes and systems, prioritised inventories of risk and impact categories
RG1.1, RG3.3, RG3.4, RG3.5, RR1.3, RR1.4, RR2.2, RR3.1, RR3.4; *	Risk analysis request
RG2.2	Integrated risk management strategy
RG2.3	Integrated risk management methods
RE1.4	Risk factors, emerging threats
RE3.2	Asset/resource criticality
RE3.5	IT risk profile
RR1.1, RR1.4, RR2.2	IT risk issues and opportunities
CobiT ME3	Catalogue of legal and regulatory requirements related to IT service delivery, report on compliance of IT activities with external legal and regulatory requirements

* Input from/output to outside Risk IT, Val IT and CobiT

To	Outputs
RE2.2, RE2.3, RE2.4	Risk analysis scope

RE2.2 Estimate IT risk.

Across the scope of the IT risk analysis, estimate the probable frequency and probable magnitude of loss or gain associated with IT risk scenarios as influenced by applicable risk factors. Estimate the maximum amount of damage that could be suffered (e.g., a worst-case loss when specific risk factors converge) or opportunity that could be gained. Consider compound scenarios of cascading and/or coincidental threat types (e.g., an external threat plus an internal accident). Based on the most important scenarios, develop expectations for specific controls, capability to detect and other response measures. Evaluate known operational controls and their effect on probable frequency, and probable magnitude and applicable risk factors. Estimate residual risk exposure levels and compare to acceptable risk tolerance to identify exposures that may require a risk response.

From	Inputs
RG1.3	IT risk tolerance thresholds
RG2.3	Integrated risk management methods
RE1.2	Operating environment data, historical IT risk and loss data
RE1.3	Real-time problem and loss data, root-cause analysis and loss trends
RE1.4	Risk factors, emerging threats
RE2.1	Risk analysis scope
RE3.2	Asset/resource criticality
RE3.3	IT capability assessment
RE3.4	IT risk scenario components
RE3.5	IT risk profile
RR1.3	Independent IT assessment findings in context, vulnerability events
RR2.1	Risk and control baseline
CobiT PO6	Enterprise IT control framework
CobiT ME2	Report on effectiveness of IT controls

To	Outputs
RE2.3	Scenario analysis results

RE2.3 Identify risk response options.

Examine the range of risk response options, such as avoid, reduce/mitigate, transfer/share, accept and exploit/seize. Document the rationale and potential trade-offs across the range. Specify high-level requirements for projects or programmes that, based on risk tolerance, will mitigate risk to acceptable levels; identify costs, benefits and responsibility for project execution. Develop requirements and expectations for material controls at the most appropriate points, or where they are expected to be rolled up to give meaningful visibility.

From	Inputs
RG1.3	IT risk tolerance thresholds
RG3.4, RR3.4	Risk response requirements
RE2.1	Risk analysis scope
RE2.2	Scenario analysis results
RE3.5	IT risk profile
RR1.1, RR1.4, RR2.2	IT risk issues and opportunities
RR1.2, RR2.2	Control gaps and policy exceptions
RR2.1	Risk and control baseline
Val IT PM4	Approved investment programmes
CobiT PO5	IT budgets
CobiT PO10	Project management guidelines
CobiT ME2	Report on effectiveness of IT controls
*	Operating budget

* Input from/output to outside Risk IT, Val IT and CobiT

To	Outputs
RE2.4, RR1.1	Risk analysis results

RE2.4 Perform a peer review of IT risk analysis.

Perform a peer review of the risk analysis results before sending them to management for approval and use in decision making. Confirm that the analysis is documented in line with enterprise requirements. Review the basis for the estimates of loss/gain probabilities and ranges. Verify that any human estimators were properly calibrated beforehand and look for evidence of 'gaming the system', i.e., a conscious or otherwise suspect choice of inputs that may result in a desired or expected outcome. Verify that the experience level and credentials of the analyst were appropriate for the scope and complexity of the review. Finally, provide an opinion on whether the expected reduction in uncertainty was achieved and whether the value of information gained exceeded the cost of measurement.

From	Inputs
RE2.1	Risk analysis scope
RE2.3	Risk analysis results

To	Outputs
RR1.1	Peer-review recommendations

MANAGEMENT GUIDELINES—RE2

RACI Chart

Roles

Key Activities	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RE2.1 Define IT risk analysis scope.		I	R	C	I	C	A	R	C		C
RE2.2 Estimate IT risk.		I	R	C	C	I	A/R	R	R		C
RE2.3 Identify risk response options.			C	C	C	R	A	R	R		I
RE2.4 Perform a peer review of IT risk analysis.			A/R				I		I		I

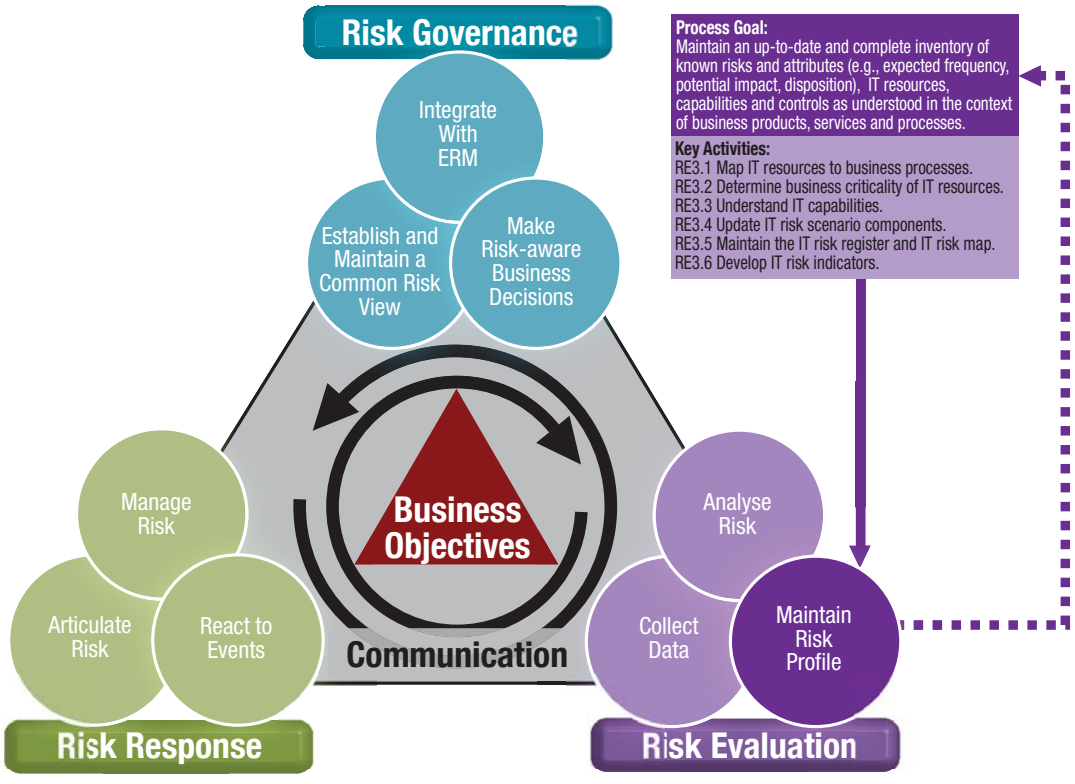
A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics

Activity Goals	Process Goal	Domain Goal
• Define IT risk analysis scope. • Estimate IT risk. • Identify risk response options. • Perform a peer review of IT risk analysis.	• Develop useful information to support risk decisions that take into account the business relevance of risk factors.	• Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.
Activity Metrics	**Process Metrics**	**Domain Metrics**
• Percentage of time analyses are substantiated by later experience or testing (accuracy) • Percentage of time that peer review finds no significant logical, calculation or incompleteness errors (defensibility) • Percentage of time that parallel assessments on the same scenarios performed by different analysts get the same results (consistency) • Percentage of time that analyses are performed by trained analysts (higher-level metric related to accuracy, defensibility and consistency) • A 'satisfaction index' derived over risk analysis reporting (e.g., the percentage of favourable satisfaction survey responses from business executives regarding the readability, usefulness and accuracy of risk analysis reports)	• Percentage of risks for which the probable frequency of occurrence and the probable magnitude of the business impact are measured within the scope • Percentage of critical assets, targets and resources reviewed for the effect of known operational controls • Percentage of risk analysis undergoing peer review before being sent to management • Ratio of cumulative actual losses to expected loss magnitude	• The cumulative business impact from IT-related incidents and events not identified by risk evaluation processes

PROCESS OVERVIEW

Figure 33—Process RE3 Maintain Risk Profile



PROCESS DETAIL

RE3 Maintain risk profile.

Maintain an up-to-date and complete inventory of known risks and attributes (e.g., expected frequency, potential impact, disposition), IT resources, capabilities and controls as understood in the context of business products, services and processes.

RE3.1 Map IT resources to business processes.

Inventory business processes, supporting people, applications, infrastructure, facilities, critical manual records, vendors, suppliers and outsourcers. Understand the dependency of key business activities on IT service management processes and IT infrastructure resources (e.g., applications, middleware, servers, storage, networking and physical facilities).

From	Inputs
RG1.1	Key services and supporting business processes and systems, high-level risk scenarios
RG2.1; CobiT PO7	Roles and responsibilities
RE3.3	IT capability assessment
CobiT DS9	IT configuration/asset details
*	Business continuity plan

To	Outputs
RE3.2	Asset/resource inventory
RE3.2, RE3.3, RE3.4; CobiT PO5, DS1	Service mapping

* Input from/output to outside Risk IT, Val IT and CobiT

RE3.2 Determine business criticality of IT resources.

Determine which IT services and IT infrastructure resources are required to sustain the operation of key services and critical business processes. Analyse dependencies and weak links across the 'full stack', i.e., from the top layer down to physical facilities. Gain the consensus of business and IT leadership on the enterprise's most valued information and related technology assets (e.g., those used to manage business operations, provide capabilities, generate capital, provide competitive advantage, protect the enterprise from personnel turnover, and manage the intentions and decisions of executive leadership).

From	Inputs
RG1.1	Asset/resource criticality (macro level)
RG1.1, RG2.2	Prioritised inventories of risk and impact categories
RG1.3	IT risk tolerance thresholds
RG2.3	Integrated risk management methods
RE3.1	Asset/resource inventory, service mapping
CobiT PO2	Information architecture, assigned data classifications, classification procedures and tools
CobiT DS1	Updated IT service portfolio
CobiT DS4	Criticality of IT configuration items, incident/ disaster thresholds, IT continuity plan
CobiT ME1	Historical risk trends and events
*	Criticality of business services and processes

To	Outputs
RE2.1, RE2.2, RE3.3, RE3.4, RR2.2, RR3.2; Val IT IM5; CobiT DS8, DS10, DS13	Asset/resource criticality

* Input from/output to outside Risk IT, Val IT and CobiT

RE3.3 Understand IT capabilities.

Inventory and evaluate IT process capability, skills and knowledge of people, and IT performance outcomes across the spectrum of IT risk (e.g., IT benefit/value enablement, IT programme and project delivery, IT operations and service delivery). Determine where normal process execution can or cannot provide the right controls and the ability to take on acceptable risk (e.g., not having sufficient IT project delivery capability in specific technical areas, but having strong IT programme management and outsourcing capabilities, therefore, will outsource in certain cases). Identify where reducing process outcome variability can contribute to a more robust internal control structure, improve IT and business performance, and exploit/seize opportunities.

From	Inputs
RE3.1	Service mapping
RE3.2	Asset/resource criticality
CobiT DS1	Service level agreements (SLAs), service level metrics
CobiT DS1, DS8	Process performance reports

To	Outputs
RG1.1, RG3.3, RE1.2, RE2.2, RE3.1, RE3.4, RE3.5, RR1.4, RR2.1	IT capability assessment

RE3.4 Update IT risk scenario components.

Review the collection of attributes and values across IT risk scenario components (e.g., actor, threat type, event, asset/resource, timing) and their inherent connections to business impact categories. Adjust entries based on changing risk conditions and emerging threats to IT benefit/value enablement, IT programme and project delivery, and IT operations and service delivery. Update distributions and ranges based on asset/resource criticality, data on the operating environment, risk event data (e.g., root-cause analysis and loss trends, real-time problem and loss data), historical IT risk data, and the potential effects of risk factors (e.g., how they may influence the frequency and/or magnitude of IT risk scenarios and their potential business impact). Link event types to risk categories and business impact categories. Aggregate event types by category, business line and functional area. At a minimum, update the IT risk scenario components in response to any significant internal or external change, and review them annually.

From	Inputs
RG1.1	Key services and supporting business processes and systems, high-level risk scenarios
RG1.1, RG2.2	Prioritised inventories of risk and impact categories
RE1.2	Operating environment data, historical IT risk and loss data
RE1.3	Real-time problem and loss data, root-cause analysis and loss trends, emerging threats
RE1.4	Risk factors, emerging threats
RE3.1	Service mapping
RE3.2	Asset/resource criticality
RE3.3	IT capability assessment
CobiT PO2	Information architecture, assigned data classifications, classification procedures and tools

To	Outputs
RG1.1, RG1.5, RE2.2, RE3.5	IT risk scenario components

RE3.5 Maintain the IT risk register and IT risk map.

Capture the risk profile within tools such as an IT risk register and IT risk map. Build out the risk profile via the results of enterprise IT risk assessment, risk scenario components, risk event data collection, ongoing risk analysis and independent IT assessment findings. For individual IT risk register entries, update key attributes such as name, description, owner, expected/actual frequency and potential/actual magnitude of associated scenarios, potential/actual business impact, and disposition (e.g., accepted, transferred, mitigated, avoided). For the IT risk map and its refinements update scores for each dimension (e.g., frequency, magnitude, business impact, cost to address in line with acceptable tolerance). At a minimum, update the IT risk map in response to any significant internal or external change, and review it annually.

From	Inputs
RG1.3	IT risk tolerance thresholds
RG3.3, RG3.4, RG3.5, RR1.1, RR1.3	IT risk profile changes
RG3.4	Documented acceptance of risk
RG3.5	Risk response priority (risk disposition)
RE1.2	Operating environment data, historical IT risk and loss data
RE1.3	Real-time problem and loss data, root-cause analysis and loss trends
RE1.4	Risk factors, emerging threats
RE3.3	IT capability assessment
RE3.4	IT risk scenario components
RR1.1	Risk analysis report
RR1.3	Independent IT assessment findings in context, vulnerability events
RR2.1	Risk and control baseline
RR2.5	IT risk action plan progress/deviations

To	Outputs
RG1.1, RG1.4, RG3.3, RG3.4, RG3.5, RE2.1, RE2.2, RE2.3, RE3.6, RR1.3 RR2.1, RR2.2; CobiT PO9	IT risk profile
RR2.1	Risk and control baseline updates

RE3.6 Develop IT risk indicators.

Design metrics or indicators that can point to IT-related events and incidents that can significantly impact the business. Base the indicators on a model of what compromises exposure and capability in risk management. These must reflect the actual risk; otherwise, a metric can be 'green' but the actual risk can still be serious. Emphasise observable metrics that will alert management when actual risk exposure exceeds acceptable thresholds across the operating environment. Provide management with an understanding of the useful and potentially key risk indicators—what they are; what they measure, from infrastructure through a strategic view; and what actions to take if they are triggered (e.g., update the risk profile, adjust risk response activities). Regularly review KRIs in use by management, and recommend adjustment for changing internal and external conditions.

From	Inputs
RG1.3	IT risk tolerance thresholds
RG3.4	Documented acceptance of risk
RE1.2	Operating environment data, historical IT risk and loss data
RE1.3	Real-time problem and loss data, root-cause analysis and loss trends
RE1.4	Risk factors, emerging threats
RE3.5	IT risk profile
RR2.2	Key IT risk indicators and escalation triggers
RR3.4	Root cause of incidents

To	Outputs
RR2.2	IT risk indicators, KRI recommendations

MANAGEMENT GUIDELINES—RE3

RACI Chart **Roles**

Key Activities	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RE3.1 Map IT resources to business processes.			I	R			C	A/R	C		I
RE3.2 Determine business criticality of IT resouces.		C		R		C	A	R			I
RE3.3 Understand IT capabilities.			C	A/R				C	C		I
RE3.4 Update IT risk scenario componenets.			C	R	I	C	C	A	R		C
RE3.5 Maintain the IT risk register and IT risk map.		I	A	R	I	I	I	R/C	C		I
RE3.6 Develop IT risk indicators.			A	C			C	C	R	C	C

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

Goals and Metrics

Activity Goals	Process Goal	RE Goal
• Map IT resources to business processes. • Determine business criticality of IT resources. • Understand IT capabilities. • Update IT risk scenario components. • Maintain the IT risk register and IT risk map. • Develop IT risk indicators.	• Maintain an up-to-date and complete inventory of known risks and attributes (e.g., expected frequency, potential impact, disposition), IT resources, capabilities and controls as understood in the context of business products, services and processes.	• Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.
Activity Metrics	**Process Metrics**	**RE Metric**
• Percentage of key business activities with a dependency linkage to supporting IT resources and IT infrastructure resources • Percentage of critical elements of the IT portfolio covered by risk triggers and thresholds • Frequency of updates to the IT risk scenario components • Number of significant internal or external change events not reviewed for impact on IT risk scenario components • Number of significant internal or external change events not reviewed for impact on the IT risk map • Number of realised events with business impact not detected by a trigger mechanism	• Number of approved risk analysis results not yet incorporated into the risk profile • Percentage of critical business services not covered by risk analysis • Completeness of attributes and values across IT risk scenario components • Completeness of key risk data attributes across the IT risk register	• The cumulative business impact from IT-related incidents and events not identified by risk evaluation processes

DOMAIN MATURITY MODEL (RE)
HIGH LEVEL

0 Non-existent when
The enterprise does not recognise the need to understand how IT-related events and conditions (risk factors) may affect its performance. A complete lack of data forces assumptions about key aspects of the risk environment during decision making and ongoing operations. There is no awareness of external requirements to evaluate IT risk.

1 Initial when
Recognition of the need for risk evaluation is emerging; however, there is minimal understanding of the business environment and the associated threats and events that may affect performance. By default, IT is accountable for risk evaluation. Current IT risk information and mitigation options are inferred from episodic assessments. Any data collection and analysis methods are *ad hoc* and may be compliance-driven. IT risk analysis skills may exist on an *ad hoc* basis, but they are not actively developed.

2 Repeatable when
Worst-case loss scenarios are the focus of discussions, although the driving factors for those scenarios may not be understood. Individuals assume responsibility for both risk evaluation and risk response. Some planned risk analysis occurs, but practitioners make major assumptions about the contributing factors for risk. Dependency analysis and scenario analysis are *ad hoc* and focus on only a limited number of business activities. Minimum skill requirements are identified for critical areas of data collection, risk analysis and risk profiling. Functional and IT silo-specific risk analysis approaches and tools exist but are based on solutions developed by key individuals.

3 Defined when
There is an emerging understanding of risk fundamentals. Gaps between IT-related risk and opportunity and overall risk appetite are being recognised. Responsibility and accountability for key risk evaluation practices are defined and process owners have been identified. The capability is in place to evaluate IT risk alongside other risk types across the enterprise. Dependency analysis and scenario analysis procedures are defined and performed across multiple business activities, business lines and products. Skill requirements are defined and documented for all enterprise risk areas, with full consideration of data collection, risk analysis and profiling. Data collection tools generally adhere to defined standards and distinguish amongst threat events, loss events and vulnerability events.

4 Managed when
Risk analysis has been accepted as a way to better understand the enterprise's resilience and be better prepared to achieve strategic objectives. All types of risk have a nominated owner, and senior business management and IT management together determine the business relevance of risk factors. Risk evaluation efficiency and effectiveness are measured and communicated, and linked to business goals and the IT strategic plan. Risk evaluation exceptions are noted by management and root-cause analysis is being standardised. All risk analysis results are subject to formal peer review, and the root cause of quality issues is investigated. The enterprise is addressing the longer-term development needs of staff with high potential in risk evaluation and related skills. Risk analysis tools are implemented according to a standardised plan, and some have been integrated with other related tools.

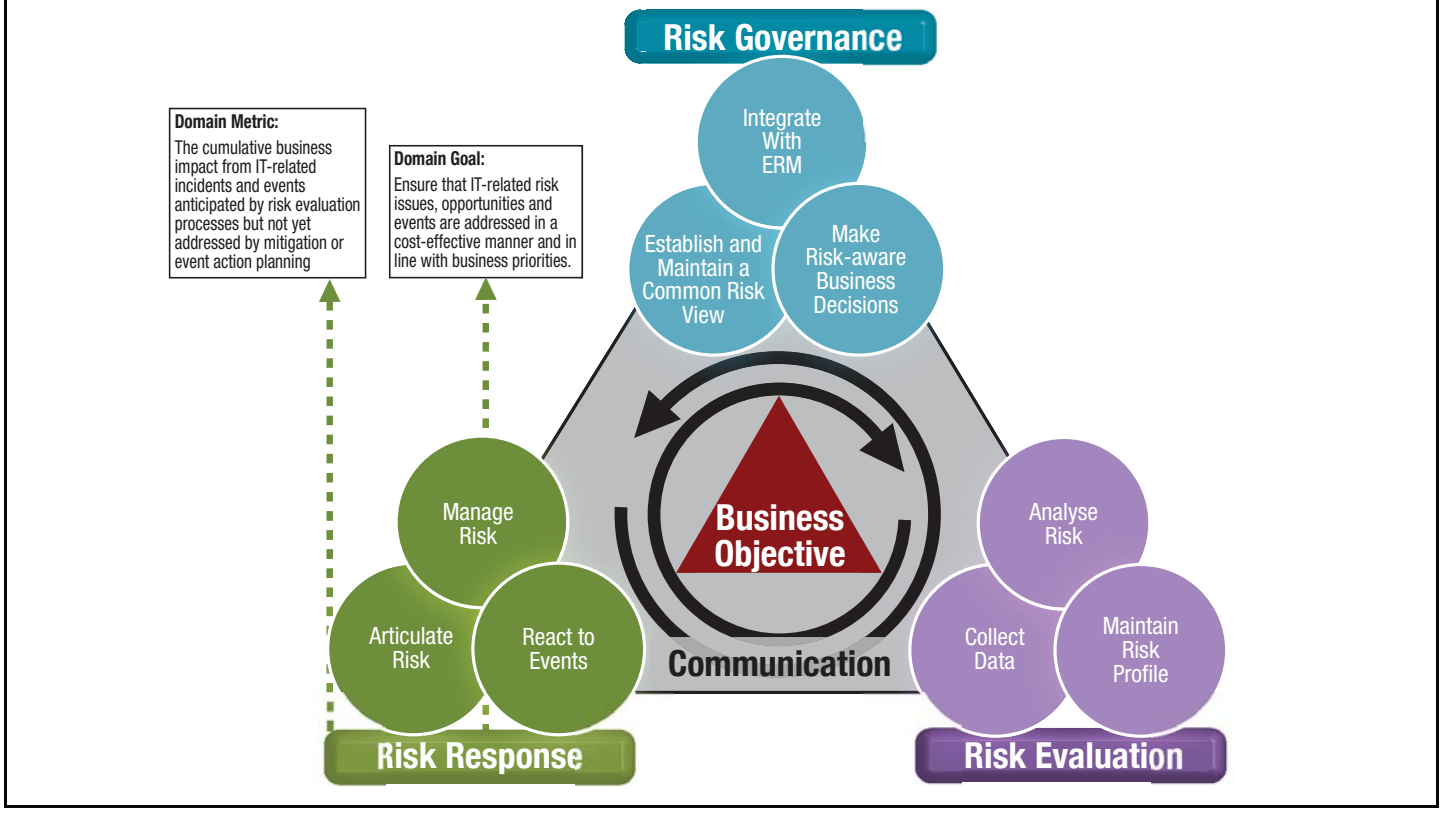
5 Optimised when
Decision makers enjoy transparency into IT risk and have available the best possible information about loss and gain probabilities, emerging exposures and opportunities. The drivers of the real risks to real operations are vigorously communicated throughout the extended enterprise. Employees at every level take direct responsibility for determining the business relevance of risk factors. The enterprise maintains an optimal balance between the qualitative and quantitative methods that support decisions on managing uncertainties and seizing risky opportunities. Risk evaluation activities are based on a broad and deep set of IT risk scenarios that integrate all business activities, business lines, products and known risk types. The enterprise formally requires continuous improvement of data collection, risk analysis and profiling skills. Automated tools enable end-to-end support and improvement of risk evaluation efforts.

Figure 34—RE Detailed Maturity Model Part 1			
	Awareness and Communication	**Responsibility and Accountability**	**Goal Setting and Measurement**
0	The enterprise does not recognise the need to understand how IT-related events and conditions (risk factors) may affect its performance. A complete lack of data forces assumptions about key aspects of the risk environment during decision making and ongoing operations. There is no awareness of external requirements to evaluate IT risk.		
1	Recognition of the need for risk evaluation is emerging; however, there is minimal understanding of the business environment and the associated threats end events that may affect performance. There is minimal feedback to decision makers regarding the effect risk decisions have on the risk condition and the business condition. The identification and analysis of IT risk is based on 'gut feel' rather than in the context of business activities, and may be perceived as producing unfounded worst-case scenarios.	By default, IT is accountable for risk evaluation. No performance measurement and reward programme exists to support individual responsibility for identifying how much risk exists.	Current IT risk information and mitigation options are inferred from episodic assessments.
2	Worst-case loss scenarios are the focus of discussions, although the driving factors for those scenarios may not be understood. Some feedback is provided to decision makers regarding the effect that IT risk decisions have on the business condition. There are localised taxonomies used as a basis for discussion of IT risk analysis concepts.	Individuals assume responsibility for both risk evaluation and risk response. There is confusion about enterprise risk evaluation responsibilities. When problems occur, a culture of blame tends to exist.	Some planned risk analysis occurs, but practitioners make major assumptions about the contributing factors for risk. Some goal setting for data collection and analysis occurs but is not tracked with key metrics.
3	There is an emerging understanding of risk fundamentals. Gaps between IT-related risk and opportunity and overall risk appetite are being recognised. Risk analysis discussions are based on a defined language/taxonomy. Decision makers are provided regular qualitative feedback regarding the effect that IT-related risk decisions have on the business condition. Enterprise-level information regarding risk analysis practices and issues is shared.	Responsibility and accountability for key risk evaluation practices are defined and process owners have been identified. The process owner is unlikely to have full authority to exercise the responsibilities. Job descriptions consider risk evaluation responsibilities.	The capability is in place to evaluate IT risk alongside other risk types across the enterprise. Risk information and mitigation options are based on defined procedures and meet the basic needs of decision makers. Regular reporting of IT risk evaluation process outcomes is directed to IT management. Measurement of risk evaluation processes emerges, but is not consistently applied.
4	Risk analysis has been accepted as a way to better understand the enterprise's resilience and be better prepared to achieve strategic objectives. Risk identification and analysis methodologies produce structured multi-risk scenarios that are well understood by management and practitioners. Risk analysis discussions are based on defined terms. Rational estimates of loss probabilities and response options are available to all stakeholders. Decision makers receive regular quantitative feedback on the effect IT-related risk decisions have on the business condition. Enterprise risk data conform to a standard model and are widely shared.	All types of risk have a nominated owner, and senior business management and IT management together determine the business relevance of risk factors. Risk evaluation responsibility and accountability are accepted and working in a way that enables a process owner to fully discharge his/her responsibilities. A reward culture is in place that motivates positive action.	IT risk information and mitigation options are based on quantitative methods and anticipate the needs of decision makers. Management is able to monitor the risk profile. Risk evaluation efficiency and effectiveness are measured and communicated and linked to business goals and the IT strategic plan. Risk evaluation exceptions are noted by management, and root-cause analysis is being standardised. The acceptable degrees of error or inconsistency in risk analysis are well established. Business management receives regular reporting of business outcomes related to IT risk evaluation
5	Decision makers enjoy transparency into IT risk and have available the best possible information about loss and gain probabilities, emerging exposures and opportunities. The drivers of the real risks to real operations are vigorously communicated throughout the extended enterprise.	Employees at every level take direct responsibility for determining the business relevance of risk factors.	The enterprise maintains an optimal balance between the qualitative and quantitative methods that support decisions on managing uncertainties and seizing risky opportunities.

Figure 35—RE Detailed Maturity Model Part 2			
	Policies, Standards and Procedures	**Skills and Expertise**	**Tools and Automation**
0			
1	Any data collection and analysis methods are *ad hoc* and may be compliance-driven. Risk evaluation may not include all the components of risk.	IT risk analysis skills may exist on an *ad hoc* basis, but they are not actively developed. Enterprise risk managers and business process owners lack IT risk evaluation understanding. IT personnel lack the skills to determine the business relevance of risk factors. Employees desire improved data collection, analysis and profiling skills, but no inventory of risk evaluation skills exists nor is a competency model established for documenting future skill requirements.	Departments and functions maintain their own informal checklists for risk evaluation within their silos.
2	Dependency analysis and scenario analysis are *ad hoc* and focus on only a limited number of business activities. Data collection, analysis and profiling methods are being used but may lack key elements and will vary across the enterprise and the IT organisation. It is difficult to normalise data across the enterprise.	Minimum skill requirements are identified for critical areas of data collection, risk analysis and risk profiling. Risk evaluation training is provided in response to needs, rather than on the basis of an agreed-upon plan, and informal training on the job occurs.	Functional and IT silo-specific risk analysis approaches and tools exist, but are based on solutions developed by key individuals. Data collected in support of risk analysis are recorded in desktop applications. However, minimal distinction is made amongst threat events, vulnerability events and loss events.
3	Risk evaluation methodologies are accepted by management. Dependency analysis and scenario analysis procedures are defined and performed across multiple business activities, business lines and products. Risk analysis takes a probabilistic approach and considers threat frequency, vulnerability and loss magnitude. Risk analysis scope regularly includes existing systems and systems under design and development. The majority of risk analysis results are subject to formal peer review.	Skill requirements are defined and documented for all enterprise risk areas, with full consideration of data collection, risk analysis and profiling. Risk evaluation training includes techniques beyond minimum policy and common tools to determine the business relevance of risk factors. Enterprise risk managers and business process owners receive targeted IT risk analysis training. Skill requirements are defined and documented for all areas of risk evaluation. A formal training plan for risk evaluation has been developed. Data are available regarding the movement of critical risk evaluation skills and competencies.	Data collection tools generally adhere to defined standards and distinguish amongst threat events, loss events and vulnerability events. Some centralised tools with standardised evaluation criteria are in place (e.g., frequency, loss/gain magnitude, business impact, control effectiveness, cost to remediate). Prototypes of workflow have been established to embed risk probabilities in decision-making procedures.
4	Data collection, dependency analysis and scenario analysis procedures are defined and performed across multiple risk types, business activities, business lines and products. All risk analysis results are subject to formal peer review and the root cause of quality issues is investigated.	Skill requirements are routinely updated for all areas of risk evaluation, proficiency is ensured for all critical areas and certification is encouraged. The enterprise is addressing the longer-term development needs of staff with high potential in risk evaluation and related skills. Mature IT risk analysis training techniques are applied according to the training plan, and knowledge sharing is encouraged. All internal IT evaluation experts are involved, and the effectiveness of the training plan is evaluated.	Risk analysis tools are implemented according to a standardised plan and some have been integrated with other related tools. Risk evaluation tools are being used in main areas to automate critical activities in support of data collection, risk analysis and risk profiling.
5	Risk evaluation activities are based on a broad and deep set of IT risk scenarios that integrate all business activities, business lines, products and known risk types. The root cause of risk is consistently understood and always used as the basis for risk response decisions. Peer review of risk analysis results and of other key risk evaluation practices is subject to rigorous root-cause analysis, and actions are always taken to improve the results.	The enterprise formally requires continuous improvement of data collection, risk analysis and profiling skills, based on clearly defined personal and enterprise goals.	Real-time data are collected on threat events, vulnerability events, loss events and discovery of risk factors. Automated tools enable end-to-end support and improvement of risk evaluation efforts.

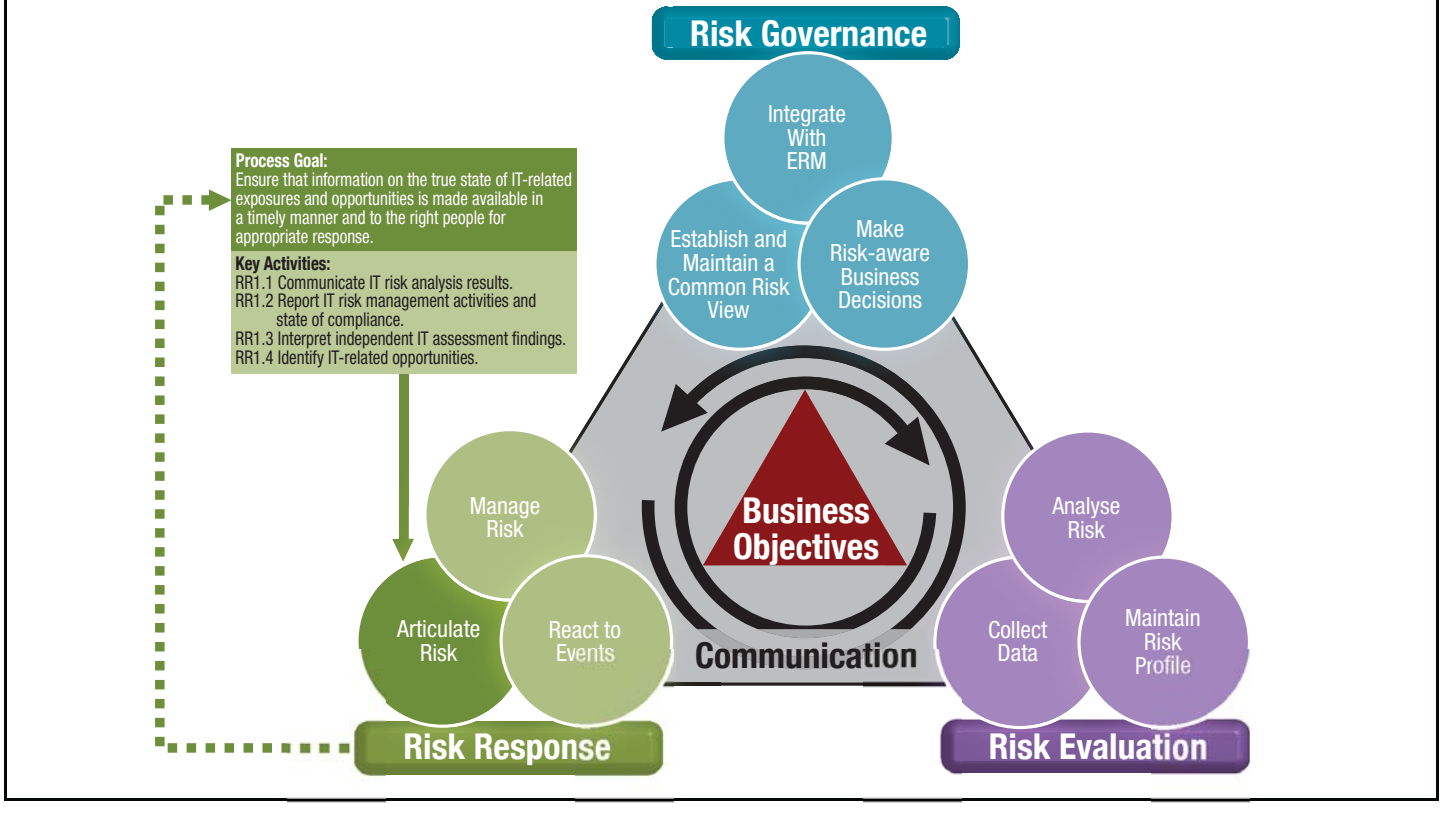
DOMAIN OVERVIEW

Figure 36—Risk Response Domain



PROCESS OVERVIEW

Figure 37—Process RR1 Articulate Risk



PROCESS DETAIL

RR1 Articulate risk.

Ensure that information on the true state of IT-related exposures and opportunities is made available in a timely manner and to the right people for appropriate response.

RR1.1 Communicate IT risk analysis results.

Report the results of risk analysis in terms and formats useful to support business decisions. Co-ordinate additional risk analysis activity as required by decision makers (e.g., report rejection, scope adjustment). Communicate clearly the risk-return context. Wherever possible, include probabilities of loss and/or gain, ranges and confidence levels that enable management to balance risk-return. Identify the negative impacts of events/scenarios that should drive response decisions and the positive impacts of events/scenarios that represent opportunities management should channel back into the strategy and objective-setting process. Provide decision makers with an understanding of worst-case and most probable scenarios; due diligence exposures; and significant reputation, legal or regulatory considerations. Include the following:

- Key components of risk (e.g., frequency, magnitude, impact) and key risk factors and their estimated effects
- Estimated probable loss magnitude or probable future gain
- Estimated high-end loss/gain potential and most probable loss/gain scenario(s) (e.g., a probable loss frequency of between three and five times per year, and a probable loss magnitude of between US $50,000 and $100,000, with 90 percent confidence).
- Additional relevant information to support the conclusions and recommendations of the analysis

From	Inputs
RG2.2	Integrated risk management strategy
RG3.2	Risk analysis deficiencies
RE2.3	Risk analysis results
RE2.4	Peer-review recommendations

To	Outputs
RG1.4, RG1.6, RG2.1, RG2.2, RG3.3, RG3.4, RG3.5, RE2.1, RE2.3, RR1.2, RR2.3, RR3.1	IT risk issues and opportunities
RG3.2, RE3.5, RR1.3, RR1.4, RR2.2, RR3.1, RR3.4	Risk analysis report
RG3.3, RG3.4, RG3.5	Loss/gain probabilities and ranges, risk response options, cost/benefit expectations
RE3.5	IT risk profile changes
Val IT IM2	Business case opportunity

RR1.2 Report IT risk management activities and state of compliance.

Meet the risk reporting needs of various stakeholders (e.g., board, risk committee, risk control functions, business unit management). To ensure strategic and efficient reporting on IT risk issues and status, apply the principles of relevance, efficiency, timeliness and accuracy. Include control effectiveness and performance, issues and gaps, remediation status, events and incidents, and their impacts on the risk profile. Include performance of risk management processes. Provide inputs to integrated enterprise reporting.

From	Inputs
RG2.2	Integrated risk reporting requirements
RR1.1, RR1.4, RR2.2	IT risk issues and opportunities
RR2.2	Key IT risk indicators and escalation triggers, risk aggregation data
CobiT PO9	Risk reporting
CobiT DS8	Incident reports
CobiT DS13	Incident tickets, error logs, process performance reports
CobiT ME2	Report on effectiveness of IT controls
CobiT ME3	Catalogue of legal and regulatory requirements related to IT service delivery, report on compliance of IT activities with external legal and regulatory requirements

To	Outputs
RG1.4, RG1.5, RG2.5; CobiT ME1, ME2	State of compliance reports
RG2.2, RG2.5; *	Inputs to integrated enterprise risk reporting
RG3.4, RE2.3, RR2.1, RR2.2, RR2.3, RR3.2; CobiT PO9, ME1, ME2	Control gaps and policy exceptions

* Input from/output to outside Risk IT, Val IT and CobiT

RR1.3 Interpret independent IT assessment findings.

Review the results and specific findings of objective third parties, internal audit, quality assurance, self-assessment activities, etc. Map them to the risk profile and the risk and control baseline, while considering established risk tolerance. Take gaps and exposures to the business for their call on disposition or the need for risk analysis. Help the business understand how corrective action plans will affect the overall risk profile. Identify opportunities for integration with other remediation efforts and ongoing risk management activities.

From	Inputs
RG1.3	IT risk tolerance thresholds
RG1.4	IT risk policy
RE3.5	IT risk profile
RR1.1	Risk analysis report
RR2.1	Risk and control baseline
CobiT AI7	Internal control monitoring
CobiT ME2	Report on effectiveness of IT controls
*	Reports from external audit, monitoring functions, internal audit, quality assurance, risk and control self-assessment

To	Outputs
RG1.1, RG3.3, RG3.4, RG3.5, RE2.2, RE3.5	Independent IT assessment findings in context
RG3.4, RG3.5, RE2.2, RE3.5, RR2.3	Vulnerability events
RE2.1	Risk analysis request
RE3.5	IT risk profile changes

RR1.4 Identify IT-related opportunities.

On a recurrent basis, consider the relative levels of IT risk to IT risk management capacity for specific business processes, business units, products, etc. For areas with relative risk and risk capacity parity (i.e., indicating an ability to take on more risk), identify IT-related opportunities that could enable the area to accept greater risk and enhance growth and return.

Look for opportunities where IT can be used to:
- Leverage enterprise resources in creating competitive advantage (e.g., use existing information in new ways, better leverage human and business resources)
- Reduce enterprise co-ordination costs
- Exploit scale and scope economies in certain key strategic resources common to several lines of business
- Leverage structural differences with competitors
- Co-ordinate activities amongst business units or in the value chain

From	Inputs
RE1.4	Emerging threats
RE3.3	IT capability assessment
RR1.1	Risk analysis report
RR2.1	Control reduction opportunities
RR3.2	Risk event alert

To	Outputs
RG1.4, RG1.6, RG2.1, RG2.2, RG3.3, RG3.4, RG3.5, RE2.1, RE2.3, RR1.2, RR2.3, RR3.1	IT risk issues and opportunities
RE2.1	Risk analysis request

MANAGEMENT GUIDELINES—RR1

RACI Chart **Roles**

Key Activities	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RR1.1 Communicate IT risk analysis results.		I	R	C	C	C	A	R	R	C	I
RR1.2 Report IT risk management activities and state of compliance.	I	I	C	R	I	A	I	I	I	I	C
RR1.3 Interpret independent IT assessment findings.	I	I	A/R	R	I	I	I		C	I	C
RR1.4 Identify IT-related opportunities.		I	I	R	I	I	A	R	R	I	I

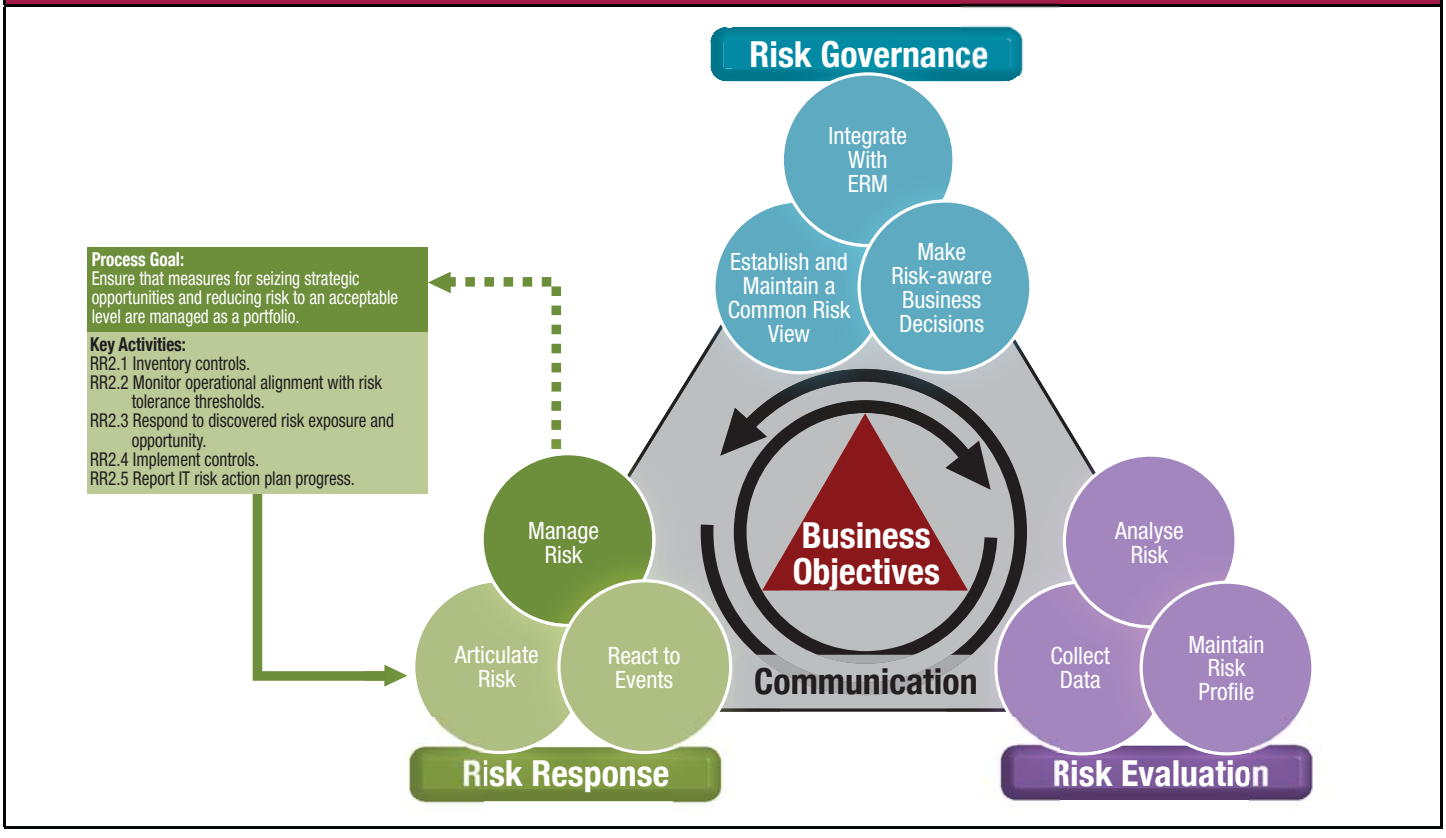
A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics

Activity Goals	Process Goal	RR Goal
• Communicate IT risk analysis results. • Report IT risk management activities and state of compliance. • Interpret independent IT assessment findings. • Identify IT-related opportunities.	• Ensure that information on the true state of IT-related exposures and opportunities is made available in a timely manner and to the right people for appropriate response.	• Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities.
Activity Metrics	**Process Metrics**	**RR Metric**
• Percentage of risk analysis reports accepted on initial delivery • Percentage of on-time risk management reports • Frequency of risk management activity reporting • Number of IT-related events with business impact not previously reported as an IT risk • Number of IT risk issues identified by outside parties yet to be interpreted and mapped into the risk profile	• Percentage of risk issues inappropriately distributed too high or too low in the enterprise hierarchy (and consequently sent up or down the chain of command for decision) • The number of IT-related events with business impact not earlier reported as an IT risk • Percentage of critical IT assets/resources covered by monitoring activities (detectability) • Timeliness of reports on IT exposures relative to the next expected threat or loss event • Potential business impact of exposures (as agreed upon by management) discovered by assurance groups	• The cumulative business impact from IT-related incidents and events anticipated by risk evaluation processes but not yet addressed by mitigation or event action planning

PROCESS OVERVIEW

Figure 38—Process RR2 Manage Risk



PROCESS DETAIL

RR2 Manage risk.

Ensure that measures for seizing strategic opportunities and reducing risk to an acceptable level are managed as a portfolio.

RR2.1 Inventory controls.

Across the risk focus areas, inventory the controls in place to manage risk and enable risk to be taken in line with risk appetite and tolerance. Classify controls (e.g., predictive, preventive, detective, corrective) and map them to specific IT risk statements and aggregations of IT risk. Develop tests for control design and tests for control operating effectiveness. Identify procedures and technology used to monitor the operation of controls (e.g., monitoring of controls when IT is involved or the automation of enterprise monitoring processes). Partition operational controls into the following categories: controls deployed in line with expectations with no known operating deficiencies, controls deployed in line with expectations with known operating deficiencies, and controls deployed beyond expectations with no known operating deficiencies. This third category of controls may not be justified and could indicate opportunity for cost reduction while maintaining the same level of risk.

From	Inputs
RG1.1	Risk focus areas
RG1.3	IT risk tolerance thresholds
RG1.4	IT risk policy
RG2.1	IT risk domain owners
RG2.2	Integrated risk management strategy
RG3.4, RR3.4	Risk response requirements
RE3.3	IT capability assessment
RE3.5	IT risk profile
RE3.5, RR2.4	Risk and control baseline updates
RR1.2, RR2.2	Control gaps and policy exceptions
CobiT PO6	Enterprise IT control framework
CobiT AI7	Internal control monitoring
CobiT ME2	Report on effectiveness of IT controls
CobiT ME3	Catalogue of legal and regulatory requirements related to IT service delivery, report on compliance of IT activities with external legal and regulatory requirements
*	Legal and regulatory requirements mappings

* Input from/output to outside Risk IT, Val IT and CobiT

To	Outputs
RG2.5, RE2.2, RE2.3, RE3.5, RR1.3, RR2.2, RR3.4; CobiT PO6	Risk and control baseline
RR1.4	Control reduction opportunities

RR2.2 Monitor operational alignment with risk tolerance thresholds.

Ensure that each business line accepts accountability for operating within its individual and portfolio tolerance levels and for embedding monitoring tools into key operating processes. Monitor control performance, and measure variance from thresholds against objectives. For key risk issues, periodically test control design and operating effectiveness. Obtain buy-in from management on indicators that will function as KRIs. When implementing KRIs, set thresholds and checkpoints (e.g., weekly, daily, continuously), and configure where to send notifications (e.g., line management, senior management, internal audit) so the recipients can respond or adjust their plans. Integrate KRI data into ongoing performance indicator reporting. Ensure that there is a detailed examination of areas of residual risk outside of tolerance thresholds (e.g., request risk analysis).

From	Inputs
RG1.3	IT risk tolerance thresholds
RG2.2	Integrated risk management strategy
RE3.2	Asset/resource criticality
RE3.5	IT risk profile
RE3.6	IT risk indicators, KRI recommendations
RR1.1	Risk analysis report
RR1.2	Control gaps and policy exceptions
RR2.1	Risk and control baseline
RR3.2	Risk event alert
*	Risk culture survey results, data on adherence to policy and standards, data on risk tolerance thresholds vs. policy vs. operations

* Input from/output to outside Risk IT, Val IT and CobiT

To	Outputs
RG1.4, RG1.6, RG2.1, RG2.2, RG3.3, RG3.4, RG3.5, RE2.1, RE2.3, RR1.2, RR2.3, RR3.1	IT risk issues and opportunities
RG2.2; *	Monitoring requirements
RG2.3, RE3.6, RR1.2, RR2.3, RR3.2	Key IT risk indicators and escalation triggers
RG3.4, RE2.3, RR2.1, RR2.3, RR3.2; CobiT PO9, ME1, ME2	Control gaps and policy exceptions
RG3.4, RR1.2; CobiT PO9	Risk aggregation data
RE2.1	Risk analysis request

* Input from/output to outside Risk IT, Val IT and CobiT

RR2.3 Respond to discovered risk exposure and opportunity.

Emphasise projects that are expected to reduce the potential frequency and magnitude of adverse events/losses, and balance them with projects enabling the seizing of strategic business opportunities. Hold cost/benefit discussions regarding the contribution of new or existing controls towards operating within IT risk tolerance. Select candidate IT controls based on specific threats, the degree of risk exposure, probable loss and mandatory requirements specified in IT standards. Monitor changes to the underlying business operational risk profiles and adjust the rankings of risk response projects.

From	Inputs
RG3.3	Full economic life cycle cost and benefits
RG3.4, RR3.4	Risk response requirements
RG3.5	Risk management benefits assigned to IT portfolio, risk response priority (risk disposition)
RR1.1, RR1.4, RR2.2	IT risk issues and opportunities
RR1.2, RR2.2	Control gaps and policy exceptions
RR1.3	Vulnerability events
RR2.2	Key IT risk indicators and escalation triggers
Val IT IM5	Programme plan
CobiT PO1	Strategic IT plan, tactical IT plans, IT project portfolio, IT service portfolio, IT sourcing strategy, IT acquisition strategy
CobiT PO2	Information architecture, assigned data classifications, classification procedures and tools
CobiT PO3	Technology opportunities
CobiT PO5	IT budgets
*	Enterprise architecture road map or blueprint, business operational risk profiles

* Input from/output to outside Risk IT, Val IT and CobiT

To	Outputs
RG2.2, RG2.5, RG3.3, RR2.4, RR2.5, RR3.1; Val IT PM4; CobiT PO4, PO9, AI6, ME1, ME2	IT risk action plans
Val IT IM1; CobiT PO9	IT risk response definition

RR2.4 Implement controls.
Take appropriate steps to ensure the effective deployment of new controls and adjustments to existing controls. Communicate with key stakeholders early in the process. Before relying on the control, conduct pilot testing and review performance data to verify operation against design. Map new and updated operational controls to monitoring mechanisms that will measure control performance over time, and prompt management corrective action when needed. Identify and train staff on new procedures as they are deployed.

From	Inputs
RG2.1, RG2.2, RG2.3, RR2.3, RR3.4	IT risk action plans
RG3.4, RR3.4	Risk response requirements

To	Outputs
RR2.1	Risk and control baseline updates
RR3.2	Control performance monitoring requirements
CobiT DS7	Specific training requirements for IT risk management

RR2.5 Report IT risk action plan progress.
Monitor IT risk action plans at all levels to ensure the effectiveness of required actions and determine whether acceptance of residual risk was obtained. Ensure that committed actions are owned by the affected process owner(s) and deviations are reported to senior management.

From	Inputs
RG2.1, RG2.2, RG2.3, RR2.3, RR3.4	IT risk action plans
RR3.1	Incident response plans

To	Outputs
RG1.6, RG2.5, RE3.5, RR3.1	IT risk action plan progress/deviations

MANAGEMENT GUIDELINES—RR2

RACI Chart

Key Activities	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
	Roles										
RR2.1 Inventory controls.		I	A/R	C	I	I	C	C	R		C
RR2.2 Monitor operational alignment with risk tolerance thresholds.			C	C		I	A	R	R		C
RR2.3 Respond to discovered risk exposure and opportunity.	I	A	C	R	C	I	R	C	C	C	
RR2.4 Implement controls.	I	A	C	R	C	I	R	C	C	C	I
RR2.5 Report IT risk action plan progress.	I	I	I	R	I	I	I	A	R	I	I

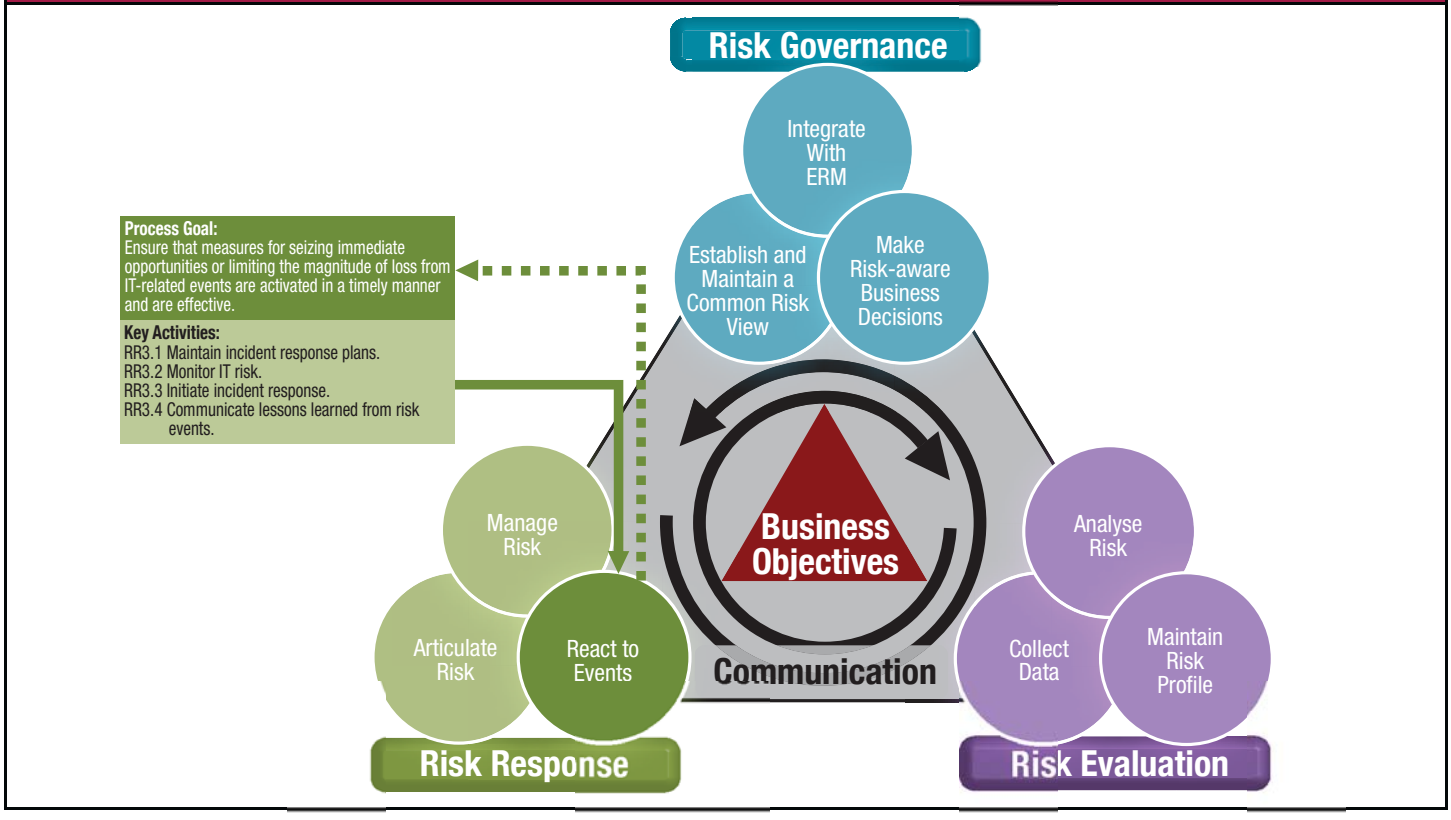
A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics

Activity Goals	Process Goal	RR Goal
• Inventory controls. • Monitor operational alignment with risk tolerance thresholds. • Respond to discovered risk exposure and opportunity. • Implement controls. • Report IT risk action plan progress.	• Ensure that measures for seizing strategic opportunities and reducing risk to an acceptable level are managed as a portfolio.	• Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities.
Activity Metrics	**Process Metrics**	**RR Metric**
• Existence of a risk and control baseline for use in monitoring • Percentage of risk tolerance thresholds embedded into the risk and control baseline • Percentage of controls that are directly related to maintaining the defined risk tolerance • Percentage of IT risk issues exceeding defined risk tolerance for which action plans have been established (alternatively, percentage of mitigation plans that have not been developed) • Number of required KRIs that are fully implemented (e.g., thresholds and checkpoints set, notifications configured) • Amount of KRI data integrated into ongoing performance indicator reporting • Number and value of missed IT-related opportunities	• Satisfaction of the risk owner regarding risk mitigation project outcomes • Percentage of IT risk action plans executed on time (per management's decision, set date) • Percentage of unaccepted IT risk issues without action plans developed • Percentage of unaccepted IT risk issues with action plan developed • Amount of investment spent on risk mitigation efforts that are later cancelled • Number of pending examinations of areas of residual risk outside of tolerance thresholds	• The cumulative business impact from IT-related incidents and events anticipated by risk evaluation processes but not yet addressed by mitigation or event action planning

PROCESS OVERVIEW

Figure 39—Process RR3 React to Events



PROCESS DETAIL

RR3 React to events.

Ensure that measures for seizing immediate opportunities or limiting the magnitude of loss from IT-related events are activated in a timely manner and are effective.

RR3.1 Maintain incident response plans.

Prepare for the materialisation of threats through plans that document the specific steps to take when a risk event may cause an operational, developmental and/or strategic business impact (i.e., IT-related incident) or has already caused a business impact. Maintain open communication about risk acceptance, risk management activities, analysis techniques and results available to assist with plan preparation. When developing action plans, consider how long the enterprise may be exposed and how long it may take to recover. Based on the potential or known impact, define pathways of escalation across the enterprise, from line management to executive committees. Verify that incident response plans for highly critical processes are adequate.

From	Inputs
RG2.1, RG2.2, RG2.3, RR2.3, RR3.4	IT risk action plans
RE1.2	Operating environment data, historical IT risk and loss data
RE1.3	Real-time problem and loss data, root-cause analysis and loss trends, emerging threats
RE1.4	Emerging threats
RR1.1	Risk analysis report
RR1.1, RR1.4, RR2.2	IT risk issues and opportunities
RR2.5	IT risk action plan progress/deviations

To	Outputs
RG2.2, RR2.5, RR3.2, RR3.3, RR3.4; COBIT PO4, PO8, PO9, AI6, DS5, DS10, ME1, ME2	Incident response plans
RE2.1	Risk analysis request
COBIT DS4	Availability, continuity and recovery specification

RR3.2 Monitor IT risk.

Monitor the environment. When a control limit has been breached, either escalate to the next step or confirm that the measure is back within limits. Categorise incidents (e.g., loss of business, policy violation, system failure, fraud, lawsuit), and compare actual exposures against acceptable thresholds. Communicate business impacts to decision makers. Continue to take action and drive desired outcomes. Ensure policy is followed and that there is clear accountability for follow-up actions.

From	Inputs
RG1.3	IT risk tolerance thresholds
RG2.2	Integrated risk management strategy
RG2.3	Integrated risk management methods
RE3.2	Asset/resource criticality
RR1.2, RR2.2	Control gaps and policy exceptions
RR2.2	Key IT risk indicators and escalation triggers
RR2.4	Control performance monitoring requirements
RR3.1	Incident response plans
COBIT DS5	Security threats and vulnerabilities
COBIT DS13	Incident tickets, error logs, process performance reports

To	Outputs
RR1.4, RR2.2, RR3.3	Risk event alert

RR3.3 Initiate incident response.

Take action to minimise the impact of an incident in progress. Identify the category of the incident and follow the steps in the response plan. Inform all stakeholders and affected parties that an incident is occurring. Identify the amount of time required to carry out the plan and make adjustments, as necessary, for the situation at hand. Ensure that the correct action is taken.

From	Inputs
RR3.1	Incident response plans
RR3.2	Risk event alert

To	Outputs
RE1.3, RR3.4	Incident response actions taken
COBIT DS8	Incident tickets

RR3.4 Communicate lessons learned from risk events.

Examine past adverse events/losses and missed opportunities. Determine whether there was a failure stemming from lack of awareness, capability or motivation. Research the root cause of similar risk events and the relative effectiveness of actions taken then and now. For behavioural incidents, determine the extent of any underlying problems (e.g., a serious systemic problem vs. an isolated case that could be managed through staff training or greater documentation of procedures). Identify tactical corrections; potential investments in projects; or adjustments to overall risk governance, evaluation and/or response processes. For IT operations and service delivery incidents related to IT service offerings and service levels (e.g., defects, rework), integrate with the IT service desk and incident response process and the IT problem management process to identify and correct the underlying root cause. Identity the root cause of IT benefit/value enablement and IT programme and project delivery incidents through open communication across business and IT functions. Request additional risk analysis as needed. Communicate root cause, additional risk response requirements and process improvements to risk governance processes and appropriate decision makers.

From	Inputs
RG1.3	IT risk tolerance thresholds
RG2.3	Integrated risk management methods
RE1.2	Operating environment data, historical IT risk and loss data
RE1.3	Real-time problem and loss data, root-cause analysis and loss trends, emerging threats
RE1.4	Risk factors, emerging threats
RR1.1	Risk analysis report
RR2.1	Risk and control baseline
RR3.1	Incident response plans
RR3.3	Incident response actions taken
COBIT DS8	Incident reports
COBIT DS10	Problem records, known problems, known errors and workarounds

To	Outputs
RG1.6, RE1.3, RE3.6	Root cause of incidents
RG2.1, RE2.3, RR2.1, RR2.3, RR2.4	Risk response requirements
RG2.2, RG2.3, RG2.5	Process improvements
RG2.2, RG2.5, RG3.3, RR2.4, RR2.5, RR3.1; Val IT PM4; COBIT PO4, PO9, AI6, ME1, ME2	IT risk action plans
RE2.1	Risk analysis request
COBIT PO4	Process framework improvements

MANAGEMENT GUIDELINES—RR3

RACI Chart

Roles

Key Activities	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RR3.1 Maintain incident response plans.	I	I	I	R	C	I	I	A	R	C	I
RR3.2 Monitor IT risk.			C	I	I	I	I	A	R	C	R
RR3.3 Initiate incident response.	I	I	I	I	I	I	R	A	R	C	I
RR3.4 Communicate lessons learned from risk events.	I	I	A/R	R	C	I	C	C	R	C	I

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

Goals and Metrics—RR3

Activity Goals	Process Goal	RR Goal
• Maintain incident response plans. • Monitor IT risk. • Initiate incident response. • Communicate lessons learned from risk events.	• Ensure that measures for seizing immediate opportunities or limiting the magnitude of loss from IT-related events are activated in a timely manner and are effective.	• Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities.
Activity Metrics	**Process Metrics**	**RR Metric**
• Percentage of incident response plans past their next required review date • Number of incident response plans with unresolved quality issues • Percentage of risk events with business impact not subject to post-mortem review or lessons learned	• Number of events with business impact due to delayed incident response plan execution • Number of incident response plans without an accountable owner • Timeliness of enacting incident response plans • Percentage of incident response plans with one or more open issues regarding their quality and/or dissemination	• The cumulative business impact from IT-related incidents and events anticipated by risk evaluation processes but not yet addressed by mitigation or event action planning

DOMAIN MATURITY MODEL (RR)
HIGH LEVEL

0 Non-existent when
The enterprise does not recognise the need to manage IT risk issues and exposures to the business and its operations. No crisis communication processes are in place. Monitoring of internal control does not exist. There is no awareness of external requirements to deploy controls, capabilities and resources to limit the frequency and impact (loss magnitude) of IT-related events.

1 Initial when
Recognition of the need for risk response is emerging, but it is viewed as limited to risk avoidance, meeting compliance requirements and reduction of financial consequences through insurance. There is minimal individual awareness of threats and what to do when they materialise. There is minimal accountability for ensuring that reasonable risk response measures are in place and reflect the threat environment and asset values. IT-related events and conditions that could affect day-to-day operations are occasionally discussed at management meetings, but specific risk responses are not considered. IT controls exist but are based on compliance requirements, vary widely in relation to risk and operate in isolated silos. A lack of skills and competency for risk response may force the enterprise to accept risk beyond tolerance levels when value propositions are particularly compelling.

2 Repeatable when
There is individual awareness of threats and points of contact for direction when they materialise. IT risk response issues are communicated by management but IT risk response discussions may be impaired by competing business-unit-specific risk language. There is an emerging leader for IT risk response. Control deficiencies may be identified but are not remediated in a timely manner. Risk mitigation processes are starting to be implemented where IT risk issues are identified. Minimum skill requirements are identified for critical areas of risk articulation, monitoring, and project and crisis management. Common approaches to the use of risk monitoring and response tools exist but are based on solutions developed by key individuals.

3 Defined when
Across the enterprise there is individual understanding of business-impacting threats and the specific actions to take if the business threat materialises. Responsibility and accountability for key risk response practices are defined, and process owners have been identified. Control deficiencies are identified and remediated in a timely manner. An enterprise-level risk response policy defines when and how to respond to risk. Job descriptions include expectations for risk response. Employees are periodically trained in IT-related threats, risk scenarios, and controls relevant to their roles and responsibilities. A plan has been defined for use and standardisation of tools to automate certain IT operational risk management activities, such as user provisioning.

4 Managed when
There is both individual and enterprise understanding of the full requirements for responding to risk. Senior business management and IT management together determine whether a risk condition exceeds defined risk tolerances. A reward culture is in place that motivates positive action. The efficiency and effectiveness of risk response are measured and communicated and linked to business goals and the IT strategic plan. All aspects of the risk response process are documented and quantitatively managed. Skill requirements are routinely updated for all risk response areas, including risk articulation, risk monitoring, project and crisis management, and seizing opportunities. Tools are being used in main areas to enable enterprise risk portfolio management and monitor critical controls, capabilities and resources.

5 Optimised when
The extended enterprise is well aware of the full requirements and the strategies and plans in place for responding to risk. The responses to real threats to real operations are vigorously communicated throughout the extended enterprise. The enterprise as a whole collaborates with external entities to respond to common and pandemic risk issues. The enterprise measures the effectiveness of risk response efforts both internally and in collaboration with external entities. The full range of risk response strategies is holistically applied and, where fully justified, cost-effective controls mitigate exposure to risk on a continuing basis. The enterprise formally requires continuous improvement of risk response skills based on clearly defined personal and enterprise goals. The enterprise employs advanced risk response technologies to take on additional risk intelligently and seize competitive opportunities.

Figure 40—RR Detailed Maturity Model Part 1			
	Awareness and Communication	**Responsibility and Accountability**	**Goal Setting and Measurement**
0	The enterprise does not recognise the need to manage IT risk issues and exposures to the business and its operations. No crisis communication processes are in place. No monitoring of internal control exists. There is no awareness of external requirements to deploy controls, capabilities and resources to limit the frequency and impact (loss magnitude) of IT-related events.		
1	Recognition of the need for risk response is emerging, but it is viewed as limited to risk avoidance, meeting compliance requirements and reduction of financial consequences through insurance. There is minimal individual awareness of threats and what to do when they materialise. There is minimal communication around detection of adverse events/incidents and actions to take in line with business priorities.	There is minimal accountability for ensuring that reasonable risk response measures are in place and reflect the threat environment and asset values. Individuals assume responsibility for both risk evaluation and risk response.	IT-related events and conditions that could affect day-to-day operations are occasionally discussed at management meetings, but specific risk responses are not considered. Control deficiencies are discussed in a reactive mode and are difficult to define. Minimal management information exists to help detect events in a timely manner and respond in line with business priorities.
2	There is growing awareness of the need to respond to risk, as evidenced by the introduction of strategies beyond avoidance, such as reduction, sharing or acceptance in the context of risk appetite and tolerance. There is individual awareness of threats and points of contact for direction when they materialise. IT risk response issues are communicated by management, but IT risk response discussions may be impaired by competing business-unit-specific risk language.	There is an emerging leader for IT risk response. The leader is usually held accountable, even if this is not formally agreed. Overall, there is confusion about responsibility for risk response. When problems occur, a culture of blame tends to exist.	Control deficiencies may be identified but they are not remediated in a timely manner. Some risk response goal-setting occurs but it may not be focused on real risks to real operations.
3	IT and business executives can explain their top three IT risk issues (i.e., combinations of control, value and threat conditions that impose a noteworthy level of risk) and the steps they are taking to respond, in line with risk appetite and tolerance. Across the enterprise there is individual understanding of business-impacting threats and the specific actions to take if the business threat materialises. Employees are aware of their responsibility for control activities. There is a common understanding of the need to enact risk response measures. IT risk strategies and plans are communicated by management. IT risk response discussions are based on a defined language/taxonomy. Enterprise-level information on risk response is shared.	Responsibility and accountability for key risk response practices are defined and process owners have been identified. The process owner is unlikely to have full authority to exercise his/her responsibilities. Job descriptions consider risk response responsibilities.	Control deficiencies are identified and remediated in a timely manner. Unacceptable tolerance and mitigation are reported to the appropriate manager. Risk appetite and tolerance are applied during the development of IT risk mitigation and event action plans. Regular reporting of IT risk response process outcomes is directed to IT management.
4	Management is advised on changes in the business and IT environment that could significantly affect the IT risk scenarios. There is both individual and enterprise understanding of the full requirements for responding to risk. Risk response discussions are based on defined terms. Enterprise risk response information conforms to a standard model and is widely shared.	Senior business management and IT management together determine whether a risk condition exceeds defined risk tolerances. Risk mitigation and response responsibility and accountability are accepted and working in a way that enables a process owner to fully discharge his/her responsibilities. A reward culture is in place that motivates positive action.	Efficiency and effectiveness of risk response are measured and communicated and linked to business goals and the IT strategic plan. The operating effect of control activities is evaluated on a periodic basis, and the process is adequately documented. Regular reporting is made to business management of the business outcomes related to IT risk response process.

Figure 40—RR Detailed Maturity Model Part 1 *(cont.)*			
	Awareness and Communication	**Responsibility and Accountability**	**Goal Setting and Measurement**
5	The extended enterprise is well aware of the full requirements and the strategies and plans in place for responding to risk. The responses to real threats to real operations are vigorously communicated throughout the extended enterprise.	Employees at every level take direct responsibility for responding to risk. The enterprise as a whole collaborates with external entities to respond to common and pandemic risk issues.	The enterprise measures the effectiveness of risk response efforts both internally and in collaboration with external entities.

Figure 41—RR Detailed Maturity Model Part 2			
	Policies, Standards and Procedures	**Skills and Expertise**	**Tools and Automation**
0			
1	IT controls exist but are based on compliance requirements, vary widely in relation to risk and operate in isolated silos.	A lack of skills and competency for risk response may force the enterprise to accept risk beyond tolerance levels when value propositions are particularly compelling. IT risk articulation, monitoring and crisis management skills may exist in silos, but they are not actively developed. Enterprise risk managers and business process owners lack IT risk response understanding. IT personnel lack the project management and crisis management skills critical for risk mitigation programmes and minimising the impact of risk events. Employees desire improved risk response skills, but no inventory of these skills exists nor is there an established competency model for documenting future skill requirements.	Technical security tools are deployed in a haphazard manner that is generally unrelated to risk, impact and cost effectiveness. Some control-centric inventory and incident logging tools may exist; usage is based on standard desktop applications.
2	Risk mitigation processes are starting to be implemented where IT risk issues are identified.	Minimum skill requirements are identified for critical areas of risk articulation, monitoring, and project and crisis management. Risk response training is provided in response to tactical needs, rather than on the basis of an agreed–upon plan, and informal training occurs on the job.	Common approaches to the use of risk monitoring and response tools exist but are based on solutions developed by key individuals.
3	An enterprise-level risk response policy defines when and how to respond to risk. A process to address a key IT risk issue is usually instituted, once it is identified.	Job descriptions include expectations for risk response. Employees are periodically trained in IT-related threats, risk scenarios and controls relevant to their roles and responsibilities. Skill requirements are defined and documented for all enterprise risk areas, with full consideration of IT risk articulation, monitoring and crisis management. Risk response training includes techniques beyond minimum policies and common tools for project management and crisis management. Enterprise risk managers and business process owners receive targeted IT risk response training. Skill requirements are defined and documented for all areas of risk response. A formal training plan for risk response has been developed. Data are available regarding the movement of critical risk response skills and competencies.	A plan has been defined for the use and standardisation of tools to automate certain IT operational risk management activities, such as user provisioning.

Figure 41—RR Detailed Maturity Model Part 2 *(cont.)*			
	Policies, Standards and Procedures	**Skills and Expertise**	**Tools and Automation**
4	There are streamlined mechanisms for reporting risk incidents upward to senior management without delay or 'spin'. All aspects of the risk response process are documented and quantitatively managed. Standards for developing and maintaining the processes and procedures are adopted and followed.	Skill requirements are routinely updated for all risk response areas, including risk articulation, risk monitoring, project and crisis management, and seizing opportunities. Proficiency is ensured for all critical areas, and certification is encouraged. Mature training techniques are applied according to the training plan, and knowledge sharing is encouraged. All internal domain risk response experts are involved, and the effectiveness of the training plan is evaluated. The enterprise is addressing the longer-term development needs of staff with high potential in risk response and related skills.	Tools are being used in main areas to enable enterprise risk portfolio management and monitor critical controls, capabilities and resources.
5	The full range of risk response strategies is holistically applied and, where fully justified, cost-effective controls mitigate exposure to risk on a continuing basis. Process documentation is evolved to automated workflows. Processes, policies and procedures are standardised and integrated to enable end-to-end risk response and improvement.	The enterprise formally requires continuous improvement of risk response skills based on clearly defined personal and enterprise goals. There are frequent reminders and discussions of IT-related threats, risk scenarios, controls and progress towards meeting key risk response goals.	Real-time monitoring of emerging risk factors and threats with standard tools occurs. Technology is leveraged to its fullest extent to document processes, identify gaps, and evaluate the effectiveness of risk-based controls, capabilities and resources. The enterprise employs advanced risk response technologies to take on additional risk intelligently and seize competitive opportunities.

APPENDIX 1. OVERVIEW OF REFERENCE MATERIALS

The following list is an overview of the materials that have been used and referenced during the development of this framework.

AIRMIC, ALARM, IRM, 'A Risk Management Standard', 2002, *www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf*

Alfred P. Sloan Foundation, *Framework for Voluntary Preparedness: Briefing Regarding Private Sector Approaches to Title IX of H.R. 1 and Public Law 110-53*, 'Implementing Recommendations of the 9/11 Commission Act of 2007', USA, 2007

Barnier, B.; 'Driving Value From Nonrevenue-generating Activities: Myths and Misunderstandings of Governance and Risk Management', *ISACA Journal*, ISACA, USA, 2009

Barnier, B.; 'Reducing Operational Risks by Creating Resilience in IT and Infrastructure', IBM, USA, 2008

Caralli, R.; J. Stevens; D. White; L. Young; S. Merrell; S. Bacon; 'CERT Resiliency Engineering Framework v0.95R', Carnegie Mellon, USA, 2008

Caralli, R.; J. Stevens; C. Wallen; D. White; W. Wilson; L. Young; 'Introducing the CERT Resiliency Engineering Framework: Improving the Security and Sustainability Processes', Carnegie Mellon, 2007

Wallen, C.; B. Barnier; D. Nolan; D. O'Neill; 'Managing Resiliency, Taking a Strategic Approach', *FSTC Innovator*, USA, 2009

Club de la Securite de l'Information Français (CLUSIF), 'MEHARI 2007: Concepts and Mechanisms', France, 2007

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

Ernst & Young, *Managing Information Technology Risk: A Global Survey for the Financial Services Industry*, USA, 2008

Rasmussen, M.; 'Taking Control of IT Risk, Defining a Comprehensive IT Risk Management Strategy', Forrester Research Inc., 2006

Gerrard, M.; 'Increase the Value of IT Demand Governance: Add Investment Risk Management', Gartner, USA, 2005

HM Treasury, *Thinking About Risk (Managing your risk appetite: A practitioner's guide; Setting and communicating your risk appetite; Managing your risk appetite: Good practices examples*), UK, 2006

Holthause, D.; 'A Risk-Return Model With Risk and Return Measured as Deviations From a Target Return', USA, 1981

Hubbard, D.; *How to Measure Anything: Finding the Value of "Intangibles" in Business*, John Wiley and Sons Inc., USA, 2007

IBM, 'IT and Infrastructure Risk Management', USA, 2009

Information Security Forum, *Business Impact Assessment*, UK, 2008

Information Security Forum, *ISF Standard of Good Practice, SPRINT Risk Analysis Method*, UK, 2007

Institute for Internal Auditors, *Guide to the Assessment of IT Risk (GAIT)*, USA, 2007

ISO/IEC, ISO/DIS 31000, *Risk Management—Principles and Guidelines on Implementation*, Switzerland, 2009

ISO/IEC, ISO/FDIS 27005, *Information Technology—Security Techniques—Information Security Risk Management*, Switzerland, 2008

ISO/IEC, ISO/IEC27006, *Information Technology—Security Techniques—Requirements for Bodies Providing Audit and Certification of Information Security Management Systems*, Switzerland, 2007

ISACA, COBIT 4.1, USA, 2007, *www.isaca.org*

ISACA, *COBIT® Mapping: Mapping of PMBOK With COBIT® 4.0*, USA, 2006

ISACA, *COBIT® Mapping: Mapping of PRINCE2 With COBIT® 4.0*, USA, 2007

ISACA, *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0*, USA, 2008, *www.isaca.org*

ISACA; *IT Control Objectives for Basel II, The Importance of Governance and Risk Management for Compliance*, USA, 2007, *www.isaca.org*

Jones, J.; 'An Introduction to Factor Analysis of Information Risk (FAIR)', Risk Management Insight, USA, 2005, *http://fairwiki.riskmanagementinsight.com/*

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

Jones, J.; 'Risk Decisions: Whose Call Is It?', Risk Management Insight, USA, 2007

Jones, J.; 'The Case for Risk-based Security', Risk Management Insight, USA, 2007

Messmer, E.; 'Open Group's Security Forum Devising Risk-management Taxonomy', *NetworkWorld*, USA, 2008

Moody, M.; 'Risk and Insurance Management Society (RIMS): Data From Risk Managers Will Help Share ERM Initiatives', The Rough Notes Company Inc., USA, 2007

Open Compliance and Ethics Group (OCEG), *Red Book 2.0: Foundation Guidelines*, USA, 2009

Peccia, A.; 'An Operational Risk Rating Model Approach to Better Measurement and Management of Operational Risk', Citigroup, USA, 2004

Premier Ministre: Secrétariat Général de la Défense Nationale, Direction Centrale de la Sécurité des Systèmes d'Information, 'EBIOS: Expression of Needs and Identification of Security Objectives', France, 2003

PricewaterhouseCoopers LLP, 'A Practical Guide to Risk Assessment', USA, 2008

PricewaterhouseCoopers LLP, 'Extending Enterprise Risk Management (ERM) to Address Emerging Risks', USA, 2009

PricewaterhouseCoopers LLP, 'How to Prepare for Standard and Poor's Enterprise Risk Management Evaluations', webcast, USA, 2008

PricewaterhouseCoopers with IIA, 'IT Risk—Closing the Gap: Giving the Board What It Needs to Understand, Manage and Challenge IT Risk', USA, 2007

Protiviti, 'Credit Rating Analysis of Enterprise Risk Management at Non-Financial Companies: Are You Ready?', USA, 2008

Protiviti Flash Report, 'Societe Generale Aftermath a Call to Action', USA, 2008

Ren, F.; S. Dewan; *Information Technology and Firm Boundaries: Impact on Risk-Return Profile*, The Paul Merage School of Business, University of California, Irvine, USA, 2006

Reznik, S.; 'Back to Business with IT Governance', *The Journal of Corporate Accounting and Finance*, vol. 18, no. 6, Sep/Oct 2007, Wiley Periodicals Inc., USA, 2007

Reznik, S.; 'Make "MyCobiT" Your CobiT', *CobiT Focus*, ISACA, USA, January 2008

Risk and Insurance Management Society (RIMS), *RIMS Risk Maturity Model (RMM) for Enterprise Risk Management*, USA, *www.rims.org/erm/pages/riskmaturitymodel.aspx*

Risk and Insurance Management Society (RIMS), *RIMS Risk Maturity Model (RMM) for Enterprise Risk Management: Executive Summary*, USA, *www.rims.org/erm/pages/riskmaturitymodel.aspx*

Risk and Insurance Management Society (RIMS), *RIMS: Risk Manager Core Competency*, USA, 2007

Ross, R.; S. Katzke; 'Managing Risk from Information Systems: An Organizational Perspective', US Department of Commerce, USA, 2008

Standards Australia, AS/NZS 4360:2004, *Australian/New Zealand Standard for Risk Management*, Australia, 2004, *www.saiglobal.com*

Symantec, *IT Risk Management Process 2: Myths and Realities*, Canada, 2008

The Open Group, 'Requirements for Risk Assessment Methodologies', Technical Guide, USA, 2009

Tanriverdi, H.; T. Ruefli; 'The Role of Information Technology in Risk/Return Relations of Firms', McCombs School of Business, The University of Texas at Austin, USA, 2005

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

APPENDIX 2. HIGH-LEVEL COMPARISON OF RISK IT WITH OTHER RISK MANAGEMENT FRAMEWORKS AND STANDARDS

The Risk IT framework is built upon the six principles defined in *The Risk IT Framework*. **Figure 42** 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, 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 42 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 the comparison.
- The second set of columns provides the mapping for the risk-management-related frameworks.
- The last set of columns describes the principles/features 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 42—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 the following:

- Risk IT focuses on IT.
- Risk IT fits 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)[9].
- 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).

[9] ISACA, *COBIT® Mapping: Mapping of PMBOK With COBIT® 4.0*, USA, 2006, and ISACA, *COBIT® Mapping: Mapping of PRINCE2 With COBIT® 4.0*, USA, 2007

APPENDIX 3. 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[10], one of three possible sorts of events: • 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[11]
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 appetite
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[11]
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
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[11].

[10] 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.

[11] Jones, J.; 'FAIR Taxonomy', Risk Management Insight, USA, 2008

Page intentionally left blank

LIST OF FIGURES

Figure 1—Positioning COBIT, Val IT and Risk IT 7
Figure 2—IT Risk Categories 7
Figure 3—IT Risk in the Risk Hierarchy 11
Figure 4—Audiences and Benefits 12
Figure 5—Risk IT Principles 13
Figure 6—Risk IT Framework 15
Figure 7—Risk Map Indicating Risk Appetite Bands 17
Figure 8—Responsibilities and Accountability for IT Risk Management 19
Figure 9—IT Risk Communication Components 20
Figure 10—Risk Communication Flows 21
Figure 11—Elements of Risk Culture 22
Figure 12—Expressing IT Risk in Business Terms 23
Figure 13—IT Risk Scenario Development 25
Figure 14—IT Risk Scenario Components 25
Figure 15—Risk IT Response Options and Prioritisation 29
Figure 16—Risk and Opportunity 31
Figure 17—Risk IT Process Model Overview ..... Foldout (after page 33)
Figure 18—*The Risk IT Practitioner Guide* Overview 35
Figure 19—Example Inputs and Outputs (RE2.3) 38
Figure 20—Example of RACI Chart (RE2) 38
Figure 21—Role Definitions 39
Figure 22—Example of Goals and Metrics Table (RE2) 40
Figure 23—Maturity Model 41
Figure 24—Risk Governance Domain 44
Figure 25—Process RG1 Establish and Maintain a Common Risk View 44
Figure 26—Process RG2 Integrate With ERM 50
Figure 27—Process RG3 Make Risk-aware Business Decisions 56
Figure 28—RG Detailed Maturity Model Part 1 61
Figure 29—RG Detailed Maturity Model Part 2 62
Figure 30—Risk Evaluation Domain 64
Figure 31—Process RE1 Collect Data 64
Figure 32—Process RE2 Analyse Risk 68
Figure 33—Process RE3 Maintain Risk Profile 72
Figure 34—RE Detailed Maturity Model Part 1 78
Figure 35—RE Detailed Maturity Model Part 2 79
Figure 36—Risk Response Domain 80
Figure 37—Process RR1 Articulate Risk 80
Figure 38—Process RR2 Manage Risk 84
Figure 39—Process RR3 React to Events 89
Figure 40—RR Detailed Maturity Model Part 1 94
Figure 41—RR Detailed Maturity Model Part 2 95
Figure 42—Risk Management Frameworks and Standards Compared 99

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
  - Defininition 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—Focusses 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—Focusses 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—Focusses on one key element of the investment management process
- *Val IT™ Mapping: Mapping of Val IT™ to MSP™, PRINCE2™ and ITIL V3®*, 2009—Focusses 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