Information Security Governance:

Guidance for Boards of Directors and Executive Management

2nd Edition

GOVERNANCE INSTITUTE®

LEADING THE IT GOVERNANCE COMMUNITY

Information Security Governance:

Guidance for Boards of Directors and Executive Management

2nd Edition

"The rising tide of cybercrime and threats to critical information assets mandate that boards of directors and senior executives are fully engaged at the governance level to ensure the security and integrity of those resources."

— Shirley M. Hufstedler, Board of Directors
Harman International Industries

"To enable secure business operations, an organization must have an effective security governance strategy."

— Sunil Misra, Chief Security Advisor and Managing Partner
Unisys Corp.

"The complexity and criticality of information security and its governance demand that it be elevated to the highest organizational levels. As a critical resource, information must be treated like any other asset essential to the survival and success of the organization."

— Terry Hancock, CEO
Easy I Group

IT Governance Institute®
Leading the IT Governance Community

IT Governance Institute®

The IT Governance Institute (ITGI™) (*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.

Disclaimer

The IT Governance Institute (the "Owner") has designed and created this publication, titled *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition* (the "Work"), primarily as an educational resource for boards of directors, executive management and IT security professionals. 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, boards of directors, executive management and IT security professionals should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

Disclosure

Copyright © 2006 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*
Web site: *www.itgi.org*

ISBN 1-933284-29-3
Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition
Printed in the United States of America

Acknowledgements

From the Publisher

The IT Governance Institute wishes to recognise:

The ITGI Board of Trustees
Everett C. Johnson, CPA, Deloitte & Touche LLP (retired), USA, International President
Abdul Hamid Bin Abdullah, CISA, CPA, Auditor General's Office, Singapore, Vice President
William C. Boni, CISM, Motorola, USA, Vice President
Jean-Louis Leignel, MAGE Conseil, France, Vice President
Lucio Augusto Molina Focazzio, CISA, Colombia, Vice President
Howard Nicholson, CISA, City of Salisbury, Australia, Vice President
Bent Poulsen, CISA, CISM, VP Securities Services, Denmark, Vice President
Frank Yam, CISA, CIA, CCP, CFE, CFSA, FFA, FHKCS, Focus Strategic Group, Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President
Robert S. Roussey, CPA, University of Southern California, USA, 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 Focus Group
W. Krag Brotby, CISM, Senior Security Consultant, USA, Author
Jennifer Bayuk, CISA, CISM, Bear Stearns & Co. Inc., USA
Curtis Coleman, CISM, CISSP, MSIA, Seagate Technology LLC, USA
Leonardo Garcia, CISA, CISM, CISSP, BS 7799LA, ISO 9000LA, Innovaciones Telemáticas, México
Ronda R. Henning, CISM, CISSP-ISSAP, CISSP-ISSMP, Harris Corporation, USA
Stephen R. Katz, CISSP, Security Risk Solutions LLC, USA
William Malik, CISA, Malik Consulting LLC, USA
Yogita Parulekar, CISA, CISM, CA, Oracle Corporation, USA
Eddie Schwartz, CISA, CISM, CISSP, MCSE, Securevision LLC, USA
Darlene Tester, CISM, CISSP, JD, CHSS, Caveo Technology, USA
Marc Vael, Ph.D., CISA, CISM, KPMG, Belgium

ISACA's Certified Information Security Manager® (CISM®) Board
David Simpson, CISA, CISM, CISSP, Chair, CQR Consulting, Australia
Kent Anderson, CISM, Network Risk Management LLC, USA
Evelyn Anton, CISA, CISM, UTE, Uruguay
Claudio Cilli, CISA, CISM, CIA, CISSP, Tangerine Consulting, Italy
Robert Coles, Ph.D., CISA, CISM, MBCS, UK
Kyeong-Hee Oh, CISA, CISM, CISSP, Green Soft, Korea
Hitoshi Ota, CISA, CISM, Mizuho Corporate Bank Ltd., Japan
Ashok Pawar, CISA, CISM, CAIIB, State Bank of India, India
Gary Swindon, CISM, Orlando Regional Healthcare, USA

The ITGI Committee
William C. Boni, CISM, Chair, Motorola, USA
Jean-Louis Leignel, Vice Chair, MAGE Conseil, France
Erik Guldentops, CISA, CISM, Belgium
Tony Hayes, Queensland Government, Australia
Anil Jogani, CISA, FCA, Tally Solutions Ltd., UK
John W. Lainhart IV, CISA, CISM, IBM Business Consulting Services, USA
Ron Saull, CSP, Great-West Life and IGM Financial, Canada
Michael Schirmbrand, CISA, CISM, CPA, KPMG LLP, Austria
Eddy Schuermans, CISA, PricewaterhouseCoopers LLP, Belgium

The Subject Matter Expert Reviewers
Julia Allen, Carnegie-Mellon, USA
William Barrett, CISA, CPA, CRP, Ernst & Young LLP, USA
Endre P. Bihari, CISM, CCSA, GAICD, MCSE, Performance Resources, Australia
Chris Boswell, CISA, CISSP, CA, USA
Claudio Cilli, CISA, CISM, CIA, CISSP, Tangerine Consulting, Italy
Candi Carrera, Tellindus, Luxembourg
Ulises Castillo, CISA, Scitum, SA de CV, Mexico
Milthon J. Chavez, CISA, CISM, CIFI, MCH Consultoria Integral, Venezuela
Amitava Dutta, Ph.D., CISA, George Mason University, USA
Chris Ekonomidis, CISA, CISSP, Ernst & Young LLP, USA
Lawrence A. Gordon, Ph.D., University of Maryland, USA
Erik Guldentops, CISA, CISM, Belgium
Gary Hardy, ITWinners, South Africa
Avinash W. Kadam, CISA, CISM, CISSP, CBCP, MIEL e-Security Pvt. Ltd., India
John W. Lainhart IV, CISA, CISM, IBM Business Consulting Services, USA
Alexandra Lajoux, National Association of Corporate Directors, USA
Cory Notrica, CISA, CISM, CISSP, Ernst & Young LLP, USA
Vernon R. Poole, CISM, IPFA, Sapphire Technologies, UK
N. Ramu, CISA, FCA, Lovelock & Lewes, India
Robert S. Roussey, CPA, University of Southern California, USA
Howard A. Schmidt, CISM, CISSP, Former Chief Security Executive, eBay and Microsoft, USA
Gad J. Selig, Ph.D., PMP, University of Bridgeport and GPS Group Inc., USA
Dirk Steuperaert, CISA, PricewaterhouseCoopers, Belgium
Johann Tello-Meryk, CISA, CISM, Primer Banco del Istmo, Panama
Ghassan Youssef, MSc., CISM, Bank Audi, Audi Saradar Group, Lebanon

The ITGI Affiliates and Sponsors
ISACA chapters
Commonwealth Association of Corporate Governance
Bindview Corporation
CA

ITGI WOULD LIKE TO ACKNOWLEDGE:

Unisys, whose generous support and sponsorship contributed significantly to the development of the *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*.

UNISYS

ITGI appreciates the support the following organisations have provided to this project:

AICPA®

THE CENTER FOR INTERNET SECURITY

KPMG

NACD
NATIONAL ASSOCIATION OF CORPORATE DIRECTORS

PRICEWATERHOUSECOOPERS

SANS INSTITUTE

Table of Contents

Introduction 7

1. What Is Information Security Governance?—An Overview 11
Desired Outcomes 11
Knowledge and the Protection of Information Assets 12
Benefits of Information Security Governance 13
Process Integration 14

2. Why Are Information Security and Information Security Governance Important? 15
Information Security Governance Defined 17

3. Who Should Be Concerned With Information Security Governance? 21
Boards of Directors/Trustees 21
Executives 21
Steering Committee 22
Chief Information Security Officer 22

4. What Should the Board of Directors/Trustees and Senior Executives Be Doing? 24
Illustrative Matrix of Outcomes and Directives 25

5. What Are Some Thought–provoking Questions to Ask? 27
Questions to Uncover Information Security Issues 27
Questions to Find Out How Management Addresses Information Security Issues 27
Questions to Self-assess Information Security Governance Practices 28

6. What Should Information Security Governance Deliver? 29
Strategic Alignment 29
Risk Management 29
Resource Management 30
Performance Measurement 30
Value Delivery 30

7. How Is Information Security Governance Evolving? 32

8. What Can Be Done to Successfully Implement Information Security Governance? 34
Questions for Directors 34
Questions for Management 34

9. How Does My Organisation Compare on Information Security Governance? 36
Maturity Level Description 36

Appendix—Regulatory and Standards Bodies' Guidance on Information Security Governance 40

References 46

Introduction

Organisations today face a global revolution in governance that directly affects their information management practices. There is an increased need to focus on the overall value of information protected and delivered—in terms of enabled services. Due to the high-profile organisational failures of the past decade, legislatures, statutory authorities and regulators have created a complex array of new laws and regulations designed to force improvement in organisational governance, security, controls and transparency. Previous and new laws on information retention and privacy, coupled with significant threats of information systems disruptions from hackers, worms, viruses and terrorists, have resulted in a need for a governance approach to information management, protecting the organisation's most critical assets—its information and reputation.

Information and the systems that handle it are critical to the operation of virtually all organisations. Access to reliable information has become an indispensable component of conducting business; indeed, in a growing number of organisations, information **is** the business.

This increasing dependence on information was apparent more than a decade ago when Peter Drucker stated:

> *The diffusion of technology and the commodification of information transforms the role of information into a resource equal in importance to the traditionally important resources of land, labor and capital.*[1]

During the intervening years, value escalation of and dependence on information have increased exponentially. There is every indication that this quickening pace will continue unabated into the foreseeable future. Gartner recently estimated that in less than a decade, organisations will typically deal with 30 times more information than they do today.[2] With the chaos, glaring vulnerabilities and perpetual crisis-mode activities observed in most information technology operations, that is not a reassuring notion.

Organisations continue to witness information-related crime and vandalism becoming the choice of a growing global criminal element. Existing institutions burdened by countless conflicting jurisdictions and inadequate resources have not been successful in reducing the amount or impact of these activities. Therefore, a large portion of the task of protecting critical information resources falls squarely on the shoulders of executives and boards of directors.

---

[1] Drucker, Peter; 'Management Challenges for the 21st Century', *Harpers Business*, 1993

[2] Hallawell, Arabella; *Gartner Global Security and Privacy Best Practices*, Gartner Analyst Reports, USA, 2004, *www.csoonline.com/analyst/report2332.html*

Until recently, the focus of security had been on protecting the IT systems that process and store the vast majority of information, rather than on the information itself. However, this approach is too narrow to accomplish the level of integration, process assurance and overall protection that is now required.

To achieve effectiveness and sustainability in today's complex, interconnected world, information security must be addressed at the highest levels of the organisation, not regarded as a technical specialty relegated to the IT department.

An enlightened approach to information security takes the larger view that an organisation's information and the knowledge based on it must be adequately protected regardless how it is handled, processed, transported or stored. It addresses the universe of risks, benefits and processes involved with all information resources. The security of information, as with other critical organisational resources, must be addressed at the total enterprise level.

Information security is not only a technical issue, but a business and governance challenge that involves adequate risk management, reporting and accountability. Effective security requires the active involvement of executives to assess emerging threats and the organisation's response to them.[3]

As organisations strive to remain competitive in the global economy, they respond to constant pressures to cut costs through automation, which often requires deploying more information systems. Whilst managers become ever more dependent on these systems, the systems have become vulnerable to a widening array of risks that can threaten the existence of the enterprise. This combination is forcing management to face difficult decisions about how to effectively address information security. This is in addition to scores of new and existing laws and regulations that demand compliance and higher levels of accountability.

The Data Governance Council, with a focus on the review and approval aspects of board responsibilities, recently recommended that boards provide strategic oversight regarding information security, including:

1. Understanding the criticality of information and information security to the organisation
2. Reviewing investment in information security for alignment with the organisation strategy and risk profile
3. Endorsing the development and implementation of a comprehensive information security programme

[3] Corporate Governance Task Force, 'Information Security Governance: Call to Action', USA, 2004

4. Requiring regular reports from management on the programme's adequacy and effectiveness[4]

In this regard, governing boards and executive management should review:
- The scale and return of the current and future investments in information resources to ensure that they are optimised
- The potential for technologies to dramatically change organisations and business practices, thereby creating new opportunities and value whilst reducing costs

They should also consider the associated ramifications of the:
- Increasing dependence on information and the systems and communications that deliver the information
- Dependence on entities beyond the direct control of the enterprise
- Increasing demands to share information with partners, suppliers and customers
- Impact on reputation and enterprise value resulting from information security failures
- Failure to set the tone at the top with regard to the importance of security

Whilst executive management has the responsibility to consider and respond to these issues, boards of directors will increasingly be expected to make information security an intrinsic part of the enterprise's governance efforts, aligned with their IT governance focus and integrated with processes they have in place to govern other critical functions. The purpose of this publication is to provide boards and senior executives a basis, rationale and acknowledged approach for protecting vital information assets that support critical business processes.

This guide, prepared by one of the world's leading institutions dedicated to researching issues and principles of IT governance, is written to address these concerns. It covers fundamental issues such as:
- What is information security governance?
- Why is it important?
- Who is responsible for it?

It also provides practical, pragmatic advice on:
- What information security governance should deliver
- Questions to ask regarding information security governance
- How information security governance is evolving
- How to measure an organisation's maturity level relative to information security governance

[4] IBM, *Data Governance Council, Oversight of Information Security*, USA, 2005

1. What Is Information Security Governance?—An Overview

Information security governance is the responsibility of the board of directors and senior executives. It must be an integral and transparent part of enterprise governance and be aligned with the IT governance framework. Whilst senior executives have the responsibility to consider and respond to the concerns and sensitivities raised by information security, boards of directors will increasingly be expected to make information security an intrinsic part of governance, integrated with processes they already have in place to govern other critical organisational resources.

To exercise effective enterprise and information security governance, boards and senior executives must have a clear understanding of what to expect from their enterprise's information security programme. They need to know how to direct the implementation of an information security programme, how to evaluate their own status with regard to an existing security programme and how to decide the strategy and objectives of an effective security programme.

Governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly.[5]

Whilst there are many aspects to information security governance, there are several matters that can assist in focusing on the question, 'What is information security governance?'. These are the:

- Desired outcomes of information security governance
- Knowledge and protection of information assets
- Benefits of information security governance
- Process integration

Desired Outcomes

Information security governance consists of the leadership, organisational structures and processes that safeguard information. Critical to the success of these structures and processes is effective communication amongst all parties based on constructive relationships, a common language and shared commitment to addressing the issues. The five basic outcomes of information security governance should include:

1. Strategic alignment of information security with business strategy to support organisational objectives
2. Risk management by executing appropriate measures to manage and mitigate risks and reduce potential impacts on information resources to an acceptable level
3. Resource management by utilising information security knowledge and infrastructure efficiently and effectively

[5] IT Governance Institute, *Board Briefing on IT Governance, 2nd Edition*, USA, 2003, *www.itgi.org*. The Chartered Institute of Management Accountants (CIMA) and the International Federation of Accountants (IFAC) also adopted this definition in 2004.

4. Performance measurement by measuring, monitoring and reporting information security governance metrics to ensure that organisational objectives are achieved
5. Value delivery by optimising information security investments in support of organisational objectives

The National Association of Corporate Directors (NACD), the leading membership organisation for boards and directors in the US, recognises the importance of information security. It recommends four essential practices for boards of directors, as well as several specific practices for each point. The four practices, which are based on the practicalities of how boards operate, are:[6]

- Place information security on the board's agenda.
- Identify information security leaders, hold them accountable and ensure support for them.
- Ensure the effectiveness of the corporation's information security policy through review and approval.
- Assign information security to a key committee and ensure adequate support for that committee.

Knowledge is fast becoming the sole factor of productivity, sidelining both capital and labor.[7]

Knowledge and the Protection of Information Assets

Data are the raw materials of information. Data by themselves are useless until they are organised or manipulated in such a way that they provide information. Information has been defined as data with meaning, relevance and purpose. Clearly, absent these attributes, there can be little justification for expending resources to protect it or, for that matter, retain it. Information is the basis for knowledge. Putting information together in such a way that it can be used to accomplish something useful is knowledge. Knowledge is created from information. Knowledge is, in turn, captured, transported and stored as organised information.

Information and the knowledge based on it have increasingly become recognised as information assets, i.e., a business-critical asset, without which most organisations would simply cease to function. It is a business enabler, requiring organisations to provide adequate protection for this vital resource. But to achieve effectiveness and sustainability in today's complex, interconnected world, security over information assets must be addressed at the highest levels of the organisation, not regarded as a technical specialty relegated to the IT department.

[6] National Association of Corporate Directors, 'Information Security Oversight: Essential Board Practices', USA, 2001
[7] *Op. cit.,* Drucker

Governing for enterprise security means viewing adequate security as a non-negotiable requirement of being in business. If an organisation's management—including boards of directors, senior executives and all managers—does not establish and reinforce the business need for effective enterprise security, the organisation's desired state of security will not be articulated, achieved or sustained. To achieve a sustainable capability, organisations must make enterprise security the responsibility of leaders at a governance level, not of other organisational roles that lack the authority, accountability and resources to act and enforce compliance.[8]

Benefits of Information Security Governance

Information security governance generates significant benefits, including:

- An increase in share value for organisations that practice good governance
- Increased predictability and reduced uncertainty of business operations by lowering information security-related risks to definable and acceptable levels
- Protection from the increasing potential for civil or legal liability as a result of information inaccuracy or the absence of due care
- The structure and framework to optimise allocation of limited security resources
- Assurance of effective information security policy and policy compliance
- A firm foundation for efficient and effective risk management, process improvement, and rapid incident response related to securing information
- A level of assurance that critical decisions are not based on faulty information
- Accountability for safeguarding information during critical business activities, such as mergers and acquisitions, business process recovery, and regulatory response

The benefits add significant value to the organisation by:

- Improving trust in customer relationships
- Protecting the organisation's reputation
- Decreasing likelihood of violations of privacy
- Providing greater confidence when interacting with trading partners
- Enabling new and better ways to process electronic transactions
- Reducing operational costs by providing predictable outcomes—mitigating risk factors that may interrupt the process

Although 28 percent of all (organisations in the Aberdeen study) are operating security programmes at best-in-class levels, the findings indicated that less than 10 percent operate best-in-class [security] governance programmes.[9]

[8] Allen, Julia; *Governing for Enterprise Security*, Carnegie Mellon University, USA, 2005
[9] 'Best Practices in Security Governance', Aberdeen Group, USA, 2005

In 2003, McKinsey, in conjunction with Institutional Investors Inc., concluded that major international investors were willing to pay a premium for shares in an enterprise known to be well governed.[10] The premium ranged from 11 to 16 percent in 1996, to 18 to 28 percent in 2000. The demand for disclosure of the effectiveness of controls and attestation increased with the advent of financial reporting regulations and statutory requirements. This study suggests obvious implications for adequate and effective security governance.

The benefits of good information security are not just a reduction in risk or a reduction in the impact should something go wrong. Good security can improve reputation, confidence and trust from others with whom business is conducted, and can even improve efficiency by avoiding wasted time and effort recovering from a security incident.[11]

Process Integration

A promising concept, driven in large part by the increasing tendency to segment security into separate but related functions, focuses on the integration of an organisation's management assurance processes regarding security. This can serve to improve overall security and operational efficiencies.

These activities are at times fragmented and segmented in silos with different reporting structures. They tend to use different terminology and generally reflect different understandings of their processes and outcomes with, at times, little in common. This makes it difficult, if not impossible, to seamlessly integrate them. Results include overlapping security initiatives, which waste resources, or major gaps that can lead to serious security compromises. An illustrative example is a case where two people posing as repair technicians physically took several electronically well-secured database servers from a customs office. Another involved a technically secure network used to process fraudulent orders. In both cases, the lack of integration of management processes left large gaps, resulting in serious impacts.

Evaluating management processes from start to finish, along with their controls, can mitigate the tendency for security gaps to exist amongst various functions.

---

[10] McKinsey and Institutional Investors Inc., 'McKinsey/KIOD Survey on Corporate Governance', January 2003, *www.mckinsey.com/clientservice/organizationleadership/service/corpgovernance/pdf/cg_survey.p*

[11] IT Governance Institute, COBIT® *Security Baseline*, USA, 2004, *www.itgi.org*

2. Why Are Information Security and Information Security Governance Important?

A key goal of information security is to reduce adverse impacts on the organisation to an acceptable level of risk. Information security protects information assets against the risk of loss, operational discontinuity, misuse, unauthorised disclosure, inaccessibility and damage. It also protects against the ever-increasing potential for civil or legal liability that organisations face as a result of information inaccuracy and loss, or the absence of due care in its protection.

Information security covers all information processes, physical and electronic, regardless whether they involve people and technology or relationships with trading partners, customers and third parties. Information security addresses information protection, confidentiality, availability and integrity throughout the life cycle of the information and its use within the organisation.

Information security addresses the protection of information, confidentiality, availability and integrity throughout the life cycle of the information and its use within the organisation.

Given the dramatic rise of information crimes, including phishing and other cyberattacks, few today would contend that improved security is not a requirement. With new worms/malware and the increase in reported losses of confidential customer information and intellectual property theft, senior management is left with little choice but to address these issues. Information security requires a balance between sound management and applied technology. With the widespread use of networks, individuals and organisations are concerned with other risks pertaining to privacy of personal information and the organisation's need to protect the confidentiality of information, whilst encouraging electronic business.[12]

The systems and processes that handle information have become pervasive throughout enterprises. Organisations may survive the loss of other assets, including facilities, equipment and people, but few can continue with the loss of their critical information (i.e., accounting and financial reporting information and operations and process knowledge and information) or customer data. The risks, benefits and opportunities these resources present have made information security governance a critical facet of overall governance.

Information security should be an integral part of enterprise governance, aligned with IT governance and integrated into strategy, concept, design, implementation and operation. Protecting critical information must constitute one of the major risks to be considered in management strategies and should also be recognised as a crucial contributor to success.

[12] *Op. cit.,* IT Governance Institute, CobiT *Security Baseline*

Thus, information security governance requires senior management commitment, a security-aware culture, promotion of good security practices and compliance with policy. It is easier to buy a solution than to change a culture, but even the most secure system will not achieve a significant degree of security if used by ill-informed, untrained, careless or indifferent personnel.

Information security is a top-down process requiring a comprehensive security strategy that is explicitly linked to the organisation's business processes and strategy. Security must address entire organisational processes, both physical and technical, from end to end.

To ensure that all relevant elements of security are addressed in an organisational security strategy, several security standards have been developed to provide guidance and ensure comprehensiveness. Some of the most commonly used standards include *Control Objectives for Information and related Technology* (CobiT), ISO 17799, and others such as FIPS Publication 200 and NIST 800-53 in the US.

A formal security strategy is implemented in part by developing and deploying comprehensive security policies that reflect the objectives of the organisation and address each element of the strategy. To provide effective governance, a set of enterprise standards for each policy must be developed to define boundaries for acceptable processes and procedures along with assigned roles and responsibilities. Education, awareness and training must be provided to all personnel as part of an ongoing process to ensure that behaviours support secure, reliable operations.

Along with security policies, a comprehensive security programme includes:
- Development/maintenance of security policies
- Assignment of roles, responsibilities, authority and accountability
- Development/maintenance of a security and control framework that consists of standards, measures, practices and procedures
- Periodic assessments of risks and business impact analyses
- Classification and assignment of ownership of information assets
- Adequate, effective and tested controls for people, processes and technology
- Integration of security into all organisational processes
- Processes to monitor security elements
- Information security incident management
- Effective identity and access management processes for users and suppliers of information
- Meaningful monitoring and metrics of security performance
- Education of all users, managers and board members regarding information security requirements

- Annual information security evaluations and performance reports to the board of directors
- Plan for remedial action to address information security deficiencies
- Training in the operation of security processes
- Development and testing of plans for continuing the business in case of interruption or disaster

Some aspects of a security programme may hold more relevance for senior management than others. For example, countries such as Japan, France, Canada, India, the US and Australia are focusing on the adequacy and testing of controls for financial reporting from a regulatory/statutory or legal perspective. Information security is one of the critical requirements of controlled financial reporting. Within the European Union (EU), a focus on the privacy perspective as it relates to security and confidentiality of personal information may be of equal or greater significance.

It is critical that management ensure that adequate resources are allocated to support the overall enterprise information security strategy.

Organisations may also have special security requirements or objectives resulting from partnerships or customer contractual arrangements. Therefore, it is critical that management ensure that these considerations are tightly aligned with enterprise policies and procedures, and adequate resources are allocated to support the overall enterprise strategy.

A comprehensive security programme implements the protection of information assets through a layered series of technological and non-technological safeguards and controls (i.e., safety and environmental security measures, perimeter and physical security, background checks, access control security measures, user identifiers, passwords, IT technical measures and manual and automated procedures). These safeguards and controls are necessary and should address threats and vulnerabilities in a manner that reduces potential impacts to a defined, acceptable level. Necessary and key controls and their objectives are covered comprehensively within CobiT.

Information Security Governance Defined

Information security governance is a subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, manages risks appropriately, uses organisational resources responsibly, and monitors the success or failure of the enterprise security programme.

Information security deals with all aspects of information (spoken, written, printed, electronic or any other medium) and information handling (created, viewed, transported, stored or destroyed). This is contrasted with IT security that is concerned with security of information within the boundaries of the network infrastructure technology domain. Typically, confidential information disclosed in an elevator conversation or sent via regular mail

would be outside the scope of IT security. However, from an information security perspective, the nature and type of compromise is not as important as the fact that security has been breached; that is the crucial concern.

To achieve effective information security governance, management must establish and maintain a framework to guide the development and maintenance of a comprehensive information security programme.

The information security governance framework generally consists of:
- An information security risk management methodology
- A comprehensive security strategy explicitly linked with business and IT objectives
- An effective security organisational structure
- A security strategy that talks about the value of information protected—and delivered
- Security policies that address each aspect of strategy, control and regulation
- A complete set of security standards for each policy to ensure that procedures and guidelines comply with policy
- Institutionalised monitoring processes to ensure compliance and provide feedback on effectiveness and mitigation of risk
- A process to ensure continued evaluation and update of security policies, standards, procedures and risks

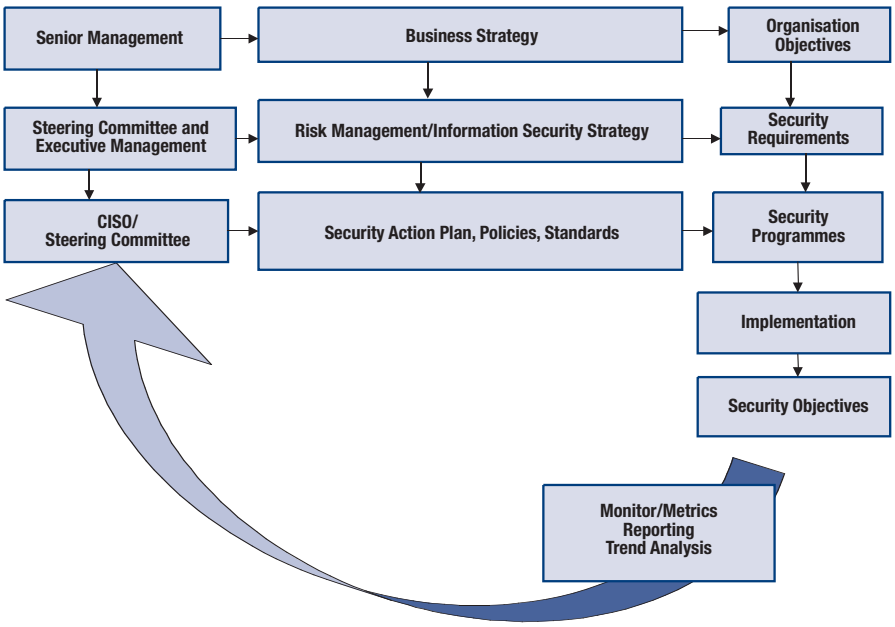
Information security governance is a subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, manages risks appropriately, uses organisational resources responsibly, and monitors the success or failure of the enterprise security programme.

This framework in turn provides the basis for the development of a cost-effective information security programme that supports the organisation's goals and provides an acceptable level of predictability for operations by limiting the impacts of adverse events. The overall objective of the programme is to provide assurance that information assets are given a level of protection commensurate with their value or the risk their compromise poses to the organisation.

The framework generates a set of activities that supports fulfilment of this objective. **Figure 1** indicates the necessary people components in developing a security strategy aligned with business objectives.

To promote alignment, the business strategy provides one of the inputs into risk management and information security strategy development. Other inputs are the business processes, risk assessments, business input analyses and the information resources critical for their success. Regulatory requirements must also be considered in developing the security strategy. Security requirements are the output of the risk management activity and are input to the planning activity together with the current state of the enterprise relative to these security requirements. Other inputs to the planning stage are the available resources and applicable constraints for achieving the desired state of security.

Figure 1—Conceptual Information Security Governance



The strategy provides the basis for an action plan comprised of one or more security programmes that, as implemented, achieve the security objectives. The strategy and action plans must contain provisions for monitoring as well as defined metrics to determine the level of success. This provides feedback to the chief information security officer (CISO) and steering committee to allow for mid-course correction and ensure that security initiatives are on track to meet defined objectives.

Once managers and directors know what information resources need what level of protection, information security baselines can be developed and implemented. Information security baselines are the minimum acceptable security that should be provided to protect information resources. Baselines vary depending on the sensitivity and criticality of the asset. Baselines can be expressed as technical, procedural and personnel standards throughout the enterprise. They are normally developed using a combination of accepted global standards such as CobiT, ISO 17799 and country-specific guidance such as FIPS Publication 200, NIST Special Publication 800-53 and Corporate Information Security Working Group (CISWG), as well as decisions by the organisation on the acceptable level of risk weighed against the cost of mitigation. An example of a baseline is CobiT *Security Baseline*,[13] which provides security awareness and guidance for professional users, home users, managers, executives, senior executives and boards of directors/trustees.

[13] *Op. cit.*, IT Governance Institute, CobiT *Security Baseline*

Whilst emerging definitions of the scope of information security are adding concepts such as information usefulness and possession—the latter to cope with theft, deception and fraud—the networked economy adds the critical need for trust and accountability in electronic transactions.

In this context, the security objective is met when:

- Information is available and usable when required, and the systems that provide it can appropriately resist or recover from attacks (*availability*)
- Information is observed by or disclosed to only those who have a need to know (*confidentiality*)
- Information is protected against unauthorised modification (*integrity*)
- Business transactions as well as information exchanges between enterprise locations or with external trading partners can be trusted (*authenticity and non-repudiation*)

The relative priority and significance of availability, confidentiality, integrity, authenticity and non-repudiation vary according to the data within the information system and the business context in which they are used. For example, integrity is especially important relative to management information due to the impact that information has on critical strategy-related decisions and financial reporting. Confidentiality may be the most critical today as it relates to personal, financial or medical information, or the protection of trade secrets and other forms of intellectual property (IP).

3. Who Should Be Concerned With Information Security Governance?

Boards of Directors/Trustees

It is a fundamental responsibility of senior management to protect the interests of the organisation's stakeholders. This includes understanding risks to the business to ensure that they are adequately addressed from a governance perspective. To do so effectively requires managing risks, including information security risks, by integrating information security governance in the overall enterprise governance framework of the organisation.

Information security governance requires strategic direction and impetus. It requires commitment, resources and assignment of responsibility for information security management, as well as a means for the board to determine that its intent has been met. Experience has shown that the effectiveness of information security governance is dependent on the involvement of senior management in approving policy, and appropriate monitoring and metrics coupled with reporting and trend analysis.

Members of the board need to be aware of the organisation's information assets and their criticality to ongoing business operations. This can be accomplished by periodically providing the board with the high-level results of comprehensive risk assessments and business impact analyses. It may also be accomplished by business dependency assessments of information resources. A result of these activities should include board members validating/ratifying the key assets they want protected and confirming that protection levels and priorities are appropriate to a recognised standard of due care.

The tone at the top must be conducive to effective security governance. It is unreasonable to expect lower-level personnel to abide by security policies if senior management does not. Visible and periodic board member endorsement of intrinsic security policies provides the basis for ensuring that security expectations are met at all levels of the enterprise. Penalties for non-compliance must be defined, communicated and enforced from the board level down.

Essential security practices for directors:

- **Place information security on the board's agenda.**
- **Identify information security leaders, hold them accountable and ensure support for them.**
- **Ensure the effectiveness of the corporation's information security policy through review and approval.**
- **Assign information security to a key committee.**[14]

Executives

Implementing effective security governance and defining the strategic security objectives of an organisation are complex, arduous tasks. They require leadership and ongoing support from executive management to succeed. Developing an effective information security strategy requires

[14] O*p. cit.,* National Association of Corporate Directors

integration with and co-operation of business unit managers and process owners. A successful outcome is the alignment of information security activities in support of organisational objectives. The extent to which this is achieved will determine the effectiveness of the information security programme in meeting the desired objective of providing a predictable, defined level of management assurance for business processes and an acceptable level of impact from adverse events.

An example of this is the foundation for the US federal government's cybersecurity, which requires assigning clear and unambiguous authority and responsibility for security, holding officials accountable for fulfilling those responsibilities, and integrating security requirements into budget and capital planning processes.[15]

Steering Committee

Information security affects all aspects of an organisation. To ensure that all stakeholders affected by security considerations are involved, a steering committee of executives should be formed. Members of such a committee may include, amongst others, the chief executive officer (CEO) or designee, business unit executives, chief financial officer (CFO), chief information officer (CIO)/IT director, chief security officer (CSO), CISO, human resources, legal, risk management, audit, operations and public relations. A steering committee serves as an effective communication channel for management's aims and directions and provides an ongoing basis for ensuring alignment of the security programme with organisational objectives. It is also instrumental in achieving behaviour change toward a culture that promotes good security practices and policy compliance.

Chief Information Security Officer

All organisations have a CISO whether or not anyone holds that title. It may be *de facto* the CIO, CSO, CFO or, in some cases, the CEO, even when there is an information security office or director in place. The scope and breadth of information security concerns are such that the authority required and the responsibility taken inevitably end up with a C-level officer or executive manager. Legal responsibility, by default, extends up the command structure and ultimately resides with senior management and the board of directors. Failure to recognise this and implement appropriate governance structures can result in senior management being unaware of this responsibility and the attendant liability. It usually results in a lack of effective alignment of security activities with organisational objectives.

[15] *The US National Strategy to Secure Cyberspace*, 2003, *www.whitehouse.gov/pcipb*

Increasingly, prudent management is elevating the position of information security officer to a C-level or executive position as organisations begin to understand their dependence on information and the growing threats to it. Ensuring that the position exists, and assigning it the responsibility, authority and required resources, demonstrates management's and board of directors' awareness of and commitment to sound information security governance.

4. What Should the Board of Directors/Trustees and Senior Executives Be Doing?

Boards and management have several fundamental responsibilities to ensure that information security governance is in force. Amongst the issues they should focus on are:

Understand Why Information Security Needs to Be Governed

- Risks and threats are real and could have significant impact on the enterprise.
- Reputational damage can be considerable.
- Effective information security requires co-ordinated and integrated action from the top down.
- IT investments can be substantial and easily misdirected.
- Cultural and organisational factors are equally important.
- Rules and priorities need to be established and enforced.
- Trust needs to be demonstrated toward trading partners whilst exchanging electronic transactions.
- Trust in reliability of system security needs to be demonstrated to all stakeholders.
- Security incidents are likely to be exposed to the public.

Take Board-level Action

- Become informed about information security.
- Set direction, i.e., drive policy and strategy and define a global risk profile.
- Provide resources to information security efforts.
- Assign responsibilities to management.
- Set priorities.
- Support change.
- Define cultural values related to risk awareness.
- Obtain assurance from internal or external auditors.
- Insist that management makes security investments and security improvements measurable, and monitors and reports on programme effectiveness.

Take Senior Management-level Action

- Provide oversight for the development of a security and control framework that consists of standards, measures, practices and procedures, after a policy has been approved by the governing body of the organisation and related roles and responsibilities assigned. (**Design***)*[16]
- Set direction for the creation of a security policy, with business input. (**Policy Development**)
- Ensure that individual roles, responsibilities and authority are clearly communicated and understood by all. (**Roles and Responsibilities**)

[16] The key words highlighted in this subsection refer to the International Federation of Accountants' guideline, *Managing Security of Information*, USA, 1998.

- Require that threats and vulnerabilities be identified, analysed and monitored, and industry practices used for due care.
- Require the set-up of a security infrastructure.
- Set direction to ensure that resources are available to allow for prioritisation of possible controls and countermeasures implement accordingly on a timely basis, and maintained effectively. (**Implementation**)
- Establish monitoring measures to detect and ensure correction of security breaches, so all actual and suspected breaches are promptly identified, investigated and acted upon, and to ensure ongoing compliance with policy, standards and minimum acceptable security practices. (**Monitoring**)
- Require that periodic reviews and tests be conducted.
- Institute processes that will help implement intrusion detection and incident response.
- Require monitoring and metrics to ensure that information is protected, correct skills are on hand to operate information systems securely and security incidents are responded to on a timely basis. Education in security measures and practices is of critical importance for the success of an organisation's security programme. (**Awareness, Training and Education**)
- Ensure that security is considered an integral part of the systems development life cycle process and is explicitly addressed during each phase of the process.

Illustrative Matrix of Outcomes and Directives

The relationships amongst the outcomes of effective information security governance and management directives are shown in **figure 2**. These directives are not meant to be comprehensive but they do illustrate some primary tasks and levels for which the board and executive management are responsible.

Figure 2—Relationships of Outcomes With Management Directives

Management Level	Strategic Alignment	Risk Management	Value Delivery	Performance Measurement	Resource Management	Integration
Board of directors/ trustees	Set direction for a demonstrable alignment.	Set direction for a risk management policy that applies to all activities and regulatory compliance.	Set direction for reporting of security activity costs and value of information protected.	Set direction for reporting of security effectiveness.	Set direction for a policy of knowledge management and resource utilisation.	Set direction for a policy of assuring process integration.
Senior executives	Institute processes to integrate security with business objectives.	Ensure that roles and responsibilities include risk management in all activities. Monitor regulatory compliance.	Require business case studies of security initiatives and value of information protected.	Require monitoring and metrics for reporting security activities.	Ensure processes for knowledge capture and efficiency metrics.	Provide oversight of all management process functions and plans for integration.
Steering committee	Review and assist security strategy and integration efforts, ensure that business unit managers and process owners support integration.	Identify emerging risks, promote business unit security practices, and identify compliance issues.	Review and advise adequacy of security initiatives to serve business functions and value delivered in terms of enabled services.	Review and advise the extent to which security initiatives meet business objectives.	Review processes for knowledge capture and dissemination.	Identify critical business processes and management assurance providers. Direct assurance integration efforts.
Chief information security officer	Develop security strategy, oversee the security programme and initiatives, and liaise with business unit managers and process owners for ongoing alignment.	Ensure risk and business impact assessments, develop risk mitigation strategies, and enforce policy and regulatory compliance.	Monitor utilisation and effectiveness of security resources and reputation and the delivery of trust.	Develop and implement monitoring and metrics collection and analysis and reporting approaches. Direct and monitor security activities.	Develop methods for knowledge capture and dissemination. Develop metrics for effectiveness and efficiency.	Liaise with other management process functions. Ensure that gaps and overlaps are identified and addressed.

5. What Are Some Thought-provoking Questions to Ask?

Chapter 8 provides a structured set of questions and practices but those responsible for information security governance may need some initial thought-provoking and awareness-raising questions to uncover information security issues and get an initial feel for what is being done about these issues.

Questions to Uncover Information Security Issues

- Does the head of security/CISO routinely meet or brief business management?
- When was the last time top management got involved in security-related decisions? How often does top management get involved in progressing security solutions?
- Does management know who is responsible for security? Does the responsible individual know? Does everyone else know?
- Would people recognise a security incident when they saw one? Would they ignore it? Would they know what to do about it?
- Does anyone know how many computers the company owns? Would management know if some went missing?
- Are damage assessment and disaster recovery plans in place?
- Has management identified all information (customer data, strategic plans, financial data, research results, etc.) that would violate policy, legal or regulatory requirements or cause embarrassment or competitive disadvantage if it were leaked?
- Did the company suffer from the latest virus or malware attack? How many attacks were successful during the past 12-month period?
- Have there been intrusions? How often and with what impact?
- Does anyone know how many people are using the organisation's systems? Does anyone care whether or not they are allowed access, or what they are doing?
- Is security considered an afterthought or a prerequisite?

Do not treat security as an afterthought. Address it at every phase of the development life cycle.

Questions to Find Out How Management Addresses Information Security Issues

- Is the enterprise clear on its position relative to IT and security risks? Does it tend toward risk-avoidance or risk-taking?
- How much is being spent on information security? On what? How were the expenditures justified? What projects were undertaken to improve security during the past 12-month period?
- What percentage of staff had security training last year? What percentage of the management team received training?
- How does management decide who has access to the organisation's information and systems? How often are these decisions revisited?
- How does the organisation detect security incidents? How are they escalated and what does management do about them?

- Is management prepared to recover from a major security incident?
- Is there a security programme in place that covers all of the above questions? Is there clear accountability about who carries it out?
- Does IT staff understand computer forensics/chain of evidence custody considerations?

Questions to Self-assess Information Security Governance Practices

- Is management confident that security is being adequately addressed in the enterprise?
- Is management aware of the latest information security issues and best practices?
- Does the organisation participate in an incident, threat, vulnerability notification and sharing service?
- What is industry best practice and how does the enterprise compare?
- Does management regularly articulate and communicate the enterprise requirement for information security?
- Does management have a view on how much the enterprise should invest in information security improvements?
- Are information security issues considered when developing business and IT strategy?
- Does management obtain regular progress reports on the state of security and security improvement projects?
- Has management set up an independent audit or review of information security? Does management track its own progress on recommendations?

6. What Should Information Security Governance Deliver?

Key goals or objectives help provide information about the target of achievement for a process or service—they can be used effectively to determine whether organisational objectives are being met. Information security governance, when properly implemented, should provide five basic outcomes, as described in chapter 1. Some illustrative goals selected from CobiT are presented as follows.

Strategic Alignment

It is often difficult to achieve the goal of strategic alignment of information security in support of organisational objectives. Consider the following goals:

- Ensure transparency and understanding of IT security costs, benefits, strategy, policies and service levels.
- Develop a common and comprehensive set of IT security policies.
- Communicate the IT strategy, policies and control framework.
- Enforce IT security policies.
- Define security incidents in business impact terms.
- Establish clarity on the business impact of risks to IT objectives and resources.
- Establish IT continuity plan that supports business continuity plans.

The key goal of information security is to reduce adverse impacts on the organisation to an acceptable level.

Risk Management

To manage and mitigate risks and reduce potential impacts on information assets to an acceptable level, consider the following goals:

- Account for and protect all IT assets.
- Establish and reduce the likelihood and impact of IT security risks.
- Perform regular risk assessments with senior managers and key staff.
- Permit access to critical and sensitive data only to authorised users.
- Ensure critical and confidential information is withheld from those who should not have access to it.
- Identify, monitor and report security vulnerabilities and incidents.
- Develop IT continuity plans that can be executed and are tested and maintained.

A key goal of information security is to reduce adverse impacts on the organisation to an acceptable level of risk. Therefore, a key metric is the adverse impacts of information security incidents experienced by the organisation. An effective security programme will show a trend of impact reduction. Quantitative measures can include trend analysis of impacts over time.

Resource Management

Information security knowledge and infrastructure should be used efficiently and effectively. Consider the following goals:

- Maintain the integrity of information and processing infrastructure.
- Account for and protect all IT assets.
- Ensure that IT services and infrastructure can resist and recover from failures due to error, deliberate attack or disaster.
- Ensure proper use and performance of the applications and technology solutions.

Performance Measurement

Measuring, monitoring and reporting on information security processes ensures that organisational objectives are achieved. Consider these example metrics:

- Number of incidents damaging reputation with the public
- Number of systems where security requirements are not met
- Time to grant, change and remove access privileges
- Number and type of suspected and actual access violations
- Number and type of malicious code prevented
- Number and type of security incidents
- Number and type of obsolete accounts
- Number of unauthorised IP addresses, ports and traffic types denied
- Number of access rights authorised, revoked, reset or changed

Value Delivery

Security investments should be optimised to support organisational objectives. Security activities consume resources. Optimal investment levels occur when strategic goals for security are achieved and an acceptable risk posture is attained by the organisation at the lowest possible cost. The following goals should be considered:

- Ensure automated business transactions and information exchanges can be trusted.
- Make sure that IT services are available as required.
- Minimise the probability of IT service interruption.
- Minimise the impact of security vulnerabilities and incidents.
- Ensure minimum business impact in the event of an IT service disruption or change.
- Establish cost-effective action plans for critical IT risks.

As mentioned earlier in this publication, process integration is an area of increased interest related to information security governance. This is driven in large part by an organisation's need to rapidly respond to change and focuses on an organisation's tendency to segment security-related activities; thus, there is a need to ensure proper management process assurance over these activities.

This approach to information security governance includes an effort to ensure that processes and activities operate as intended from end to end, minimising hidden risks. Its succcessful implementation is evidenced by such conditions as:

- No gaps exist in information asset protection.
- Unnecessary security overlaps are eliminated.
- Assurance activities are seamlessly integrated.
- Roles and responsibilities are well defined.
- Assurance providers understand their relationship to other assurance functions and regularly liaise with each other.

7. How Is Information Security Governance Evolving?

The requirement to improve information security governance will continue into the foreseeable future. Whilst spending on security has grown in response to increasing risk, the failure of security to deal with identity theft, fraud, wholesale loss of customer personal information and a host of other criminal and destructive uses of information systems continues unabated. Numerous studies universally support the conclusions presented in this publication that information security must be addressed as a governance-level concern.

The traditional focus on technical solutions must give way to the understanding that security is fundamentally a management problem to be addressed at the highest levels. As organisational assets continue to become more intangible, the requirements of due care in the protection of information assets will require greater attention and resources. Additionally, effective information security governance is becoming a necessity to adequately address the numerous legal and regulatory/statutory requirements. Organisations that fail to address these issues will find themselves at a competitive disadvantage and fall victim to ever more technologically sophisticated criminals. They will find share value increasingly tied to governance (good and bad) as the market becomes more knowledgeable of its relevance.

The results show that announcing an Internet security breach is negatively associated with the market value of the announcing firm. The breached firms in the sample lost, on average, 2.1 percent of their market value within two days of the announcement—an average loss in market capitalisation of US $1.65 billion per breach.[18]

Momentum is growing globally to address issues of privacy and cybercrime, with stringent regulations regarding operational risk management, full financial disclosure and privacy protection. A number of jurisdictions are in the process of creating legislation that will mandate better security governance practices.[17] Organisations can expect oversight to continue to tighten until the international security situation begins to improve and failures of security and privacy become less costly to global economies, organisations and individuals.

Organisations must consider that failing to provide adequate protection of critical information assets is becoming more visible and less acceptable. Liability will ultimately find its way to the boardroom. Senior management must understand that the absence of adequate security constitutes deferred risk, which the costs to remedy represent a growing unfunded liability and exposure.

---

[17] Security breach legislation, *www.perkinscoie.com/content/ren/updates/privacy/092605.htm*
[18] *International Journal of Electronic Commerce*, volume 9, number 1, fall 2004

Management should also consider that the risks of large negligence awards and the direct financial consequences may be overshadowed by public exposure of poor governance and substandard practices. These, in turn, have the potential to lead to reputational losses likely to be reflected in reduced share value.

Firms operating at best-in-class [security] levels are lowering financial losses to less than one percent of revenue; whereas other organisations are experiencing loss rates that exceed 5 percent.[20]

Evidence provided by Aberdeen Group's research[19] indicates that losses due to ineffective security can be reduced by up to 90 percent by implementing known, commonly used security practices. This alone should be sufficient to motivate action by responsible management.

Organisations are evolving in their thoughts about information security. Much more focus is being placed on the value it can deliver to the organisation, and how it can contribute to enhanced and sustained stakeholder value. Additionally, given ever-expanding globalisation, privacy compliance issues, legal and regulatory requirements, and the risk of potential adverse actions against organisations deemed to be careless or negligent, it is increasingly prudent for boards and executive management to address effective information security as a governance concern.

[19] *Op. cit.,* Aberdeen Group
[20] *Op. cit.,* Best Practices in Security Governance

8. What Can Be Done to Successfully Implement Information Security Governance?

The following illustrative questions provide boards of directors and senior executives a sound way to begin determining the extent to which effective information security governance is (or is not) in place. These are the questions those responsible for governance should ask.

Questions for Directors

- Does the board understand the organisation's dependence on information?
- Does the organisation recognise the value and importance of information security and set the appropriate tone at the top to foster a security-conscious environment?
- Does the organisation have a security strategy? If so, is it closely aligned with the overall business strategy?
- Does the board understand the organisation's potential liabilities in the event of regulatory non-compliance? Does it understand the potential liability in the event sensitive information is compromised?
- Has the organisation suffered a major security incident? Has the cost of the incident to the organisation been determined?
- Does information security appear as a board agenda item, and is there a schedule for reporting the status of the information security programme to the board?
- Has management issued a policy statement on information security? If it has, is the policy statement subject to review, update and approval?
- Can the entity continue to operate if critical information is unavailable, compromised or lost? What would be the consequences of a security incident in terms of lost revenues, lost customers and investor confidence? What would be the consequences if the infrastructure became inoperable?
- Are the information assets subject to laws and regulations? What has the board instituted to ensure compliance?
- Does the audit committee clearly understand its role in information security and how it will set direction with management and auditors?
- Is there a CISO or officer specifically charged with managing information security in the organisation?
- Are there appropriate training and awareness programmes to ensure that personnel are aware of their security responsibilities?

Questions for Management

- How is the board kept informed of information security issues? When was the last briefing made to the board on security risks and status of security improvements?
- Has someone been appointed to be responsible for developing, implementing and managing the information security programme, and is he/she held accountable?

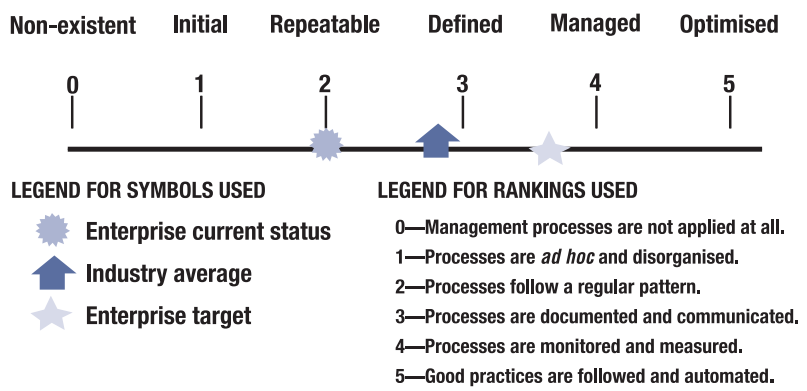
- Are security roles and responsibilities clearly defined and communicated?
- Is there a CISO or other officer with sufficient authority and resources to accomplish security objectives?
- Has the organisation ever had its network security checked by a third party?
- Has a business impact assessment been performed?
- When was the last risk assessment made on the criticality and sensitivity of information security assets? When is the next risk assessment scheduled?
- Does the risk assessment consider whether the entity can continue to operate if critical information is unavailable, compromised or lost? Does it cover the consequences of a security incident in terms of lost revenues, lost customers and investor confidence? Does it determine what the consequences would be if the infrastructure became inoperable?
- Does the CEO request an information security evaluation, and are the results reviewed with staff and reported to the board of directors?
- Is there an effective and tested process to deal with information security incidents/emergencies?
- Is there a business continuity/disaster recovery plan in place? Has it been tested under live circumstances? Is it tested regularly?
- Does the risk assessment consider what information assets are subject to laws and regulations? Does it result in adequate procedures to assure compliance with these laws and regulations?
- Is information security risk assessment a regular agenda item at IT and business management meetings and does management follow through and support improvement initiatives?
- Does the organisation have a security strategy? If so, is it closely aligned with the overall business strategy?
- Is there an ongoing process to ensure alignment of information security with business objectives?
- Are there appropriate training and awareness programmes to ensure that personnel are aware of their security responsibilities and the expectations of management?
- Is there an information asset classification process in place to ensure that critical assets are adequately protected?

9. How Does My Organisation Compare on Information Security Governance?

Boards of directors and executive management can use an information security governance maturity model to establish rankings for maturity within an organisation. When IT risk is referenced, it should be considered within the context of information security. This model[21] can be progressively applied as a method for:

- Self-assessment against the scales, deciding where the organisation is, as shown in **figure 3**
- Using the results of the self-assessment to set targets for future development, based on where the organisation wants to be on the scale, which is not necessarily at the top level
- Planning projects to reach the targets, based on an analysis of the gaps between those targets and the present status
- Prioritising project work based on project classification and an analysis of its beneficial impact against its cost

Figure 3—Maturity Model Dashboard



Maturity Level Description

0 Non-existent

- Risk assessment for processes and business decisions does not occur. The organisation does not consider the business impacts associated with security vulnerabilities and development project uncertainties. Risk management has not been identified as relevant to acquiring IT solutions and delivering IT services.

[21] Adapted from IT Governance Institute, CobiT 4.0, USA, 2005

- The organisation does not recognise the need for information security. Responsibilities and accountabilities are not assigned for ensuring security. Measures supporting the management of information security are not implemented. There is no information security reporting and no response process to information security breaches. There is a complete lack of a recognisable system security administration process.
- There is no understanding of the risks, vulnerabilities and threats to IT operations or the impact of loss of IT services to the business. Service continuity is not considered as needing management attention.

1 Initial/*Ad Hoc*

- The organisation considers IT risks in an *ad hoc* manner, without following defined processes or policies. Informal assessments of project risk take place as determined by each project.
- The organisation recognises the need for information security, but security awareness depends on the individual. Information security is addressed on a reactive basis and is not measured. Information security breaches invoke finger-pointing responses if detected, because responsibilities are unclear. Responses to information security breaches are unpredictable.
- Responsibilities for continuous service are informal, with limited authority. Management is becoming aware of the risks related to and the need for continuous service.

2 Repeatable but Intuitive

- There is an emerging understanding that IT risks are important and need to be considered. An approach to risk assessment exists, but the process is still immature and developing.
- Responsibilities and accountabilities for information security are assigned to an information security co-coordinator with no management authority. Security awareness is fragmented and limited. Information security information is generated, but not analysed. Security tends to respond reactively to information security incidents and by adopting third-party offerings, without addressing the specific needs of the organisation. Security policies are being developed, but inadequate skills and tools are still being used. Information security reporting is incomplete, misleading or not pertinent.
- Responsibility for continuous service is assigned. The approaches to continuous service are fragmented. Reporting on system availability is incomplete and does not take business impact into account.

3 Defined Process

- An organisationwide risk management policy defines when and how to conduct risk assessments. Risk assessment follows a defined process that is documented and available to all staff through training.
- Security awareness exists and is promoted by management. Security awareness briefings have been standardised and formalised. Information security procedures are defined and fit into a structure for security policies and procedures. Responsibilities for information security are assigned, but are not consistently enforced. An information security plan exists, driving risk analysis and security solutions. Information security reporting is IT-focused, rather than business-focused. *Ad hoc* intrusion testing is performed.
- Management communicates consistently the need for continuous service. High-availability components and system redundancy are being applied piecemeal. An inventory of critical systems and components is rigorously maintained.

4 Managed and Measurable

- The assessment of risk is a standard procedure and exceptions to following the procedure would be noticed by IT management. It is likely that IT risk management is a defined management function with senior-level responsibility. Senior management and IT management have determined the levels of risk that the organisation will tolerate and have standard measures for risk/return ratios.
- Responsibilities for information security are clearly assigned, managed and enforced. Information security risk and impact analysis is consistently performed. Security policies and practices are completed, with specific security baselines. Security awareness briefings are mandatory. User identification, authentication and authorisation are standardised. Security certification of staff is established. Intrusion testing is a standard and formalised process, leading to improvements. Cost-benefit analysis, supporting the implementation of security measures, is increasingly being utilised. Information security processes are co-ordinated with the overall organisation security function. Information security reporting is linked to business objectives.
- Responsibilities and standards for continuous service are enforced. System redundancy practices, including use of high-availability components, are consistently deployed.

5 Optimised

- Risk management has developed to the stage that a structured, organisationwide process is enforced, followed regularly and managed well.
- Information security is a joint responsibility of business and IT management and is integrated with enterprise security business objectives. Information security requirements are clearly defined, optimised and included in a verified security plan. Security functions are integrated with applications at the design stage and end users are increasingly accountable for managing security. Information security reporting provides early warning of changing and emerging risk, using automated active monitoring approaches for critical systems. Incidents are promptly addressed, with formalised incident response procedures supported by automated tools. Periodic security assessments evaluate the effectiveness of implementation of the security plan. Information on new threats and vulnerabilities is systematically collected and analysed, and adequate mitigating controls are promptly communicated and implemented. Intrusion testing, root cause analysis of security incidents and proactive identification of risk are the basis for continuous improvements. Security processes and technologies are integrated organisationwide.
- Continuous service plans and business continuity plans are integrated, aligned and routinely maintained. Buy-in for continuous service needs is secured from vendors and major suppliers.

Appendix—Regulatory and Standards Bodies' Guidance on Information Security Governance

There are a number of international standards and regulatory bodies that deal with security of information and the systems that handle and process it. This is not meant to be an exhaustive list but rather to give a flavour of how some of the major ones address the issue of information security. The approach, segmentation and focus vary widely but the security standards and objectives are consistent.

CobiT® 4.0 (2005)

Developed and promoted by the IT Governance Institute (ITGI), *Control Objectives for Information and related Technology* (CobiT®) starts from the premise that IT needs to deliver the information that the enterprise needs to achieve its objectives. In addition to promoting process focus and process ownership, CobiT looks at fiduciary, quality and security needs of enterprises and provides seven information criteria that can be used to generically define what the business requires from IT: effectiveness, efficiency, availability, integrity, confidentiality, reliability and compliance.

CobiT further divides IT into 34 processes belonging to four domains (Plan and Organise [PO], Acquire and Implement [AI], Deliver and Support [DS], and Monitor and Evaluate [ME]). The CobiT framework addresses information security issues of concern in more than 20 processes. However, the four processes that are most directly related to information security are:

- PO6—Communicate management aims and directions.
- PO9—Assess and manage IT risks.
- DS4—Ensure continuous service.
- DS5—Ensure systems security.

For each process, a high-level control objective is defined:

- Identifying which information criteria are most important in that IT process
- Listing which resources will usually be leveraged
- Providing considerations on what is important for controlling that IT process

CobiT further provides more than 200 detailed control objectives for management and IT practitioners who are looking for best practices in control implementation, as well as management guidelines and maturity models building on these objectives.

CobiT includes a management and governance layer, providing management with:
- Performance measurement elements (outcome measures and performance drivers for all IT processes)
- A list of key activities that provides succinct, non-technical best practices for each IT process
- A maturity model to assist in benchmarking and decision making for control over IT

CobiT Security Baseline (2004)

Also published by ITGI, it addresses security in addition to the risks of the use of IT. Using the CobiT framework, the guidance focuses on the specific risks of IT security in a way that is easy to follow and implement for all users—home, small to medium enterprises, and executives and board members of larger organisations. It provides the following elements:
- Useful reading:
  - An introduction to information security—what it means and what it covers
  - An explanation of why security is important, with examples of the most common things that can go wrong
  - Some thought-provoking questions to help determine the risk
- The CobiT-based security baseline, providing key controls and mapping to ISO 17799
- Six information security survival kits, providing essential awareness messages for specific audiences
- An appendix containing a summary of technical security risks

Guidelines for the Security of Information Systems (2002)

The Organisation for Economic Co-operations and Development's (OECD's) *Guidelines for the Security of Information Systems* is designed to assist countries and enterprises to construct a framework for security of information systems. The guidelines are intended to:
- Raise awareness of risks to and safeguards for information systems
- Offer a general framework to aid in the development and implementation of effective measures, practices and procedures for the security of information systems and encourage co-operation between the public and private sectors regarding same
- Promote confidence in information systems, their implementation and use
- Facilitate national and international development, use and security of information systems

The framework covers laws, codes of conduct, technical measures, management and user practices, and public education/awareness activities. Ultimately, the intention is that the guidelines will serve as a benchmark against which governments, the public and private sectors, and society can measure progress.

Managing Security of Information (1998)

In 1998, International Federation of Accountants (IFAC) defined the objective of information security as, 'the protection of the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality and integrity'. Any organisation may consider the security objective met when those three criteria are satisfied, that is, when information systems are available and usable when required (availability), data and information are disclosed only to those who have a right to know them (confidentiality), and data and information are protected against unauthorised modification (integrity).

Availability, confidentiality and integrity may take on differing priorities or significance depending on the data within the information system and the business context in which they are used.

Guide for Assessing the Security Controls in Federal Information Systems, NIST 800-53A (Initial Public Draft 2005)

This document was developed by the US National Institute of Standards and Technology (NIST) to further its statutory responsibilities under the US Federal Information Security Management Act (FISMA) of 2002, P.L. 107-347. NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but the standards and guidelines do not apply to national security systems. This guideline was prepared for use by US federal agencies, but it may be appropriate for non-governmental agencies on a voluntary basis. Some of its benefits are:

- It facilitates a consistent, comparable and repeatable approach for selecting and specifying security controls.
- It provides a recommendation for minimum controls for information systems.
- It promotes dynamic catalogue of security controls for information systems.
- It creates a foundation for the development of techniques and procedures for verifying security control effectiveness.

The publication is intended to provide guidance to US federal agencies until the publication of Federal Information Processing Standard (FIPS) 200, *Minimum Security Controls for Federal Information Systems* (published December 2005).

Code of Practice for Information Security Management, ISO 17799 (2005)

International Organisation for Standardisation (ISO) 17799, *Code of Practice for Information Security Management,* is intended to serve as a single reference point for identifying the range of controls needed for most situations where information systems are used in industry and commerce.

It is suitable for use by any size organisation. It treats information as an asset that, like other important business assets, has value to the organisation and consequently needs to be suitably protected.
Information security is characterised within ISO 17799 as the preservation of:
- Confidentiality—Ensuring that information is accessible only to those authorised to have access to it
- Integrity—Safeguarding the accuracy and completeness of information and processing methods
- Availability—Ensuring that authorised users have access to information and associated assets when required

The standard is based on security risk assessment. This provides the basis for cost justification and improved productivity of security staff, amongst other outcomes.

Information security protects information from a wide range of threats thereby ensuring business continuity, minimising business damage, maximising return on investments and capitalising on business opportunities. Security is achieved by implementing a suitable set of controls, which consist of policies, practices, procedures, organisational structures and/or software functions. ISO has issued other security standards including ISO 15048, *Evaluation Criteria for IT Security*.

Trust Services (SysTrust) Principles and Criteria for Systems Reliability (2003)

The American Institute of Certified Public Accountants (AICPA)/Canadian Institute of Chartered Accountants (CICA) published Trust Services (SysTrust), an assurance service designed to increase the comfort of management, customers and business partners. The SysTrust service entails the certified public accountant providing an assurance service in which he/she evaluates and tests whether a system is reliable when measured against four essential principles: availability, security, integrity and maintainability.
- Availability—The system is available for operation and use at times set forth in service level statements or agreements.
- Security—The system is protected against unauthorised physical and logical access.
- Integrity—System processing is complete, accurate, timely and authorised.
- Maintainability—When necessary, the system can be updated in a way that does not interfere or conflict with its availability, security and integrity.

SysTrust defines a reliable system as one that is capable of operating without material error, fault or failure during a specified period in a specified environment. The boundaries of the system are defined by the system owner and must include the following key components: infrastructure, software, people, procedures and data.

SysTrust is scalable, so enterprises have the flexibility to choose any or all of the SysTrust principles for verification. An opinion rendered on all criteria constitutes an opinion on the overall reliability of the system. The accountant can also render an opinion on individual criteria, such as availability or security.

Standard of Good Practice for Information Security (2005)

The Information Security Forum's (ISF's) *Standard of Good Practice for Information Security* is based on research and practical experience of members. 'The standard addresses information security from a business perspective, providing a practical basis for assessing an organisation's information security arrangements. It focuses on the arrangements that should be made by leading organisations to keep the business risks associated with critical information systems under control'.[22] Each area is broken down into a number of detailed sections, totaling 135 appropriate controls.

ISF states that, in general, implementing the standard helps organisations to:
- Move toward international best practice and maintain business integrity
- Manage the breadth and depth of information risk
- Build confidence in third parties that information security is being addressed in a professional manner
- Reduce the likelihood of disruption from major incidents
- Fight the growing threats of cybercrime
- Comply with legal and regulatory requirements

The standard breaks security into five component areas:
- Security management
- Critical business applications
- Computer installations
- Networks
- Systems development

Information Security Governance: Call to Action (2004)

In December 2003, the US Department of Homeland Security co-hosted a National Cyber Security Summit in Santa Clara, California, USA. The immediate outcome was the formation of five task forces by the private sector, including the Corporate Governance Task Force. In its report, the task force called upon all organisations to make information security governance a corporate board-level priority. The key focus was to begin the process, with the subsequent goal of systematic improvement of performance over time.

[22] Information Security Forum, *Standard of Good Practice for Information Security*, version 4, UK, 2003

The report also includes a number of recommendations for government and industry action, including:

- Organisations should adopt the information security governance framework described in the report to embed cybersecurity into their corporate governance process.
- Organisations should signal their commitment to information security governance by stating on their web sites that they intend to use the tools developed by the task force to assess their performance and report the results to their board of directors.
- The US Department of Homeland Security should endorse the information security governance framework and its core set of principles, and encourage the private sector to make cybersecurity part of its corporate governance efforts.
- The Committee of Sponsoring Organisations of the Treadway Commission (COSO) should revise *Internal Controls—An Integrated Framework* so it explicitly addresses information security governance.

References

Aberdeen Group, 'Best Practices in Security Governance', USA, 2005

Allen, Julia; *Governing for Enterprise Security*, Carnegie Mellon University, USA, 2005

American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants, *Privacy Framework Principles and Criteria*, USA and Canada, 2005

American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants, *SysTrust Principles and Criteria for Systems Reliability*, USA and Canada, 2003

'Building Security in the Digital Resource: An Executive Resource', *Business Roundtable*, 2002

Business Software Alliance, 'Information Security Governance: Toward a Framework for Action', USA, 2003

Corporate Governance Task Force, *Information Security Governance: Call to Action*, USA, 2004

Corporate Information Security Working Group (CISWG), *Report of the Best Practices and Metrics*, USA, 2004

Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standard, (FIPS) PUB 200, *Minimum Security Requirements for Federal Information and Information Systems, Initial Public Draft*, USA, 2005

Department of Commerce, National Institute of Standards and Technology, Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems, Initial Public Draft*, USA, 2005

Department of Commerce, National Institute of Standards and Technology, Draft Special Publication 800-26 Revision 1, *Guide for Information Security Program Assessments and System Reporting*, USA, 2005

Drucker, Peter; 'Management Challenges for the 21st Century', *Harpers Business*, 1993

European Union (EU), *EU Privacy Directive*, 1995

General Accounting Office, *Federal Information System Controls Audit Manual*, USA, 1999

General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, USA, 1996

Federal Financial Institutions Examination Council, *IT Examination Handbook: Management*, USA, 2004, *www.ffiec.gov/ffiecinfobase/html_pages/it_01.html*

Federal Information Security Management Act (FISMA), USA, 2002

Hallawell, Arabella; *Gartner Global Security and Privacy Best Practices*, Gartner Analyst Reports, USA, 2004, *www.csoonline.com/analyst/report2332.html*

IBM, Data Governance Council, *Oversight of Information Security*, USA, 2005

'Information Security Addendum to Principles of Corporate Governance', *Business Roundtable*, USA, 2003

Institute of Internal Auditors, *Information Security Governance: What Directors Need to Know*, USA, 2001

Institute of Internal Auditors, *Information Security Management and Assurance: A Call to Action for Corporate Governance*, USA, 2000

Institute of Internal Auditors, *Presenting the Information Security Case to the Board of Directors*, USA, 2001

Information Security Forum, *Standard of Good Practice for Information Security*, version 4, UK, 2003

International Federation of Accountants, *International Information Technology Guidelines—Managing Security of Information*, USA, 1998

International Organisation for Standardisation, *Code of Practice for Information Security Management*, ISO 17799, Switzerland, 2005

IT Governance Institute, *Board Briefing on IT Governance, 2nd Edition,* USA, 2003

IT Governance Institute, CobiT 4.0, USA, 2005, *www.itgi.org*

IT Governance Institute, CobiT *Security Baseline*, USA, 2004, *www.itgi.org*

KPMG, *Creating Stakeholder Value in the Information Age: The Case for Information Systems Governance*, UK, 2004, *www.kpmg.co.uk/services/ras/irm/isg.cfm*

McKinsey and Institutional Investors Inc., 'McKinsey/KIOD Survey on Corporate Governance', January 2003, *www.mckinsey.com/clientservice/organizationleadership/service/corpgovernance/pdf/cg_survey.p*

Moulton, Rolf; Robert Coles; 'Applying Information Security Governance', *Computers and Security*, Elsevier Ltd., UK, 2003

National Association of Corporate Directors, 'Information Security Oversight: Essential Board Practices', USA, 2001

Organisation for Economic Co-operation and Development, *Guidelines for the Security of Information Systems and Networks—Towards a Culture of Security*, France, 2002

The US National Strategy to Secure Cyberspace, USA, 2003

LEADING THE IT GOVERNANCE COMMUNITY

3701 ALGONQUIN ROAD, SUITE 1010

ROLLING MEADOWS, IL 60008 USA

PHONE: +1.847.590.7491

FAX: +1.847.253.1443

E-MAIL: *info@itgi.org*

WEB SITE: *www.itgi.org*

Board of Directors/Executive Management

Information security governance consists of the leadership, organisational structures and processes that safeguard critical information assets.

Responsibilities		Outcomes
Boards should provide strategic oversight regarding information security, including: • Understanding the criticality of information and information security to the organisation • Reviewing investment in information security for alignment with the organisation strategy and risk profile • Endorsing the development and implementation of a comprehensive information security programme • Requiring regular reports from management on the programme's adequacy and effectiveness	**Governing boards and executive management should review:** • The scale and return of the current and future investments in information resources to ensure they are optimised • The potential for technologies to dramatically change organisations and business practices, thereby creating new opportunities and value while reducing costs	**The five basic outcomes of information security governance should include:** • Strategic alignment of information security with business strategy to support organisational objectives • Risk management by executing appropriate measures to manage and mitigate risks and reduce potential impacts on information resources to an acceptable level • Resource management by utilising information security knowledge and infrastructure efficiently and effectively • Performance measurement by measuring, monitoring and reporting information security governance metrics to ensure organisational objectives are achieved • Value delivery by optimising information security investments in support of organisational objectives

Benefits of good information security governance:

- Improved trust in customer relationships
- Protecting the organisation's reputation
- Decreasing likelihood of violations of privacy and potential liabilities
- Providing greater confidence when interacting with trading partners
- Enabling new and better ways to process electronic transactions
- Reducing operational costs by providing predictable outcomes—mitigating risk factors that may interrupt the process

A comprehensive security program will include:

- Development/maintenance of security policies
- Assignment of roles, responsibilities, authority and accountability
- Development/maintenance of a security and control framework that consists of standards, measures, practices and procedures
- Periodic assessments of risks and business impact analyses
- Classification and assignment of ownership of information assets
- Adequate, effective and tested controls for people, processes and technology
- Processes to monitor security elements
- Information security incident management
- Effective identity and access management process for users and suppliers of information
- Meaningful monitoring and metrics of security performance
- Education of all users, managers and board members regarding information security requirements
- Annual information security evaluations and performance reports to the board of directors
- Plan for remedial action to address information security deficiencies
- Training in the operation of security processes
- Development and testing of plans for continuing the business in case of interruption or disaster

This material is based on *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition.*
Copyright © 2006 IT Governance Institute® (ITGI™). All rights reserved. For additional information on this publication and ITGI, visit *www.itgi.org*.