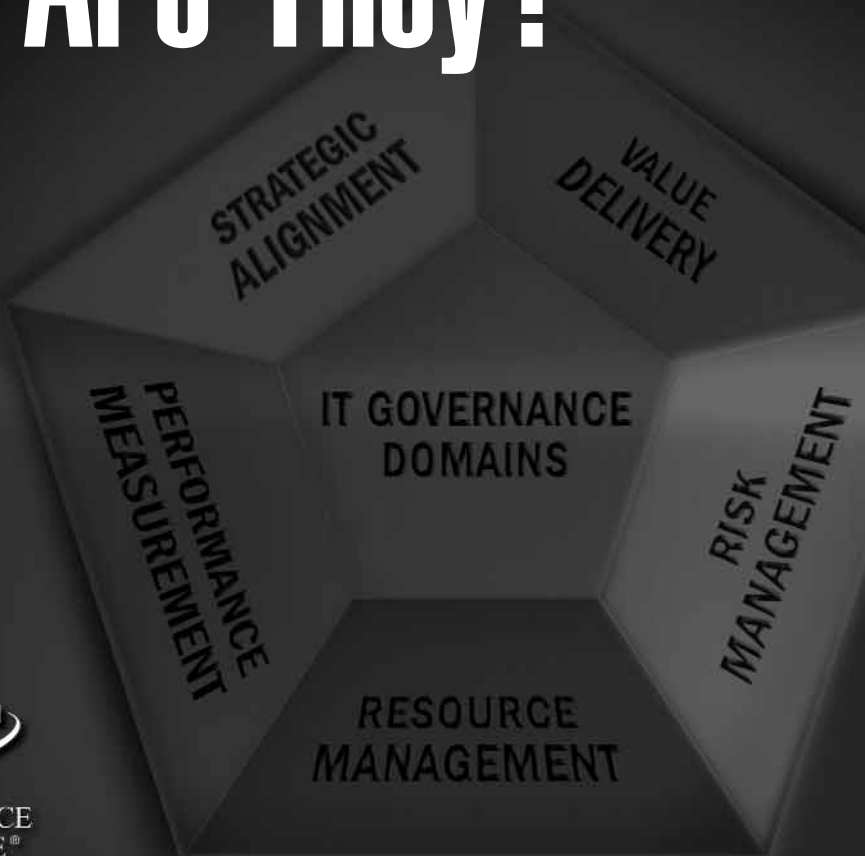


# Information Risks: Whose Business Are They?



**The IT Governance Institute\***

The IT Governance Institute (ITGI) ([www.itgi.org](http://www.itgi.org)) was established in 1998 to advance international thinking and standards in directing and controlling an enterprise's information technology. Effective IT governance helps ensure that IT supports business goals, optimises business investment in IT, and appropriately manages IT-related risks and opportunities. The IT Governance Institute offers original research, electronic resources and case studies to assist enterprise leaders and boards of directors in their IT governance responsibilities.

**Information Systems Audit and Control Association\***

With more than 47,000 members in more than 100 countries, the Information Systems Audit and Control Association (ISACA®) ([www.isaca.org](http://www.isaca.org)) is a recognised worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the *Information Systems Control Journal*®, develops international information systems auditing and control standards, and administers the globally respected Certified Information Systems Auditor™ (CISA®) designation, earned by more than 38,000 professionals since inception, and the Certified Information Security Manager® (CISM®) designation, a groundbreaking credential earned by 5,100 professionals in its first two years.

**Disclaimer**

IT Governance Institute (the "Owner") has designed and created this publication, titled *Information Risks: Whose Business Are They?* (the "Work"), primarily as an educational resource for chief information officers, senior management and IT management. The Owner makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of any 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, chief information officers, senior management and IT management should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

**Disclosure**

Copyright © 2005 by the IT Governance Institute. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system, or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise), without the prior written authorisation of the IT Governance Institute. Reproduction of selections of this publication, for internal and noncommercial or academic use only, is permitted and must include full attribution of the material's source. No other right or permission is granted with respect to this work.

**IT Governance Institute**

3701 Algonquin Road, Suite 1010  
Rolling Meadows, IL 60008 USA  
Phone: +1.847.253.7491  
Fax: +1.847.253.1443  
E-mail: [info@itgi.org](mailto:info@itgi.org)  
Web site: [www.itgi.org](http://www.itgi.org)

ISBN 1-933284-10-2

*Information Risks: Whose Business Are They?*

Printed in the United States of America

## Acknowledgements

### From the Publisher

#### The IT Governance Institute wishes to recognise:

##### The ITGI Board of Trustees

Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, International President  
 Abdul Hamid Bin Abdullah, CISA, CPA, Auditor General's Office, Singapore, Vice President  
 William C. Boni, CISM, Motorola, USA, Vice President  
 Ricardo Bria, CISA, SAFE Consulting Group, Spain, Vice President  
 Everett C. Johnson, Jr., CPA, Deloitte & Touche LLP (retired), USA, Vice President  
 Howard Nicholson, CISA, City of Salisbury, Australia, Vice President  
 Bent Poulsen, CISA, CISM, VP Securities Services, Denmark, Vice President  
 Frank Yam, CISA, FHKCS, CIA, CCP, CFE, CFSA, FFA, Focus Strategic Group Inc., Hong Kong,  
 Vice President  
 Robert S. Roussey, CPA, University of Southern California, USA, Past International President  
 Paul A. Williams, FCA, CITP, Paul Williams Consulting, UK, Past International President  
 Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi, USA, Trustee  
 Ronald Saull, CSP, Great-West Life and IGM Financial, Canada, Trustee  
 Erik Guldentops, CISA, CISM, Belgium, Advisor, IT Governance Institute

##### The Author and Researcher

Gary Hardy, IT Winners, South Africa  
 Lighthouse Global, UK

##### The IT Governance Institute Steering Committee

Tony Hayes, Queensland Government, Australia, Chair  
 Georges Ataya, CISA, CISM, CISSP, ICT Control sa-nv, Belgium  
 Reynaldo de la Fuente, CISA, CISM, DataSec SRL, Uruguay  
 Rupert Dodds, CISA, CISM, FCA, KPMG LLP, New Zealand  
 John Ho Chi, CISA, CISM, CBCP, CFE, Ernst & Young LLP, Singapore  
 Everett C. Johnson, CPA, Deloitte & Touche (retired), USA  
 Jean-Louis Leignel, MAGE Conseil, France  
 Akira Matsuo, CISA, CPA, ChoAoyama Audit Corp., Japan  
 Serge Yablonsky, CISA, CPA, SYC SA, France  
 Tom Wong, CISA, CIA, CMA, Ernst & Young LLP TSRS, Canada

##### The Reviewers

Steven De Haes, University of Antwerp Management, Belgium  
 Stacey Hamaker, CISA, Shamrock Technologies, USA  
 Austin Hutton, Shamrock Technologies, USA  
 Alan Simmonds, City Practitioners Ltd., UK  
 Wim Van Grembergen, Ph.D., University of Antwerp, Belgium  
 Paul A. Williams, FCA, CITP, Paul Williams Consulting, UK  
 Karen Worstell, CISM, Microsoft, USA

## Table of Contents

|   |    |
|---|----|
| ACKNOWLEDGEMENTS .....  | 3  |
| 1. EXECUTIVE SUMMARY .....                                    | 5  |
| 2. WHY IS INFORMATION RISK MANAGEMENT IMPORTANT?.....         | 7  |
| 3. WHAT ARE THE RISKS?.....                                   | 9  |
| 4. INFORMATION RISK MANAGEMENT BEST PRACTICES .....           | 13 |
| 5. WHO IS RESPONSIBLE FOR THE MANAGEMENT<br>OF IT RISKS?..... | 17 |
| 6. SUGGESTED ACTION PLAN .....                                | 20 |
| 7. SOURCES .....  | 23 |

Note: The publication is part of the IT Governance Domain Practices and Competencies Series from the IT Governance Institute. The titles include:

- *Information Risks: Whose Business Are They?*
- *Optimising Value Creation From IT Investments*
- *Measuring and Demonstrating the Value of IT*
- *Governance of Outsourcing*
- *IT Alignment—IT Strategy Committees*

## 1. Executive Summary

The management of risks is a cornerstone of IT governance, ensuring that the strategic objectives of the business are not jeopardised by IT failures. Risks associated with technology issues are increasingly evident on board agendas, as the impact on the business of an IT failure can have devastating consequences. Risk is, however, as much about failing to grasp an opportunity to use IT—for example, to improve competitive advantage or operating efficiency—as it is about doing something badly or incorrectly.

Managing IT risks and exercising proper governance are challenging experiences for business managers faced with technical complexity, dependence on an increasing number of service providers, and a limited supply of reliable risk-monitoring information.

Executives need guidance at a business level. What is the real impact on the business? What are the issues? How can I be sure that real and important risks are being addressed? When should IT risks be taken to enable business growth?

In 2004, the IT Governance Institute, in conjunction with Lighthouse Global, surveyed 200 IT professionals from 14 countries in the Americas, Asia/Pacific and Europe. The survey results show that in 80 percent of organisations, IT management, rather than the business, is responsible for defining IT risk impact (business units are responsible in only 37 percent of responding organisations), reflecting a lack of proper involvement in the risk assessment process by the business process owners. Executives should ensure that the business users define the business impact of an IT risk and agree and sign off on the risk position.

Fewer than one-quarter of the organisations surveyed review external risks and threats on a regular basis. This is worrying, given the use of outsourcing and service providers and the globalisation of businesses using IT.

Enterprises have recently demonstrated increasing interest in and adoption of best practices and standards for IT governance including, for example, ITGI's *Control Objectives for Information and related Technology* (COBIT®) framework, ISO 17799 for security and IT Infrastructure Library (ITIL) for service delivery. As these practices become adopted, it is reasonable to expect that an increasing number of risk assessments will be performed against them. In fact, many organisations, accounting firms and large IT consultancies are using assessments against best practices to encourage a greater interest in IT risks by senior executives.

**For IT governance to be effective, senior management should review and approve the risk action plan, agree to priorities and commit the necessary resources to execute the plan effectively.**

In only about one-third of the organisations surveyed by the ITGI does the board or CEO sign off on the IT risk management plan. For IT governance to be effective, senior management should review and approve the risk action plan, agree to priorities and commit the necessary resources to execute the plan effectively. Often it is the CIO who takes on this responsibility (40 percent of organisations surveyed), but this puts too much responsibility on the IT function and excludes other key stakeholders of the business.

The ITGI recommends that an IT executive committee with representation of all stakeholders review and approve the plan collectively on behalf of the board. Ultimately it is the business—the user of IT services—that must own business-related risks, including those related to use of IT. The business should set the mandate for risk management, provide the resources and funding to support a risk management plan designed to protect business interests, and monitor whether risks are being managed.

The ITGI also recommends that boards review the risk management approach for the most important IT-related risks on a regular basis, at least annually. Boards should be made aware of any significant unmitigated IT risks. The board should direct a consistent approach to the ownership of IT risk management by business and IT management ensuring that all stakeholders are properly involved.

## 2. Why Is Information Risk Management Important?

The management of risks is a cornerstone of IT governance, ensuring that the strategic objectives of the business are not jeopardised by IT failures. IT-related risks are increasingly a board-level issue as the impact on the business of an IT failure—be it an operational crash, security breach or failed project—can have devastating consequences.

Risk management itself is not a new topic and risk taking is an everyday part of managing an enterprise. However, understanding the risks relating to the use of information technology is still a challenge for business executives who probably do not have an in-depth appreciation of the technical issues. Technical complexity, misunderstanding of risks and a tendency for the media to overhype certain risks can result in some significant risks being overlooked and others receiving possibly too much emphasis. Ultimately, though, risk taking is an essential element of business today and success comes to those organisations that identify and manage risks most effectively. Risk is as much about failing to grasp an opportunity as it is about doing something badly or incorrectly.

Managing IT risks and exercising proper governance are therefore challenging experiences for business managers faced with technical complexity, dependence on an increasing number of service providers, and a limited supply of reliable risk-monitoring information.

The universal need to demonstrate good enterprise governance to shareholders and customers is the driver for increased risk management activities in large organisations. Enterprise risk comes in many varieties, not only financial. Regulators are specifically concerned about operational and systemic risk, within which technology risk and information security issues are prominent.

Recent years have seen heightened concern and focus on risk management. In 2001, COSO initiated a project to develop a framework<sup>1</sup> that would be readily usable by management to evaluate and improve the organizations' enterprise risk management (ERM). The period of the framework's development was marked by a series of high-profile business scandals and failures where investors, company personnel and other stakeholders suffered tremendous loss. In the aftermath were calls for enhanced corporate governance and risk management, with new laws, regulations and the listing of standards. The need for an ERM framework, providing key principles and concepts, a common language and clear direction and guidance, became even more compelling.

**The management of risks is a cornerstone of IT governance, ensuring that the strategic objectives of the business are not jeopardised by IT failures.**

<sup>1</sup> COSO, *Enterprise Risk Management Framework*, 2004

According to the COSO *ERM Framework*, enterprise risk management encompasses:

- Aligning risk appetite
- Enhancing risk response
- Reducing operational surprises
- Identifying and managing multiple and cross-enterprise risks
- Seizing opportunities
- Improving deployment of capital

These capabilities inherent in ERM help management achieve the entity's performance and profitability targets and prevent loss of resources. ERM helps ensure effective reporting and compliance with laws and regulations, and helps avoid damage to the entity's reputation and associated consequences. In summary, ERM helps an entity get to where it wants to go and avoid pitfalls and surprises along the way. Since IT plays such a significant part in most enterprise strategies and operations, IT risks are likely to be significant in the overall ERM approach.

Executives need guidance at a business level. What is the real impact on the business? What are the issues? How can one be sure that real and important risks are being addressed?

This executive briefing is based on research into these issues and considers:

- The areas where IT risk can occur
- Practical and real business impacts
- Good organisational practices for IT risk management—who is responsible for what
- The role senior management should play
- Techniques for minimising risk exposure

**ERM helps an entity get to where it wants to go and avoid pitfalls and surprises along the way.**

### 3. What Are the Risks?

There is no single accepted set of generic IT risk definitions, but these headings can be used as a guide:<sup>2</sup>

- Investment or expense risk—The risk that the investment being made in IT fails to provide value for money or is otherwise excessive or wasted. This includes consideration of the overall portfolio of IT investments.
- Access or security risk—The risk that confidential or otherwise sensitive information may be divulged or made available to those without appropriate authority. An aspect of this risk is privacy, the protection of personal data and information, which in many countries and regions is required by law to be addressed.
- Integrity risk—The risk that data cannot be relied on because they are unauthorised, incomplete or inaccurate
- Relevance risk—The risk associated with not getting the right information to the right persons (or process or systems) at the right time to allow the right action to be taken
- Availability risk—The risk of loss of service
- Infrastructure risk—The risk that an organisation does not have an information technology infrastructure and systems that can effectively support the current and future needs of the business in an efficient, cost-effective and well-controlled fashion (includes hardware, networks, software, people and processes)
- Project ownership risk—The risk of IT projects failing to meet objectives through lack of accountability and commitment

In 2004, the IT Governance Institute, in conjunction with Lighthouse Global, surveyed 200 IT professionals from 14 countries in the Americas, Asia/Pacific and Europe. The respondents included CIOs, IT directors and IT managers from companies with annual revenues in excess of US \$50 million. The respondents ranked the risks listed above in the following order [based on what was considered ‘very significant’ (relevance risk was not included)]:

1. Security risk—87 percent
2. Availability risk—85 percent
3. Infrastructure risk—81 percent
4. Integrity risk—81 percent
5. Project risk—72 percent
6. Investment risk—71 percent

---

<sup>2</sup> From a 2002 global study by *The Economist* Intelligence Unit

This confirms the general view in most IT organisations that security and availability are currently seen as the highest priority. Most business executives would agree that these are important. However, increasingly the business focus is on return on IT investment, and project and investments risks.

The ITGI survey respondents also ranked the threats that worry IT executives the most:

1. Attacks from outside—43 percent
2. Errors and mistakes—23 percent
3. Deliberate, from inside—15 percent
4. Physical damage—12 percent

This also reflects the current general view that security-related incidents are the most worrying threats. Indeed, these must not be underestimated, but a thorough examination of all risks by the business and its IT service providers would probably reveal a growing number of threats that exist within the customer and provider organisations themselves (such as errors, badly managed activities and poor communications between parties).

Significance of an IT risk is based on the combination of impact (what effect the risk would have on the organisation if it occurred) and likelihood (the probability of the risk occurring). Regular risk assessment is a key IT governance activity. However, to be effective, it should be driven by the business, which in particular should confirm the estimated impact.

Interestingly, the ITGI survey shows that in 80 percent of organisations, IT management, rather than the business, is responsible for defining IT risk impact (business units are responsible in only 37 percent of the responding organisations, reflecting a lack of proper involvement in the risk assessment process by the business process owners). Executives should ensure that the business users define the business impact of an IT risk and agree and sign off on the risk position.

The ITGI survey respondents ranked as follows the IT risk impact in terms of which are the most worrying to IT executives:

1. Loss of business revenue—34 percent
2. Financial loss—18 percent
3. Inability to meet business requirements—18 percent
4. Reputational damage—17 percent
5. Competitive disadvantage—8 percent
6. Problems with regulators—2 percent

**A thorough examination of all risks would probably reveal a growing number of threats that exist within the customer and provider organisations themselves.**

Increasingly, business executives are worrying about using IT for competitive advantage and, especially in certain sectors, the growing need to meet regulatory demands. Undoubtedly, IT executives will increasingly recognise these impacts as well, as boards place more and more emphasis on these issues.

ITGI recommends that to enable effective governance, IT risks should always be expressed in a business context rather than in the technical language favoured by IT risk experts. The following generic structure for expressing IT risks in any organisation is recommended, providing a framework for business management to be engaged in the risk management process:

***Business-specific risk*** (e.g., operational risk of orders not being received)

***Generic common IT risk*** (e.g., IT availability risk)

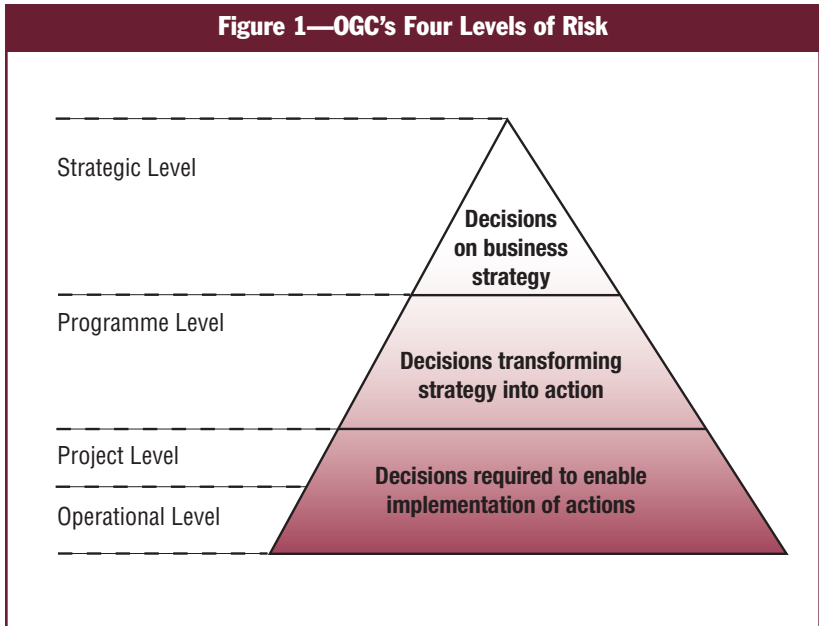
***Specific IT risk*** (e.g., denial-of-service attack on Internet customer order system)

Business risks are affected by the business environment (management style/culture; risk appetite; and industry sector factors such as competition, reputation, and national and international regulations) and, therefore, specific IT risks can be similarly affected. Thus, it is important to consider IT risks within the wider business context. It can be helpful to create enterprisewide IT risk definitions in business terms to ensure a common understanding.

Internationally, there are many published risk frameworks, most of which reflect that IT risks form part of a hierarchy of risks, with business strategic risks at the highest level. For example, the Office of Government Commerce (OGC, UK), in its Management of Risk (M\_o\_R) framework, has defined four levels of risk to help ensure that IT risks are considered by business executives from the strategy down to the operational level:

- Strategic—Risks to IT achieving its objectives, i.e., commercial, financial, political, environmental, directional, cultural, acquisition, quality, business continuity and growth
- Programme—Procurement/acquisition, funding, organisational, projects, security, safety and business continuity
- Project—People, technical, cost, schedule, resource, operational support, quality, provider failure and security
- Operational—People, technical, cost, schedule, resource, operational support, quality, provider failure, security, infrastructure failure business continuity and customer relations

The M\_o\_R framework visualises these four levels of risk in a pyramid, with appropriate escalations to higher levels for significant risks (**figure 1**).



For IT to be effectively governed, top management must be able to recognise and identify IT risks and ensure that significant risks are managed.

Because of the complexity and fast-changing nature of IT, education and awareness are essential to ensure that risks are recognised, not just at the top management level but at all levels throughout the organisation.

It is increasingly common for a dedicated risk management function to be established or for external advice to be obtained on a regular basis to ensure that risks are monitored and the rest of the organisation is kept informed. Maintenance of a risk catalogue or risk register can be helpful to ensure that a thorough review of all IT-related risk takes place on a periodic basis and for providing assurance to management that risks are being addressed.

## 4. Information Risk Management Best Practices

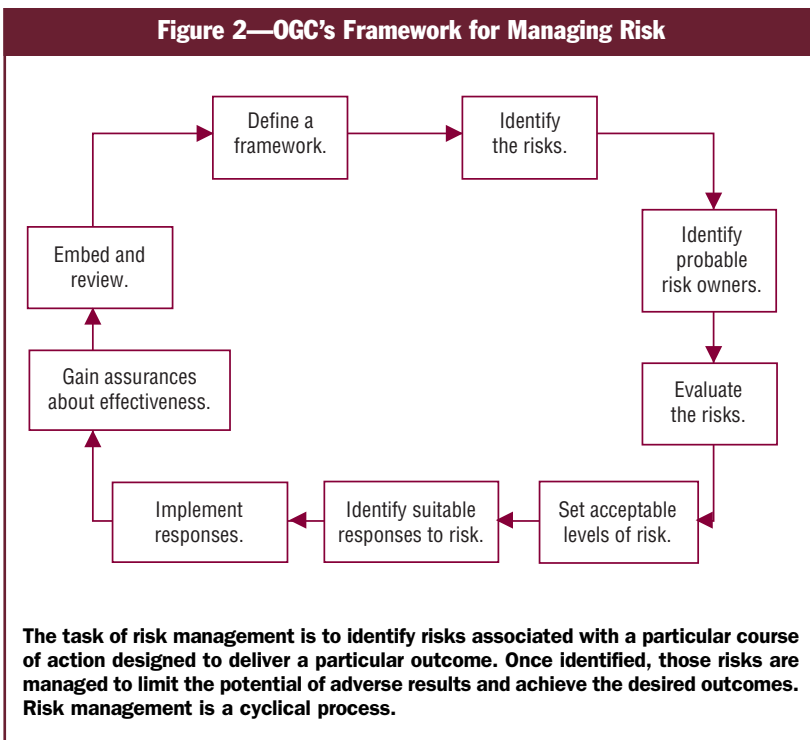
Risk management consists of two main elements:

- Risk analysis, which is concerned with gathering information about exposure to risk so the organisation can make appropriate decisions and manage risks appropriately
- Risk management, which requires processes to monitor risks, including adequate information about risks and the decision process supported by risk analysis, identification and evaluation

Once the enterprise has defined its risk appetite and identified its risk exposures, it can set strategies for managing risk and clarify responsibilities. Dependent on the type of risk and its significance to the business, management and the board may choose to:

- Mitigate, by implementing controls, e.g., acquire and deploy security technology to protect the IT infrastructure
- Transfer, by sharing risk with partners or transferring it to insurance coverage
- Accept, by formally acknowledging that the risk exists and monitoring it

The framework for managing risk depicted in **figure 2** is suggested by the OGC.<sup>3</sup>



<sup>3</sup> OGC, *Management of Risk*, [www.ogc.gov.uk](http://www.ogc.gov.uk)

The analysis of IT risks can be very time-consuming and there is a danger of ‘analysis paralysis’. To ensure effective and timely identification of risk, management workshops involving knowledgeable and interested representatives from the business, IT, audit and, if necessary, external advisors can help rapidly pinpoint key risks requiring attention and prioritise risk management actions. It is also important to identify the benefits of managing a risk as they can help justify the business case for taking action. Benefits can include financial savings, such as reduced losses and improved efficiencies, and intangibles such as improved reputation and image.

The ITGI survey shows that formal IT risk assessments are carried out by IT management in many areas:

1. IT projects—75 percent
2. Computer systems (applications)—74 percent
3. IT infrastructure—74 percent
4. IT processes—73 percent
5. Business projects—68 percent
6. People—63 percent
7. Business processes—60 percent
8. The enterprise’s systems’ connections with customers—57 percent
9. Information assets—55 percent
10. The enterprise’s systems’ connections with suppliers—51 percent

Note that it is the business side, external relationships and information itself that score at the lower end, probably because of insufficient involvement of business managers.

The survey shows that the following risk assessment techniques are the most popular:

1. Assessment of business impact—77 percent
2. Assessment of vulnerability—71 percent
3. Assessment of threat—64 percent
4. Assessment of probability/likelihood—64 percent
5. Assessment against documented controls—62 percent
6. Assessment against policies and standards—53 percent
7. Assessment against control objectives—51 percent

According to general research conducted by ITGI, enterprises have demonstrated an increasing interest in and adoption of best practices and standards for IT governance, including ITGI’s COBIT framework, ISO 17799 for security and ITIL for service delivery. As these practices are adopted, it is reasonable to expect that risk assessments will increasingly be performed against them, combined with assessments of business impact and likelihood. In fact, many organisations, accounting firms and large IT consultancies are using assessments against best practices to encourage a greater interest in IT risks by senior executives.

Risk management checklists are useful for raising awareness and reminding everyone of typical risk-related issues. Regular self-assessments, internal audits and external audits/assessments are also helpful to ensure objectivity and a thorough approach. For technical areas such as Internet security, the advice of an expert is likely to be required to ensure that any technical vulnerabilities have been identified.

The ITGI survey reveals that in only about one-third of the organisations surveyed does the board or CEO sign off on the IT risk management plan. For IT governance to be effective, senior management should review and approve the risk action plan, agree to priorities and commit the necessary resources to execute the plan effectively. Often it is the CIO who takes on this responsibility (40 percent of organisations surveyed), but this puts too much responsibility on the IT function and excludes other key stakeholders of the business. Instead, an IT executive committee with representation of all stakeholders is probably the most effective body to review and approve the plan collectively on behalf of the board.

The ITGI research asked the surveyed IT executives how well they think their organisations apply each of the following best practices, with the results depicted in **figure 3**.

**Figure 3—Organisations' Perceived Ability to Apply Best Practices**

| <b>Best Practice</b>  | <b>Very Well</b> | <b>Fairly Well</b> |
|---|------------------|--------------------|
| Senior management individuals' ownership of the risk management process                 | 28%              | 48%                |
| Clear communication of risk management policies to all staff                            | 21%              | 46%                |
| A framework for the management of risk  | 21%              | 49%                |
| An organisational culture that supports well-thought-through risk taking and innovation | 20%              | 47%                |
| The management of risk fully embedded in management processes and consistently applied  | 17%              | 45%                |
| Close linkage of risk management to the achievement of business objectives              | 23%              | 43%                |
| Assessment and management of risks associated with working with other organisations     | 20%              | 46%                |
| Active monitoring and regular reviewing of risks  | 23%              | 45%                |

As noted in the table, the results are broadly similar for all practices. Only about one-quarter or fewer of all IT executives think their organisations address these key practices very well and fewer than half believe they address it fairly well. It is probable that the business side (given its apparent insufficient involvement) would take an even more pessimistic view.

Virtually every organisation now relies on various third parties for IT services. As a result of that reliance, globalisation and the Internet, there are increasing international and national regulations and laws affecting the use of IT. It is interesting to see how well organisations consider risks from an external viewpoint. The ITGI survey shows that fewer than one-quarter of the organisations surveyed review external risks and threats on a regular basis:

- Weekly—10 percent
- Monthly—18 percent
- Every three months—24 percent
- Biannually—17 percent
- Annually—21 percent

If IT risks are to be properly considered by the board, reviews of external factors must be taken more seriously. ITGI recommends such reviews on at least a biannual basis.

**Fewer than one-quarter of the organisations surveyed review external risks and threats on a regular basis.**

## 5. Who Is Responsible for the Management of IT Risks?

Owning IT risks and giving direction for managing key risks are fundamental aspects of IT governance. An absence of top management responsibility and accountability for risk management can result in serious risks being ignored, potentially misguided actions and even the waste of costly investments.

The Institute of Risk Management (UK) recommends in its risk management standard the following responsibilities for boards:<sup>4</sup>

*The Board has responsibility for determining the strategic direction of the organisation and for creating the environment and the structures for risk management to operate effectively. This may be through an executive group, a non-executive committee, an audit committee or such other function that suits the organisation's way of operating and is capable of acting as a 'sponsor' for risk management. The Board should, as a minimum, consider, in evaluating its system of internal control:*

- *The nature and extent of downside risks acceptable for the company to bear within its particular business*
- *The likelihood of such risks becoming a reality*
- *How unacceptable risks should be managed*
- *The company's ability to minimise the probability and impact on the business*
- *The costs and benefits of the risk and control activity undertaken*
- *The effectiveness of the risk management process*
- *The risk implications of board decisions*

Ultimately it is the business—the user of IT services—that must own business-related risks, including those related to use of IT. The business should set the mandate for risk management, provide the resources and funding to support a risk management plan designed to protect business interests, and monitor whether risks are being managed. In practice, due to the complex and technical nature of IT, the IT service provider needs to provide guidance and work with business management to ensure that adequate safeguards are in place.

IT management then has a responsibility to endorse, establish and monitor the agreed risk management framework, including key principles and mitigation strategies. IT and user staff has a responsibility to implement the framework: assessing, escalating and delivering mitigating actions.

Auditors can provide initial momentum by highlighting to senior management inadequate risk management practices or specific risks that are not being adequately addressed. Auditors should align audits with key business risks and

---

<sup>4</sup> Institute of Risk Management, *The Risk Management Standard*, 2002, [www.theirm.org](http://www.theirm.org)

known areas of weakness. They should also provide independent assurance to management that appropriate risk management plans are in place and are being followed in all key areas, or make recommendations for improvement.

The OGC makes the following suggestions regarding risk ownership:

- Allocate responsibility for managing key risks at a senior level.
- Ensure that every risk has an owner. There may be separate owners for the actions to mitigate the risks.
- Ensure that anyone allocated ownership is aware of that ownership and has the authority to take on the responsibility.
- Adopt a mechanism for reporting issues, ultimately to the individual who has to retain overall responsibility.

The US National Institute of Standards and Technology (NIST) in its *Risk Management Guide*<sup>5</sup> states that the principal goal of an organisation's risk management process should be to protect the organisation and its ability to perform its mission, not just its IT assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organisation.

The ITGI's *Board Briefing on IT Governance, 2<sup>nd</sup> Edition*,<sup>6</sup> suggests the roles and responsibilities listed in **figure 4**.

| <b>Figure 4—Risk Management Roles and Responsibilities</b> |   |
|--|---|
| <b>Role</b>  | <b>Responsibility</b>   |
| Board of directors   | <ul style="list-style-type: none"> <li>• Be aware about IT risk exposures and their containment.</li> <li>• Evaluate the effectiveness of management's monitoring of IT risks.</li> </ul>   |
| IT strategy committee                                      | <ul style="list-style-type: none"> <li>• Provide high-level direction for sourcing and use of IT resources, e.g., strategic alliances.</li> <li>• Oversee the aggregate funding of IT at the enterprise level.</li> </ul>   |
| CEO  | <ul style="list-style-type: none"> <li>• Adopt a risk, control and governance framework.</li> <li>• Embed responsibilities for risk management in the organisation.</li> <li>• Monitor IT risk and accept residual IT risks.</li> </ul>   |
| Business executives  | <ul style="list-style-type: none"> <li>• Provide business impact assessments to the enterprise risk management process.</li> </ul>  |
| CIO  | <ul style="list-style-type: none"> <li>• Assess risks, mitigate efficiently and make risks transparent to the stakeholders.</li> <li>• Implement an IT control framework.</li> <li>• Ensure that roles critical for managing IT risks are appropriately defined and staffed.</li> </ul> |

<sup>5</sup> NIST, *Risk Management Guide for IT Systems*, Publication 800-30, USA

<sup>6</sup> IT Governance Institute, 2003, [www.itgi.org](http://www.itgi.org)

ITGI recommends that boards review the risk management approach for the most important IT-related risks on a regular basis, at least annually. Boards should be made aware of any significant unmitigated IT risks. The board should direct a consistent approach to the ownership of IT risk management by business and IT management, ensuring that all stakeholders are properly involved.

For risk management to be effective, individuals at all levels need to know:

***What is expected from me at a given level, and how do I contribute?***

## 6. Suggested Action Plan

There is no one approach to information risk management that will suit every organisation. However, there are proven principles and approaches that should be considered. For example, the following are some suggested ways to create an effective action plan from various international sources.

### *Setting Scope*

The Queensland Government of Australia's *Risk Management Best Practice Guide*<sup>7</sup> recommends that, to begin with, the boundary and scope of information risk management need to be clearly established in terms of:

- Identifying the business processes that rely on the integrity and availability of information for essential decisions
- Identifying and addressing the issues that need to be considered when assessing information security risks
- Identifying the information that needs to be protected and managed, and governance structures that need to be put in place for this information

### *Implementation Steps*

The *Risk Management Best Practice Guide* suggests the following key implementation steps:

1. Develop a project plan.
2. Identify major areas of responsibility/impact.
3. Develop a checklist of the minimum requirements for each mandatory control area.
4. Conduct workshops/meetings with representatives of the areas of responsibility/impact identified in step 2 to:
  - Identify the minimum controls in place
  - Identify the minimum controls not in place, and assess possible impacts and likelihoods
  - Determine the level of risk for those controls not in place
  - Prioritise and develop a time frame for implementing missing key controls
5. Plan and implement controls to cover the missing areas that expose the organisation to a high level of risk.
6. Implement remaining controls of lesser impact, and conduct a detailed assessment of the IT environment.
7. Implement ongoing risk management.

The Information Security Forum<sup>8</sup> recommends the following risk management steps:

1. Create a risk management structure covering the entire organisation, with clearly defined roles and responsibilities.

---

<sup>7</sup> [www.governmentict.qld.gov.au/02\\_infostand/standards.htm#bpg](http://www.governmentict.qld.gov.au/02_infostand/standards.htm#bpg)

<sup>8</sup> Information Security Forum (ISF), [www.securityforum.org](http://www.securityforum.org)

2. Create and follow a risk assessment process that is consistent across all risks and the organisation to identify and evaluate key risks.
3. Develop and implement policies, standards and procedures to ensure that all identified risks are managed within the organisation's risk appetite.
4. Regularly monitor the risk management processes and the corrective actions.
5. Regularly present risk reports to the board, and invite feedback into the risk processes.
6. Communicate appropriate risk information to the organisation's stakeholders.

### ***Critical Success Factors***

The OGC recommends the following useful critical success factors for management of IT risk:

- Nominate senior management individuals to support, own and lead the risk management process.
- Clearly communicate to all staff the risk management policies and the benefits of following them.
- Ensure the existence and adoption of a framework for risk management that is transparent and repeatable.
- Ensure the existence of an organisational culture that supports well-thought-through risk taking and innovation.
- Ensure that risk management is fully embedded in management processes and consistently applied.
- Closely link risk management to achievement of objectives.
- Explicitly assess and manage risks associated with working with other organisations.
- Actively monitor and regularly review risks on a constructive, 'no-blame' basis.

ITGI provides the following list of best practices to help ensure that IT risks are managed effectively:

- Embed into the enterprise an IT governance structure that is accountable, effective and transparent, with defined activities and purposes and unambiguous responsibilities.
- Establish an audit committee that considers what the significant risks are; assesses how they are identified, evaluated and managed; commissions IT and security audits; and rigorously follows up closure of subsequent recommendations.
- Appoint and oversee an internal audit function with a direct reporting line to the chief executive and the audit committee, and possibly an independent external auditor as well as other third-party reviewers.
- Coordinate and review charters, budgets and plans using risk-based planning, scope, coverage and quality of work of IT auditors and other providers of IT assurance.

- Define the scope and charter of the audit committee, ensuring that for these external audit requirements—securing annual opinion letters, management control assertions and compliance letters—the committee also covers IT and security risks.
- Monitor how management determines what IT resources are needed to achieve strategic objectives.
- Pay special attention to IT control failures and weaknesses in internal control and their actual and potential impact, while considering whether management acts promptly on them and whether more monitoring is required.
- Evaluate the scope and quality of management’s ongoing monitoring of IT risks and controls.
- Develop a process for making the return vs. risk balance explicit and measurable while accepting a balanced failure/success ratio in the portfolio of innovation projects.
- Ask the right questions. (Nonexecutive board members do not need to know the answers; they need to know the questions.)
- Understand the answers to the questions in order to ask appropriate follow-ups and to understand the implications for the enterprise.
- Ascertain that risk analysis is part of management’s strategic planning process and considers the vulnerabilities of the IT infrastructure and the exposure of intangible assets.

## 7. Sources

COSO, *Enterprise Risk Management Framework*, 2004

The Economist Intelligence Unit, *Global Study on Information Risk Management*, 2002

Information Security Forum, *Corporate Governance Requirements for Information Risk Management*, UK

Institute for Risk Management, *Risk Management Standard*, UK

IT Governance Institute, *Board Briefing on IT Governance, 2<sup>nd</sup> Edition*, USA, 2003, [www.itgi.org](http://www.itgi.org)

IT Governance Special Interest Group, *Briefing on IT Risk Management*, IMPACT Programme, UK

NIST, *Risk Management Guide for IT Systems*, Publication 800-30, USA

Office of Government Commerce, *Management of Risk: Guidance for Practitioners (M\_o\_R)*, UK

Queensland (Australia) Government, *Information Risk Management Best Practices Guide*, Australia