The Risk IT Framework

EXCERPT

Summary

Purpose

Principles

Essentials

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 Excerpt* (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*

The Risk IT Framework Excerpt
Printed in the United States of America

ACKNOWLEDGEMENTS

ISACA wishes to recognise:

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

IT Risk Task Force (2008-2009)
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
Steven Babb, CGEIT, KPMG, UK
Brian Barnier, CGEIT, ValueBridge Advisors, USA
Jack Jones, CISA, CISM, CISSP, Risk Management Insight LLC, USA
John W. Lainhart IV, CISA, CISM, CGEIT, IBM Business Consulting Services, USA
Gladys Rouissi, CISA, MComp, Commonwealth Bank of Australia, Australia
Lisa R. Young, CISA, CISSP, Carnegie Mellon University, USA

Expert Reviewers
Mark Adler, CISA, CISM, CGEIT, CFE, CFSA, CIA, CISSP, Commercial Metals, USA
Steven Babb, CGEIT, KPMG, UK
Gary Baker, CGEIT, CA, Deloitte 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

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**.

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 1—Positioning CobiT, Val IT and Risk IT

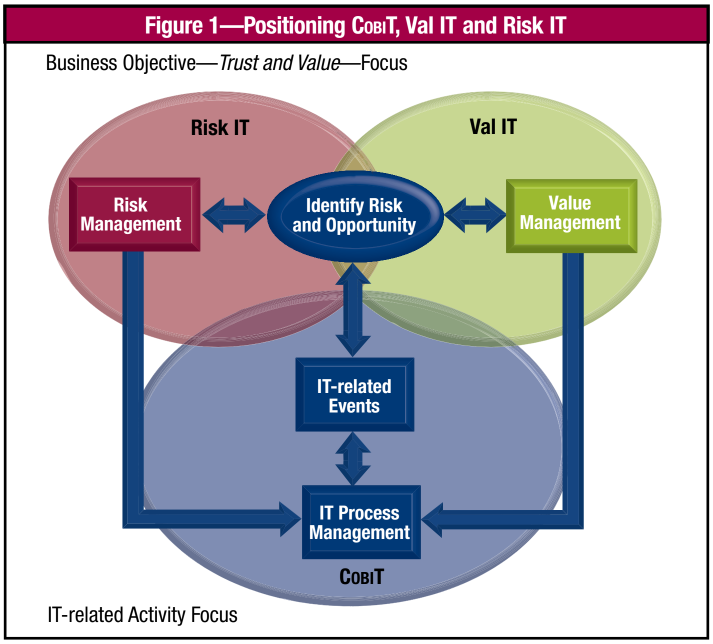
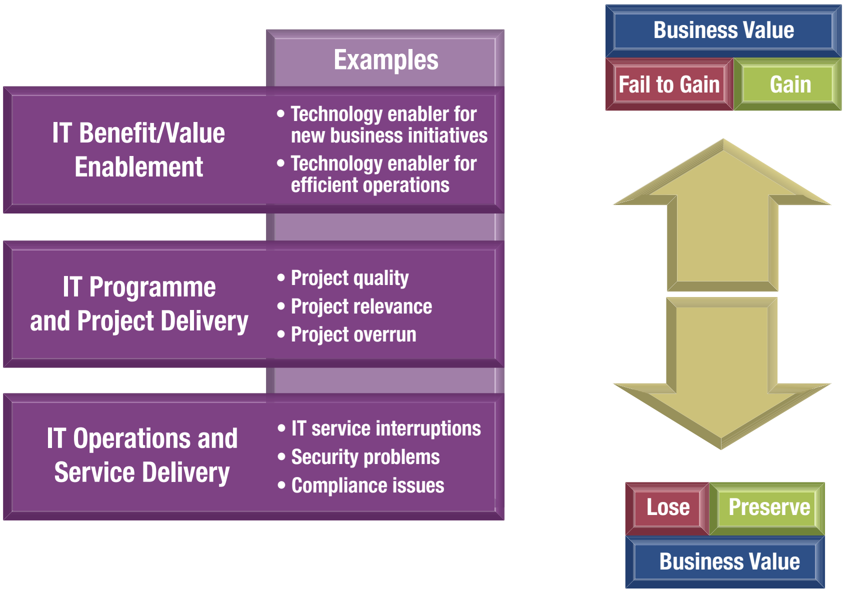

Business Objective—*Trust and Value*—Focus
Risk IT
Val IT
Risk Management
Identify Risk and Opportunity
Value Management
IT-related Events
IT Process Management
CobiT
IT-related Activity Focus

Figure 2—IT Risk Categories


Examples
IT Benefit/Value Enablement
• Technology enabler for new business initiatives
• Technology enabler for efficient operations
IT Programme and Project Delivery
• Project quality
• Project relevance
• Project overrun
IT Operations and Service Delivery
• IT service interruptions
• Security problems
• Compliance issues
Business Value
Fail to Gain
Gain
Lose
Preserve
Business Value

[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.

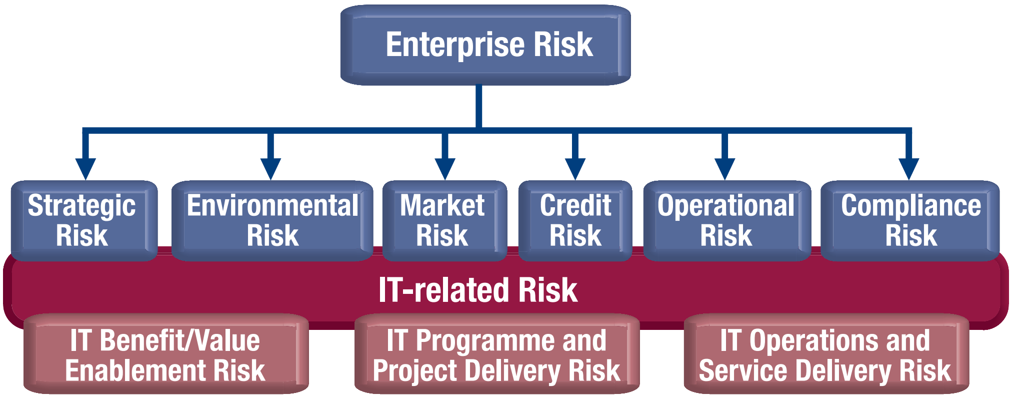
Page intentionally left blank

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

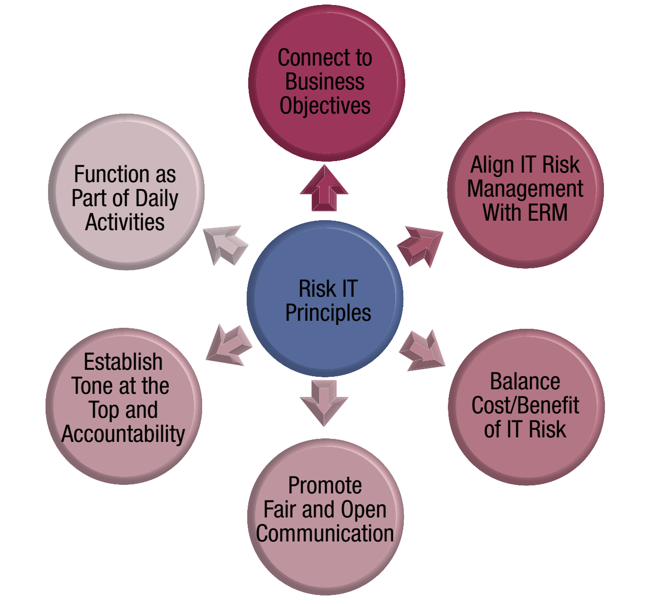
[5] AIRMIC, ALARM, IRM, 'A Risk Management Standard', 2002, *www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf*

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


Connect to Business Objectives
Function as Part of Daily Activities
Align IT Risk Management With ERM
Risk IT Principles
Establish Tone at the Top and Accountability
Balance Cost/Benefit of IT Risk
Promote Fair and Open Communication

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.

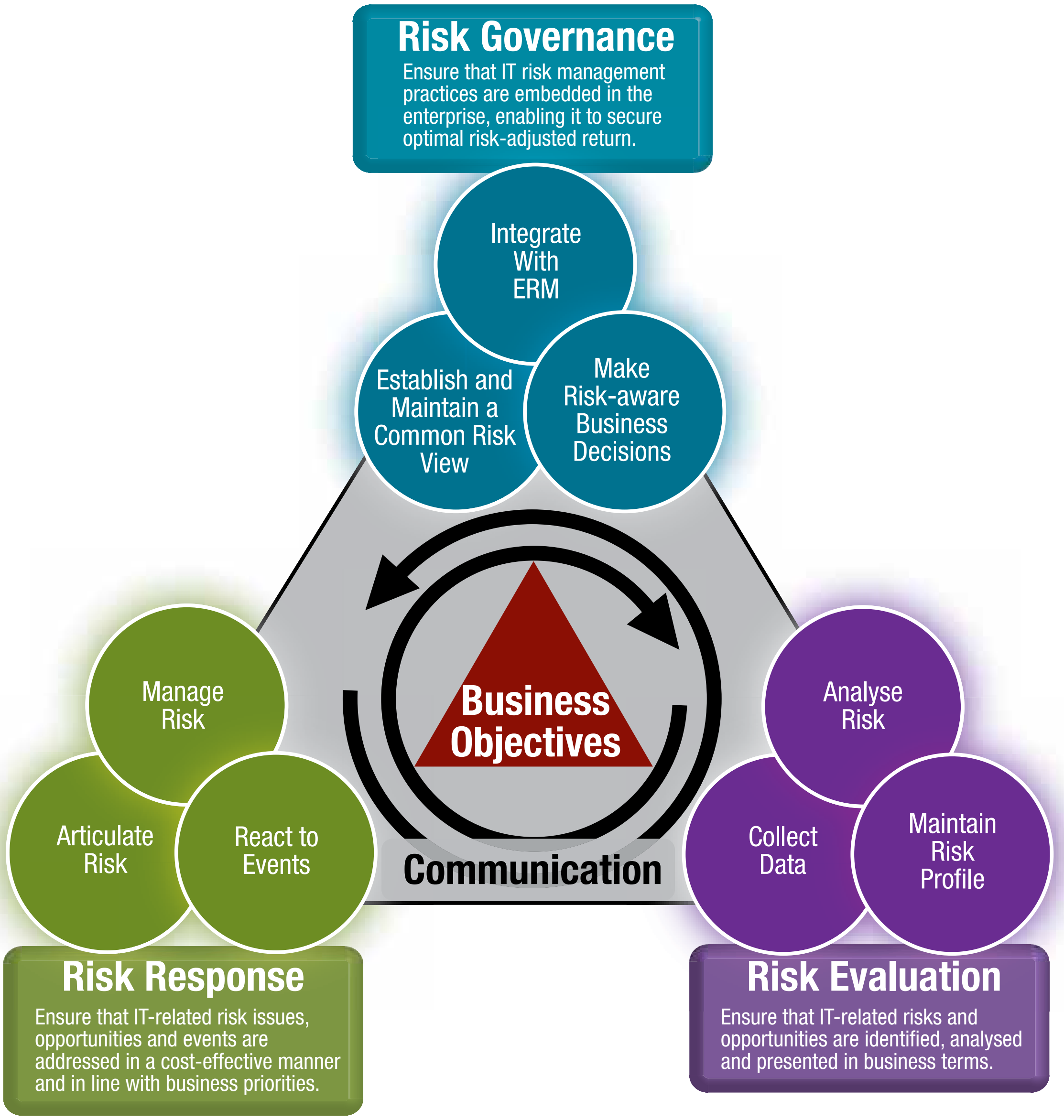
4. The Risk IT Framework

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


Risk Governance
Ensure that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return.
Integrate With ERM
Establish and Maintain a Common Risk View
Make Risk-aware Business Decisions
Business Objectives
Communication
Manage Risk
Articulate Risk
React to Events
Risk Response
Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities.
Analyse Risk
Collect Data
Maintain Risk Profile
Risk Evaluation
Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.

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

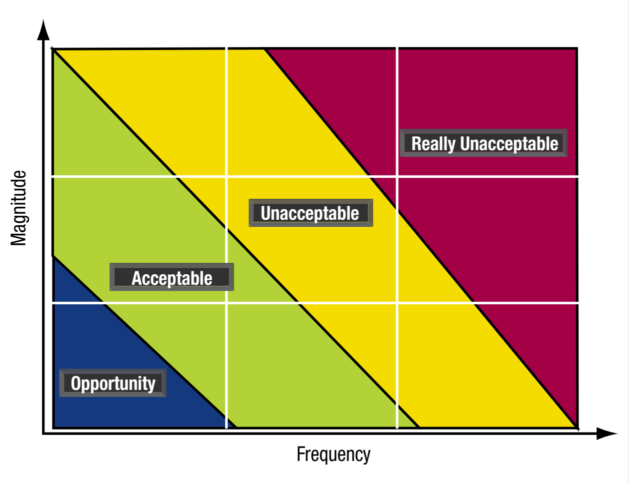
Risk appetite is the amount of risk an entity is prepared to accept when trying to achieve its objectives. When considering the risk appetite levels for the enterprise, two major factors are important:
- The enterprise's objective capacity to absorb loss, e.g., financial loss, reputation damage
- The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

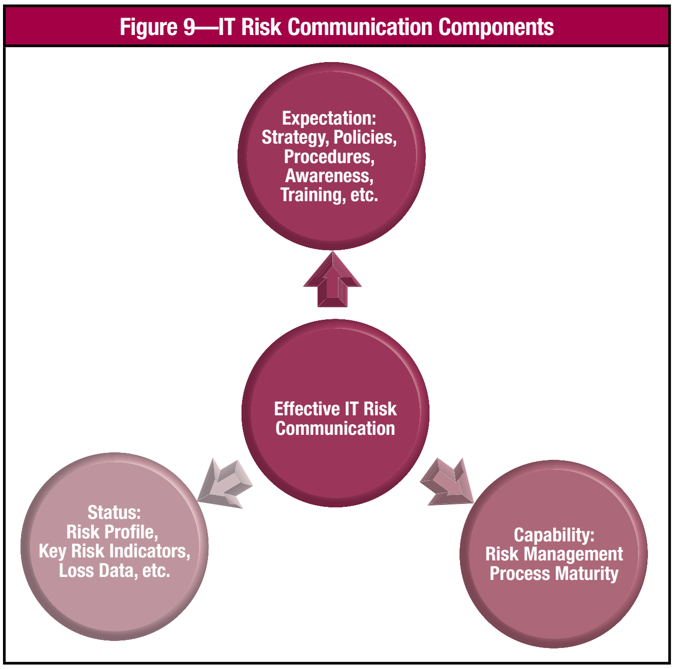
Figure 8—Responsibilities and Accountability for IT Risk Management

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


Expectation: Strategy, Policies, Procedures, Awareness, Training, etc.
Effective IT Risk Communication
Status: Risk Profile, Key Risk Indicators, Loss Data, etc.
Capability: Risk Management Process Maturity

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

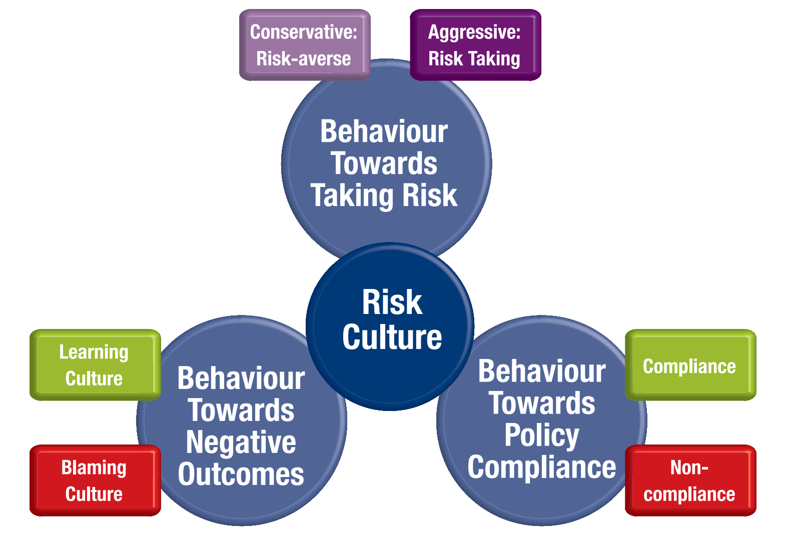
Input	Stakeholders	Output
• Executive summary IT risk reports • Current IT risk exposure/profile • KRIs	Executive management and board	• Enterprise appetite for IT risk • Key performance objectives • IT risk RACI charts • IT-related policies, expressing management's IT risk tolerance • Risk awareness 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

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**.

Figure 11—Elements of Risk Culture


Conservative: Risk-averse
Aggressive: Risk Taking
Behaviour Towards Taking Risk
Risk Culture
Learning Culture
Blaming Culture
Behaviour Towards Negative Outcomes
Behaviour Towards Policy Compliance
Compliance
Non-compliance

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

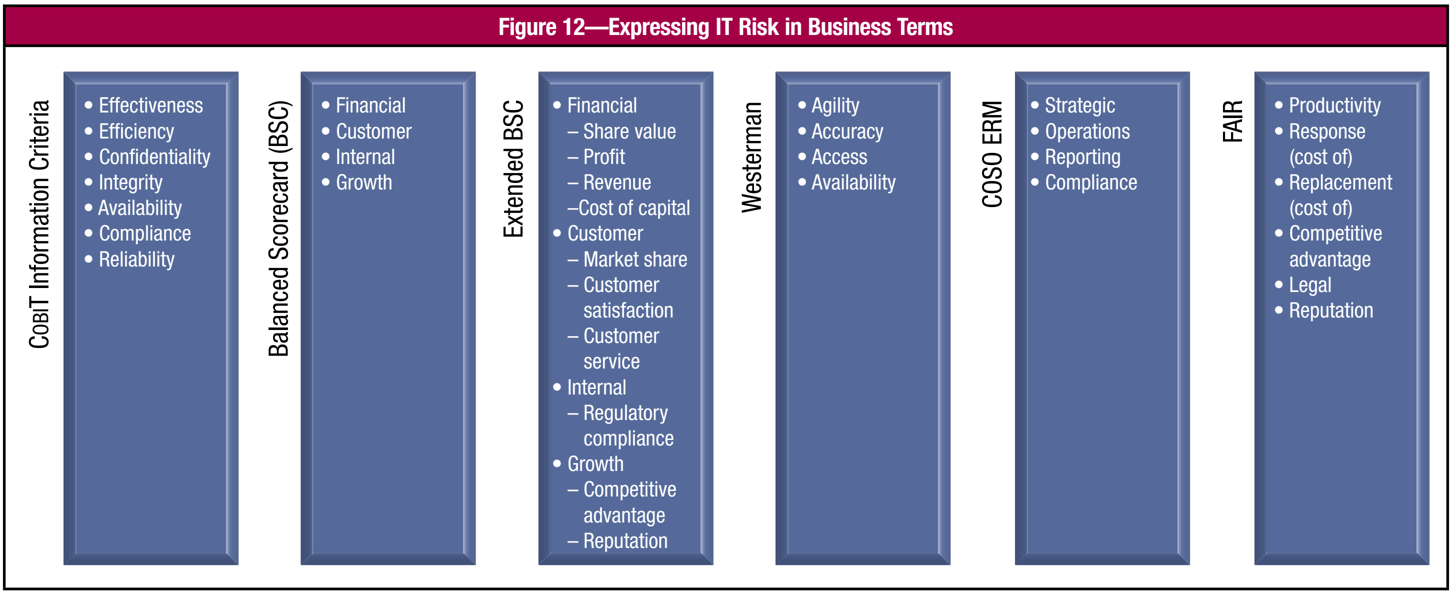
In this chapter a few essential components of the Risk Evaluation domain are discussed briefly. More information and practical guidance can be found in *The Risk IT Practitioner Guide*. The topics discussed here include:
- Describing business impact
- Risk scenarios

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	Balanced Scorecard (BSC)	Extended BSC	Westerman	COSO ERM	FAIR
• Effectiveness • Efficiency • Confidentiality • Integrity • Availability • Compliance • Reliability	• Financial • Customer • Internal • Growth	• Financial – Share value – Profit – Revenue –Cost of capital • Customer – Market share – Customer satisfaction – Customer service • Internal – Regulatory compliance • Growth – Competitive advantage – Reputation	• Agility • Accuracy • Access • Availability	• Strategic • Operations • Reporting • Compliance	• Productivity • Response (cost of) • Replacement (cost of) • Competitive advantage • Legal • Reputation

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

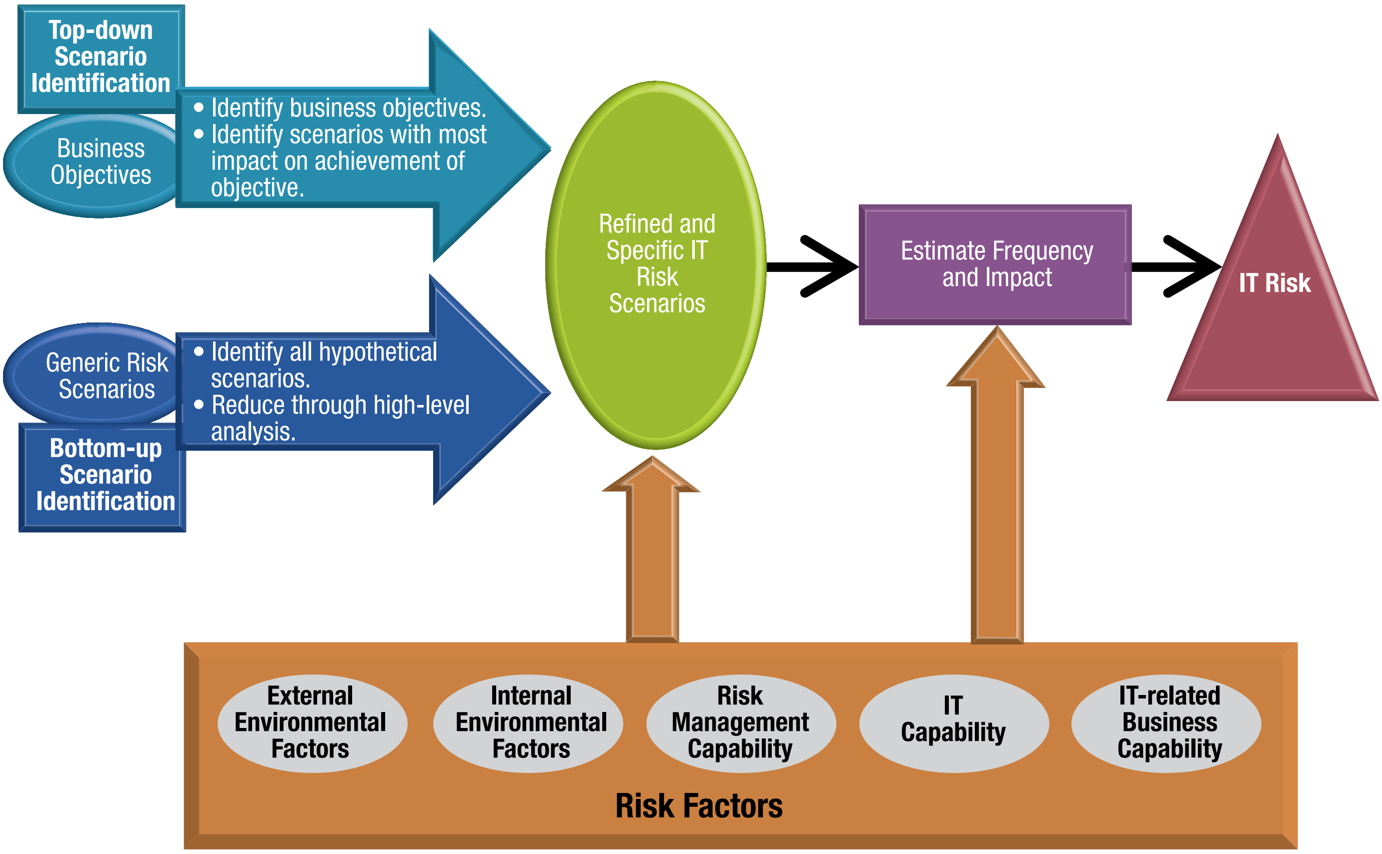
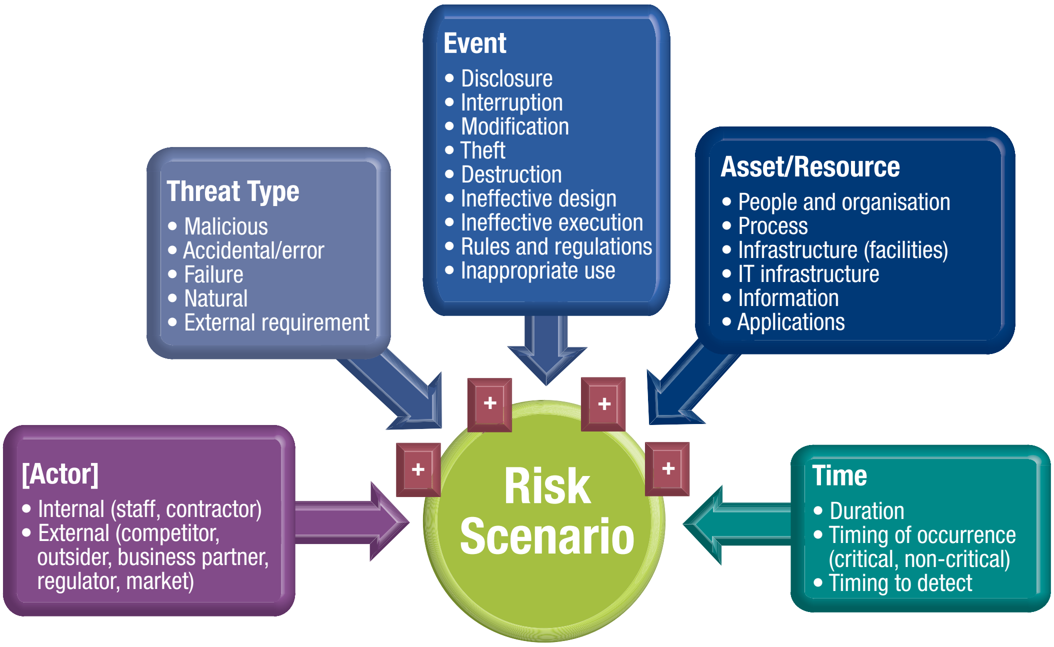

Top-down Scenario Identification
Business Objectives
• Identify business objectives.
• Identify scenarios with most impact on achievement of objective.
Generic Risk Scenarios
• Identify all hypothetical scenarios.
• Reduce through high-level analysis.
Bottom-up Scenario Identification
Refined and Specific IT Risk Scenarios
Estimate Frequency and Impact
IT Risk
External Environmental Factors
Internal Environmental Factors
Risk Management Capability
IT Capability
IT-related Business Capability
Risk Factors

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.

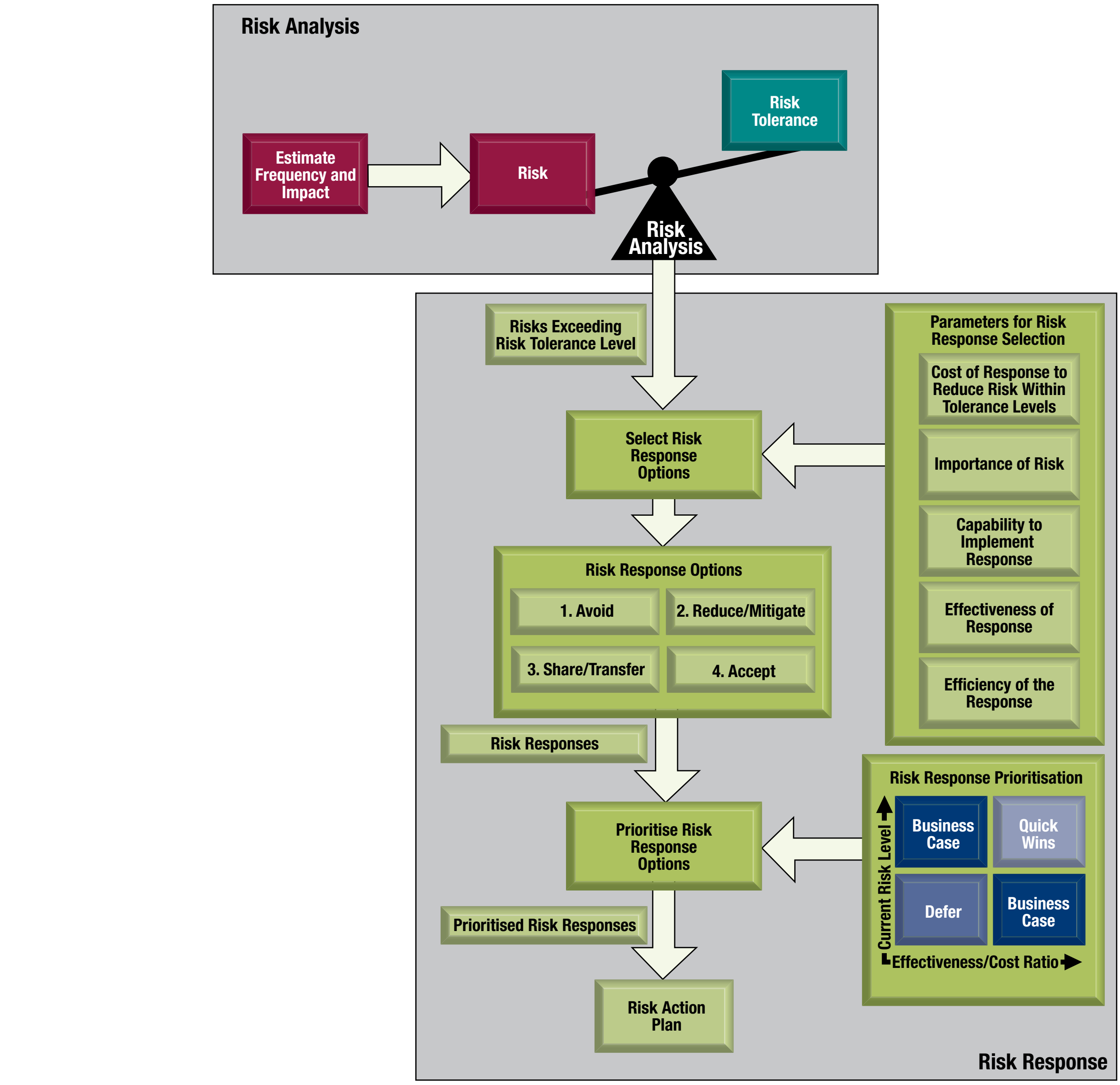
Risk Acceptance

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 Analysis
Estimate Frequency and Impact
Risk
Risk Tolerance
Risk Analysis
Risks Exceeding Risk Tolerance Level
Select Risk Response Options
Parameters for Risk Response Selection
Cost of Response to Reduce Risk Within Tolerance Levels
Importance of Risk
Capability to Implement Response
Effectiveness of Response
Efficiency of the Response
Risk Response Options
1. Avoid
2. Reduce/Mitigate
3. Share/Transfer
4. Accept
Risk Responses
Prioritise Risk Response Options
Risk Response Prioritisation
Business Case
Quick Wins
Defer
Business Case
Current Risk Level
Effectiveness/Cost Ratio
Prioritised Risk Responses
Risk Action Plan
Risk Response

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)

Pages 31 through 96 are contained in the full PDF, which is available at *www.isaca.org/riskitfw*

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

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