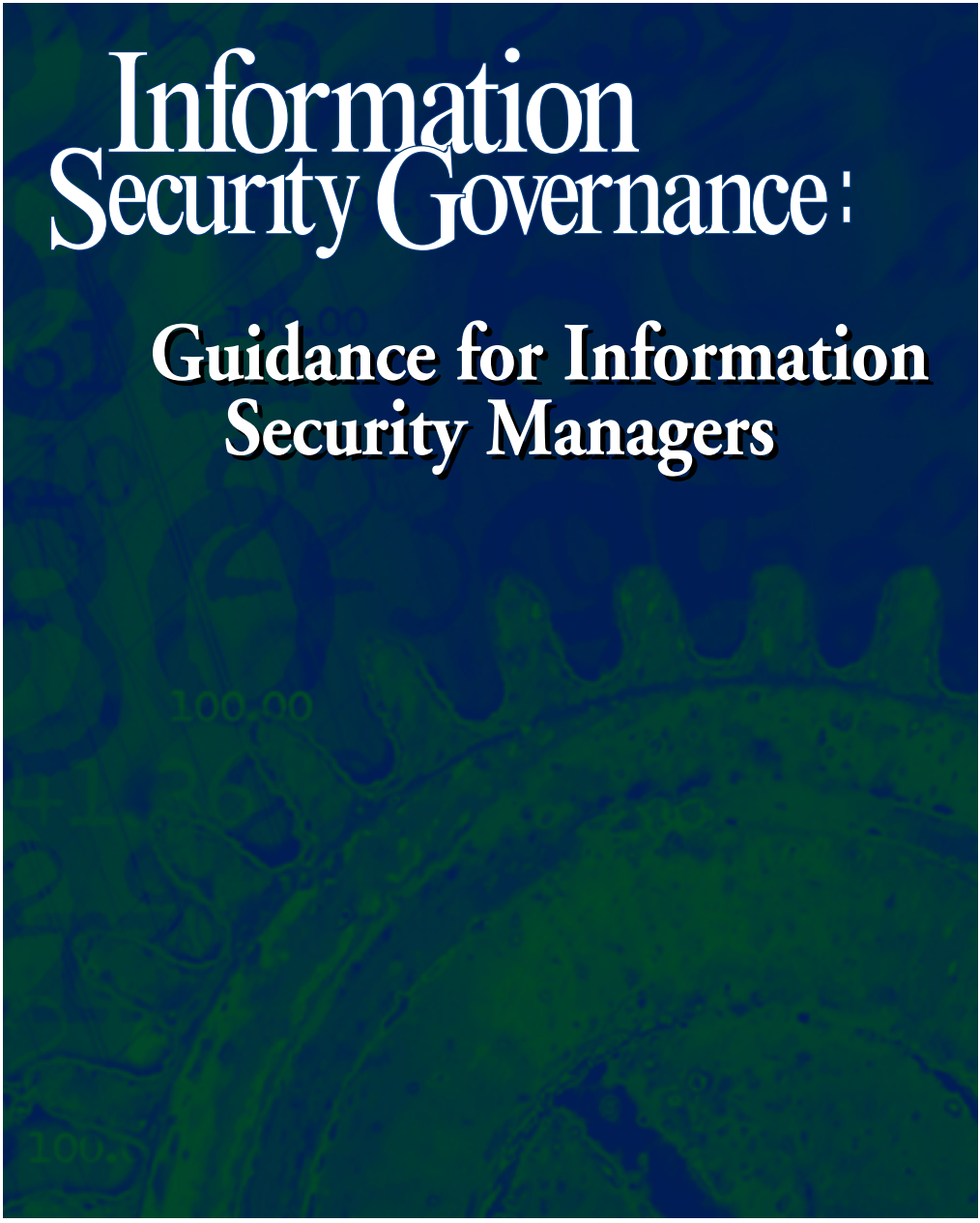
Information Security Governance:

Guidance for Information Security Managers

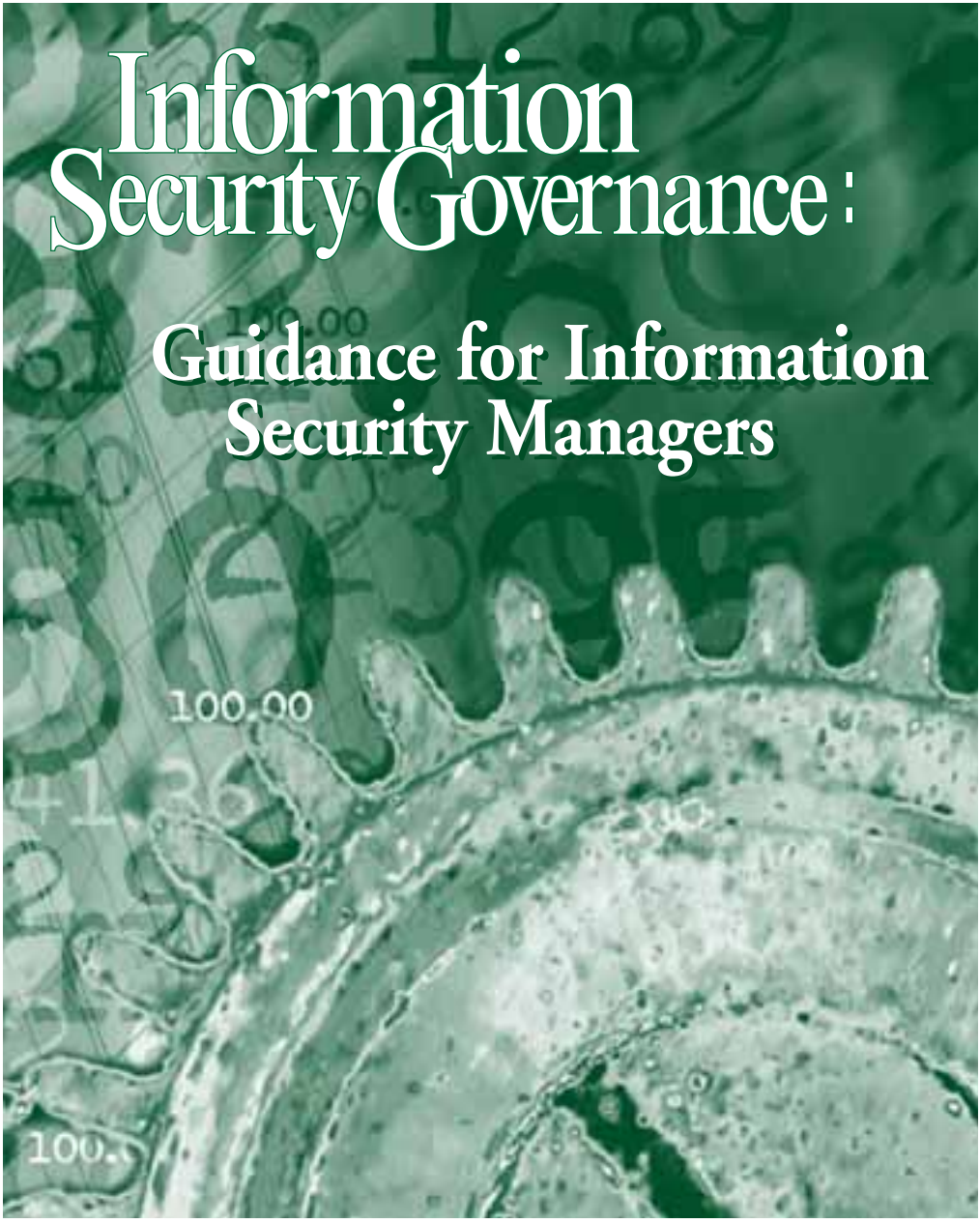


GOVERNANCE INSTITUTE®

LEADING THE IT GOVERNANCE COMMUNITY

Information Security Governance:

Guidance for Information Security Managers



GOVERNANCE INSTITUTE®

LEADING THE IT GOVERNANCE COMMUNITY

IT Governance Institute®
The IT Governance Institute (ITGI™) (*www.itgi.org*) is a non-profit, independent research entity that provides guidance for the global business community on issues related to the governance of IT assets. ITGI was established by the non-profit membership association ISACA in 1998 to help ensure that IT delivers value and its risks are mitigated through alignment with enterprise objectives, IT resources are properly allocated, and IT performance is measured. ITGI developed *Control Objectives for Information and related Technology* (COBIT®) and Val IT™, and offers original research and case studies to help enterprise leaders and boards of directors fulfil their IT governance responsibilities and help IT professionals deliver value-adding services

Disclaimer
ITGI has designed and created this publication titled *Information Security Governance: Guidance for Information Security Managers* (the 'Work') primarily as an educational resource for chief information security officers, senior management and IT management. ITGI makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, the chief information security officers, senior management and IT management should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

Disclosure
© 2008 ITGI. 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 ITGI. Reproduction and use of all portions of this publication are permitted solely for academic, internal and non-commercial use and for consulting/advisory engagements, and must include full attribution of the material's source. No other right or permission is granted with respect to this work.

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.660.5700
Fax: +1.847.253.1443
E-mail: *info@itgi.org*
Web site: *www.itgi.org*

ISBN 978-1-933284-73-6
Information Security Governance: Guidance for Information Security Managers
Printed in the United States of America

Acknowledgements

ITGI wishes to recognise:

The Author and Researcher
W. Krag Brotby, CISM, Senior Security Consultant, USA

The Reviewers
Osman Abdel Halim Azab, CISA, CISM, Arab African International Bank, Egypt
Sunil Bhaskar Bakshi, CISA, CISM, CISSP, Deloitte Haskins & Sells, India
Jose Manuel Ballester Fernandez, CISA, CISM, Temanova, Spain
Endre Paul Bihari, CISM, GAICD, Performances Resources, Australia
Johannes Jakob Buck, CISA, CISM, CISSP, Credit Suisse, Switzerland
Luis Capua, CISM, Sigen, Argentina
Zhu Hui, CISA, CISM, CBCP, CISSP, PricewaterhouseCoopers LLP, Canada
David Taiwo Isiavwe, CISA, CISM, CISSP, FCA, UBA Plc, Nigeria
Tse Woon Kwan, Ph.D., CISA, CISM, CISSP, City University of Hong Kong, China
Michel Lambert, CISA, CISM, CARRA, Canada
Barry Lewis, CISM, CISSP, Canada
Robert May, CISA, CISM, CIA, CISSP, USA
Itamar Mor, CISM, COMSEC Consulting, Israel
Naiden Vassilev Nedelchev, CISM, Mobitel EAD, Bulgaria
Caroline Neufert, CISM, Bearing Point GmbH, Germany
Vemalasakaran Periasamy, CISM, Central Bank of Malaysia, Malaysia
Marcos Semola, CISM, Atos Origen, UK
Timothy K. Smit, CISM, CISSP, Providence Health and Services, USA
Bhavani Suresh, CISA, CISM, CISSP, Adnoc Distribution, United Arab Emirates
Eduard Louis Telders, CISM, CPP, T-Mobile, USA
Robertas Vageris, CISA, CISM, ASE.LT Plc, Lithuania
Soh Wai Yoke, CISA, CISM, Deutsche Bank, Singapore
Ghassan Toufik Youssef, CISM, Banque Audi, SAL, Lebanon

ITGI Board of Trustees
Lynn Lawton, CISA, FBCS CITP, FCA, FIIA, PIIA, KPMG LLP, UK, International President
Georges Ataya, CISA, CISM, CISSP, ICT Control sa-nv, Belgium, Vice President
Avinash Kadam, CISA, CISM, CBCP, CISSP, Miel e-Security Pvt. Ltd., India, Vice President
Howard Nicholson, CISA, City of Salisbury, Australia, Vice President
Jose Angel Peña Ibarra, Consultoria en Comunicaciones e Info., SA & CV, Mexico, Vice President
Robert E. Stroud, CA Inc., USA, Vice President
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP, USA, Vice President
Frank Yam, CISA, CIA, CCP, CFE, CFSA, FFA, FHKCS, FHKIoD, Focus Strategic Group, Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President
Everett C. Johnson Jr., CPA, Deloitte & Touche LLP (retired), USA, Past International President
Ron Saull, CSP, Great-West Life Assurance and IGM Financial, Canada, Trustee
Tony Hayes, FCPA, Queensland Government, Australia, Trustee

Security Management Committee
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd., USA, Chair
Juan Manuel Aceves Mercenario, CISA, CISM, CISSP, Cerberian, Mexico
Kent E. Anderson, CISM, Network Risk Management LLC, USA
Yonosuke Harada, CISA, CISM, CAIS, InfoCom Research Inc., and Osaka University, Japan
Yves Le Roux, CISM, CA Inc., France
Mark Lobel, CISA, CISM, CISSP, PricewaterhouseCoopers LLP, USA
Vernon Richard Poole, CISM, CGEIT, Sapphire Technologies Ltd., UK
Jo Stewart-Rattray, CISA, CISM, RSM Bird Cameron, Australia
Rolf von Roessing, CISA, CISM, CISSP, FBCI, KPMG Germany, Germany

IT Governance Committee
Tony Hayes, FCPA, Queensland Government, Australia, Chair
Max H. Blecher, Virtual Alliance, South Africa
Sushil Chatterji, Edutech, Singapore
Anil Jogani, CISA, FCA, Avon Consulting Ltd., UK
John W. Lainhart IV, CISA, CISM, CGEIT, IBM, USA
Lucio Molina Focazzio, CISA, Colombia
Ron Saull, CSP, Great-West Life Assurance and IGM Financial, Canada,
Michael Schirmbrand, Ph.D., CISA, CISM, CPA, KPMG, Austria
Robert E. Stroud, CA Inc., USA
John Thorp, CMC, ISP, The Thorp Network Inc., Canada
Wim Van Grembergen, Ph.D., University of Antwerp, University of Antwerp Management School, and IT Alignment and Governance Research Institute (ITAG), Belgium

The ITGI Affiliates and Sponsors
ISACA Chapters
American Institute for Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association of Corporate Governance Inc.
FIDA Inform
Information Security Forum
Information Systems Security Association
Institut de la Gouvernance des Systèmes d'Information
Institute of Management Accountants
ISACA
ITGI Japan
Socitm Performance Management Group
Solvay Business School
University of Antwerp Management School
Aldion Consulting Pte. Ltd.
Analytix
BWise B.V.
CA Inc.
Consult2Comply
Hewlett-Packard
IBM
ITpreneurs Nederlands BV
LogLogic Inc.
Phoenix Business and Systems Process Inc.
Project Rx Inc.
Symantec Corp.
TruArx Inc.
Wolcott Group LLC
World Pass IT Solutions

Table of Contents

1. Introduction

Information Security Governance: Guidance for Information Security Managers, a companion publication to *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*,[1] is an exposition on the rationale and necessity for senior management to integrate information security into overall organisational governance at the highest levels. It provides information developed in recent years that mandates the business case for information security governance. Although, for continuity and clarity, some of the information from the board and executive management guidance publication is summarised in this document, a review of that publication is recommended for an understanding from a high-level strategic governance perspective.

'It is no longer enough to communicate to the world of stakeholders why we exist and what constitutes success, we must also communicate how we are going to protect our existence'.[2] This suggests that a clear organisational strategy for preservation is equally important to, and must accompany, a strategy for progress.

Given the rising risks and increasing expenditures of organisational resources on information security, coupled with increasingly stringent regulations and growing liabilities, it is inevitable that information security has become a matter for consideration at the highest organisational levels. Once senior management and the board of directors have an understanding of the imperatives and benefits for undertaking the integration of information security into the organisation's governance structure, they can look to this document to provide an approach and methodology for achieving that objective.

This publication discusses how to develop an information security strategy within the organisation's governance framework and how to drive that strategy through an information security programme. It provides guidance on determining information security objectives and how to measure progress toward achieving them.

> Information security is not only a technical issue, but also a business and governance challenge that involves risk management, reporting and accountability. Effective security requires the active engagement of executive management to assess emerging threats and provide strong cybersecurity leadership. The term penned to describe executive management's engagement is **corporate governance.** Corporate governance consists of the set of policies and internal controls by which organizations, irrespective of size or form, are directed and managed. Information security governance is a subset of an organization's overall governance program. Risk management, reporting, and accountability are central features of these policies and internal controls.
>
> — The Corporate Governance Task Force, 2004, *www.cyberpartnership.org/InfoSecGov4_04.pdf*

Information security governance includes the elements required to provide senior management assurance that its direction and intent are reflected in the security posture of the organisation by utilising a structured approach to implementing an information

[1] IT Governance Institute, *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*, USA, 2006
[2] Kiely, Laree; Terry Benzel; *Systemic Security Management*, Libertas Press, USA, 2006

security programme. Once those elements are in place, senior management can be confident that adequate and effective information security will protect, as far as is possible, the organisation's vital information assets.

The objective of information security is to develop, implement and manage an information security programme that achieves the five basic outcomes identified in *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition:*

- Strategic alignment of information security with business strategy to support organisational objectives
- Effective risk management by executing appropriate measures to manage and mitigate risks and reduce potential impacts on information resources to an acceptable level
- Value delivery by optimising information security investments in support of organisational objectives
- 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 achievement of organisational objectives

Information Security

Until recently, a major focus of information security has been the protection of the IT systems that process and store the vast majority of information, rather than the information itself. But this approach is technology-centric and too narrow to accomplish the level of integration, process assurance and overall security that is now required.

Information security takes the larger view that the information and the knowledge based on it must be adequately protected regardless of how it is handled, processed, transported or stored. Information security addresses the universe of risks, benefits and processes involved with all information resources. It has become clear that information must be treated with the same care and prudence as are other critical organisational resources.

As organisations strive to remain competitive in the global economy, there are constant pressures to cut costs through automation and the deployment of more information systems. At the same time that there is growing dependence on these systems, there are also mounting risks to vital information resources threatening the existence of the enterprise.

Management must also contend with the scores of new and existing laws and regulations that are demanding compliance and higher levels of accountability.

Executive and information security management are responsible for considering and responding to these issues, and ensuring governing boards are involved in and support the appropriate course of action. Management is also obligated to ensure a comprehensive information security governance framework is effectively implemented.

To accomplish this, members of executive management must have a clear understanding of what to expect from their information security programme. They need to know how to direct the implementation of an appropriate information security programme, how to evaluate the status and effectiveness of the information security programme, and how to decide the strategy and objectives of the information security programme.

This guide, prepared by one of the world's leading institutions dedicated to researching the principles of IT governance, addresses these concerns. The guide covers such fundamental issues as:

- What is information security governance?
- What are the information security roles and responsibilities of executive management?
- What is an effective business-oriented approach to providing information security governance?
- How is an information security strategy aligned with business objectives developed?
- How is an information security strategy implemented?
- How is the effectiveness of the information security programme measured and monitored?

2. Information Security Governance Guidance

As has been discussed in the companion guide, *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*, information security is concerned with all information processes, physical and electronic, regardless of whether they involve people and technology or relationships with trading partners, customers and third parties. Information security is concerned with the comprehensive aspects of information and overall protection at all points within the life cycle of information used in the organisation.

Information security deals with all aspects of information, whether spoken, written, printed, electronic or relegated to any other medium, and regardless of whether it is being created, viewed, transported, stored or destroyed. This is contrasted with IT security, which is concerned with security of information within the boundaries of the technology domain. Typically, confidential information disclosed in an elevator conversation or sent through the postal service would be outside the scope of IT security. However, from an information security perspective, the nature and type of compromise are not important; what is important is the fact that security has been breached.

Specifically, information security relates to the protection of information assets against the risk of loss, operational discontinuity, misuse, unauthorised disclosure, inaccessibility or damage. It is also concerned with the 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.

This document addresses the need for proper alignment of information security programme activities to reinforce the understanding that information is a pervasive, critical organisational asset, and that the *ad hoc* approaches of the past will no longer serve to address current and emerging issues. As with any other business-critical activity, information security programme activities must be thoroughly planned, effectively executed and constantly monitored at the highest levels of the organisation.

> Firms operating at best-in-class (security) levels are lowering financial losses to less than 1 percent of revenue, whereas other organisations are experiencing loss rates that exceed 5 percent.
>
> — Aberdeen Group, 'Best Practices in Security Governance', USA, 2005

It is important to consider the organisational necessity and benefits of information security governance. They include:

- Protection from the increasing potential for civil or legal liability as a result of information inaccuracy, improper disclosure or the absence of due care in its protection
- Increased predictability and the reduction of uncertainty in business operations by lowering information security-related risks to definable and acceptable levels
- Assurance of an effective information security policy and policy compliance
- The structure and framework to optimise allocations of limited security resources

- A level of assurance that critical decisions are not based on faulty information
- A firm foundation for efficient and effective risk management, process improvement, and rapid incident response relating to securing information
- Accountability for safeguarding information during critical business activities such as mergers and acquisitions, business process recovery, and regulatory response
- Reduced losses from security-related events, and assurance that security incidents and breaches are not catastrophic
- Improved reputation in the market that has demonstrably resulted in increased share value

McKinsey and Company, in conjunction with Institutional Investors Inc., published in the McKinsey Quarterly studies that concluded that major international investors were willing to pay a premium for shares in a company that is known to be well governed. The premium ranged from 11 to 16 percent in 1996 to 18 to 28 percent in 2000. With the advent of regulations, such as those imposed by Sarbanes-Oxley, requiring disclosure of the effectiveness of controls and attestation to the accuracy of financial reporting, these studies suggest obvious implications for adequate and effective security governance.

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

3. Information Security Programme Requirements

To achieve significant improvements, information security must be an integral part of enterprise governance and integrated into strategy, concept, design, implementation and operation. Information security must be considered in virtually all management strategies and recognised as a crucial contributor to success.

Effective information security governance requires senior management commitment and an overall culture conducive to information security at the executive and operational levels. Too often, management determines that it is easier to buy a solution than to change a culture. The result is all too often an *ad hoc* collection of poorly integrated tactical point solutions that are increasingly difficult to manage and invariably leave gaps in protection.

Education and training in the operation of information security processes are often overlooked as well. However, management should consider that even the most secure system, if operated by ill-informed, untrained, careless or indifferent personnel, will not achieve a significant degree of security.

Information security is a top-down process requiring a comprehensive information security strategy that is explicitly linked to the organisation's business processes and objectives. For security to be effective, it must address organisational processes from end to end—physical, operational and technical.

To ensure all relevant elements of security are addressed in an organisational information security strategy, several security standards have been developed. Major resources for information security governance guidance include, but are not limited to, COBIT® 4.1, the International Organisation for Standardisation (ISO)/International Electrotechnical Commission (IEC) 27000 family of security standards, Federal Information Processing Standard (FIPS) Publication 200 and US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53.

A formal information security strategy must be implemented by developing comprehensive information security policies consistent with the main focus and purpose of the organisation. To provide effective governance, a set of enterprise standards for each policy must be developed to provide defined boundaries for acceptable processes and procedures. Education, training and awareness must also be considered to convey information to all personnel as part of an ongoing process to change behaviours not conducive to secure, reliable operations.

The strategy must then be implemented through a comprehensive information security programme that includes well-conceived and complete policies and standards. In summary, the information security programme must cover such elements as:
- Assignment of roles and responsibilities
- Periodic assessments of risks and impact analysis
- Classification and assignment of ownership of information assets
- Adequate, effective and tested controls

- Integration of security in all organisational processes
- Processes to monitor security elements
- Effective identity and access management processes for users and suppliers of information
- Meaningful metrics
- Education on information security requirements for all users, managers and board members
- Training, as appropriate, in the operation of security processes
- Development and testing of plans for continuing the business in case of interruption or disaster

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

Some aspects of a security programme may hold more relevance than others for senior management. For example, some countries, such as Australia, Canada, France, India and the US, are making the adequacy and testing of controls from a regulatory/statutory or legal perspective a focus. From a European Union (EU) privacy perspective, the additional elements required for confidentiality may be of equal or greater significance.

Even organisations not bound by regulation may have special information security considerations or objectives resulting from partnerships or contractual arrangements. In virtually all circumstances, organisations have a legal requirement to exercise due care in the protection of information assets.

Increasingly, it is incumbent on management to ensure that the foregoing responsibilities are adequately addressed by enterprise policies, standards and procedures, and adequate resources are allocated to support an effective enterprise security programme.

A comprehensive information security programme will ensure protection of information assets through a layered series of technological and non-technological safeguards and controls (i.e., physical and environmental security measures, background checks, user identifiers, passwords, smart cards, biometrics, intrusion detection systems [IDSs]/intrusion prevention systems, firewalls) as well as manual and automated procedures. These safeguards and controls are necessary and should address both 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.

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 governance framework will generally consist of:

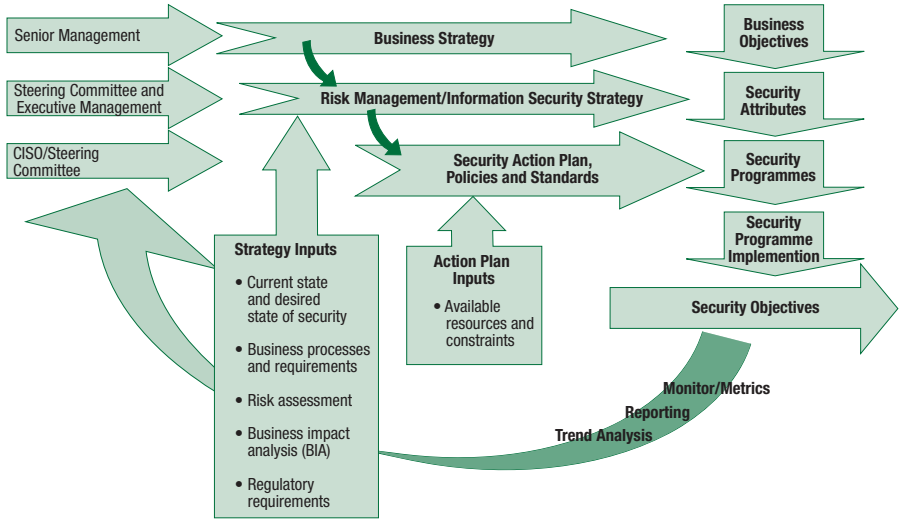
- A comprehensive information security strategy explicitly linked with IT and organisational business objectives
- An effective information security organisational structure void of conflicts of interest with appropriate authority and resources

- Governing information security policies that address each aspect of strategy, controls and regulation
- A complete set of information security standards for each policy to ensure that procedures and guidelines comply with policy
- Enterprise-specific monitoring processes to ensure compliance and provide ongoing feedback on effectiveness
- A process to ensure continued evaluation and update of the organisation's information security policies, standards and procedures
- Implementation of effective information security risk assessment methodology

This framework, in turn, provides the basis for the development of a cost-effective information security programme that supports the organisation's goals. 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 support fulfilment of this objective.

Figure 1 shows the relationships and the participants involved in developing a security strategy aligned with business objectives. The business strategy provides one of the inputs into risk management and information security strategy to promote alignment. The balance of inputs is derived from determining the desired state of security compared to the existing or current state. Business processes must also be considered, as well as the results of risk assessments and impact analysis to determine protection levels and priorities. Regulatory requirements must also be considered in developing the information security strategy.[3]

Figure 1—Information Security Governance Conceptual Framework



[3] IT Governance Institute, *op. cit.*, *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*

The objective of the information security strategy is to achieve the desired state defined by business and security attributes. The strategy provides the basis for an action plan comprised of one or more security programmes that, as implemented, achieve the information security objectives. The action plan(s) must be formulated based on available resources and constraints.

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), steering committee and management to allow for correction and ensure that information security initiatives are on track to meet defined objectives.

Information security baselines can be developed and implemented on the basis of identified and prioritised information resources that need protection. Information security baselines are the minimum acceptable security that will be provided to protect information resources. Baselines will vary depending on the sensitivity and criticality of the affected assets. Baselines can be expressed as technical, procedural and personnel standards throughout the enterprise.

Baselines are normally developed using a combination of accepted global standards and frameworks such as COBIT, ISO/IEC 27002, FIPS Publication 200 and NIST SP 800-53; legal and regulatory requirements; and decisions by the organisation about the acceptable level of risk weighed against the cost of mitigation. An example of a baseline that was created using COBIT is *COBIT® Security Baseline*,[4] available from ITGI.

Security objectives are normally met when:
- Information is available and usable, as 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 right to know (confidentiality)
- Information is protected against unauthorised modification (integrity)
- Business transactions as well as information exchanges amongst enterprise locations or with external trading partners can be trusted (authenticity and non-repudiation)

While emerging definitions 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.

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. Based on regulatory or legal requirements, confidentiality may be the most critical as it relates to personal, financial or medical information, or to the protection of trade secrets/intellectual property (IP).

[4] IT Governance Institute, *COBIT Security Baseline: An Information Security Survival Kit, 2nd Edition*, USA, 2007

The Corporate Governance Task Force has identified a core set of principles to help guide implementation of effective information security governance. Chief executive officers (CEOs) should have an annual information security evaluation conducted, review the evaluation results with staff, and report on performance to the board of directors. Organizations should:

- Conduct periodic risk assessments of information assets as part of a risk management program
- Implement policies and procedures based on risk assessments to secure information assets
- Establish a security management structure to assign explicit individual roles, responsibilities, authority and accountability
- Develop plans and initiate actions to provide adequate information security for networks, facilities, systems and information
- Treat information security as an integral part of the system life cycle
- Provide information security awareness, training and education to personnel
- Conduct periodic testing and evaluation of the effectiveness of information security policies and procedures
- Create and execute a plan for remedial action to address any information security deficiencies
- Develop and implement incident response procedures
- Establish plans, procedures and tests to provide continuity of operations
- Use security best practices guidance, such as ISO/IEC 27002, to measure information security performance

—The Corporate Governance Task Force, 'Information Security Governance: A Call to Action', 2004, *www.cyberpartnership.org/InfoSecGov4_04.pdf*

4. Roles and Responsibilities

As with other significant organisational initiatives of strategic significance, there are a variety of responsibilities that must be undertaken at various levels of the organisation to achieve effective information security governance. These range from oversight to execution. Governance tasks may be subdivided in various ways; the following delineation of roles can serve as a guide.

Executive Management

Implementing effective information security governance and defining the strategic information security objectives of an organisation are complex, arduous tasks. To succeed, they require leadership and ongoing support from executive management. It is accepted that management has an explicit obligation to ensure adequate protection of organisational assets, including information. As a result, management must consider that the requirements of a multitude of legal and regulatory rules and legal standards of due care increasingly require executive management focus and commitment, oversight, impetus, and resources.

> The foundation of the US Federal government's cybersecurity 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.
>
> — US government, The US National Strategy to Secure Cyberspace, 2003, p. 43, *www.whitehouse.gov/pcipb*

Developing and implementing an effective information security strategy also requires integration with, and co-operation of, business process owners. All too often at the operational level, the requirements of information security are seen as burdensome, inflexible, counterproductive, unprofitable and unnecessary. There are generally few visible or explicit incentives for line managers to commit resources and effort to ephemeral security objectives. Without strong support and commitment from senior management, these views often prevail and effectively sabotage security efforts. An added disincentive for most business owners is that failure of security and concomitant losses are invariably someone else's responsibility—usually the security manager's—which all but eliminates appropriate accountability. Consequently, it is imperative that senior and executive management ensure appropriate governance structures that include clarity of intent and direction, clear delineation of roles and responsibilities, adequate and effective monitoring, and suitable compliance enforcement.

Properly attended to, a successful outcome of these efforts is the alignment of information security activities in support of organisational objectives. The extent to which this is accomplished will determine the effectiveness of the information security programme in achieving the desired objective of providing a predictable, defined level of assurance for business processes and an acceptable level of impact from adverse events. It will result in optimal resource management, decreased losses from security incidents, and reduced personal and organisational liabilities.

Steering Committee

Information security affects all aspects of an organisation. To be effective, security awareness must be pervasive throughout the enterprise. To ensure that all stakeholders impacted by information security considerations are involved, many organisations use a steering committee composed of senior representatives of affected groups. This facilitates achieving consensus on priorities and trade-offs. It also serves as an effective communication channel and provides an ongoing basis for ensuring the alignment of the information security programme with business objectives. It can also be instrumental in achieving modification of behaviour toward a culture more conducive to good information security.

Many organisations utilise some form of risk council or committee. In some cases, this can be a subcommittee of the steering or executive committee. This serves to provide greater integration in the approach to overall risk management. A typical approach to continuous risk management involves identifying and prioritising risks on a periodic basis and specifically addressing the top 20 percent. Over time, this can be effective in consistently addressing the most serious risks. Since the bottom line of security is risk management, this approach also serves to achieve consensus, priority and direction for information security efforts.

Chief Information Security Officer

All organisations have a CISO, whether anyone holds that title or not. It may be *de facto* the chief information officer (CIO), chief security officer (CSO), chief financial officer (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 today is such that the authority required and the responsibility taken will inevitably end up with a C-level officer or executive manager. Legal responsibility will, by default, extend up the command structure and ultimately reside 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, and usually results in a lack of effective alignment of security activities with organisational objectives.

> Sixty percent of respondents report that their organizations employ a chief information security officer (CISO) or a chief security officer (CSO), up from 43 percent in 2006.
>
> — *CIO*, *CSO* and PricewaterhouseCoopers, 'The State of Information Security 2007, A Worldwide Study by *CIO*, *CSO* and PricewaterhouseCoopers', USA, 2007

Increasingly, prudent management is elevating the position of the 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. Management and board of directors awareness of and commitment to sound information security governance is demonstrated by ensuring that the C-level or executive position exists and is supplied with the responsibility, authority and required resources.

The number of information security managers is on the rise globally. This can be attributed to the growing awareness of the importance of this function, driven by increasingly spectacular failures of security and the growing losses that result. Unfortunately, while the number of information security managers is increasing, there is little consensus amongst organisations as to what the best reporting relationship is or what role the information security manager will play in the organisation. Responsibilities currently fall under the CISO, who reports to the CEO; to system administrators who have part-time responsibility for security management reporting within the IT organisation; or to an information security manager.

For information security to be effective, it must be aligned more closely with business than with technology.

Reporting structures for information security managers also vary widely. In the global *State of Information Security 2007* study conducted by PricewaterhouseCoopers and *CIO* and *CSO* magazines, 64 percent of respondents report that the senior information security official reports to and through an IT leader—the chief technology officer (CTO), CIO or CSO. This is up from 50 percent in 2006.[5] While this is often functionally adequate, it is unlikely to be the optimal structure and should be examined by senior management as a part of governance responsibilities. There are several reasons for this. One is that the increasingly broad requirements of information security transcend the purview of the typical CIO. Another reason is the inherent conflict of interest. Information security, due to its efforts to ensure security, is often perceived as a constraint on IT operations. CIOs and their IT departments are usually under pressure to increase performance and cut costs. Information security is often the victim of these pressures. Finally, it must be considered that for information security to be effective, it must be aligned more closely with business than with technology.

[5] *CIO, CSO* and PricewaterhouseCoopers, 'The State of Information Security 2007, A Worldwide Study by *CIO, CSO* and PricewaterhouseCoopers', USA, 2007

5. What the Board, Executive Management and Security Management Should Do

The relationship amongst the outcomes of effective security governance and management responsibilities is shown in **figure 2**. These are not meant to be comprehensive, but merely to illustrate some primary information security tasks and levels for which management is responsible.

Figure 2—Relationship of Information Security Governance Outcomes to Management Responsibilities

Management Level	Strategic Alignment	Risk Management	Value Delivery	Performance Measurement	Resource Management	Process Assurance
Board of directors	Require demonstrable alignment.	• Establish risk tolerance. • Oversee a policy of risk management. • Ensure regulatory compliance.	Require reporting of security activity costs.	Require reporting of security effectiveness.	Oversee a policy of knowledge management and resource utilisation.	Oversee a policy of assurance process integration.
Executive management	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.	Require monitoring and metrics for security activities.	Ensure processes for knowledge capture and efficiency metrics.	Provide oversight of all assurance functions and plans for integration.
Steering committee	• Review and assist security strategy and integration efforts. • Ensure that business owners support integration.	Identify emerging risks, promote business unit security practices and identify compliance issues.	Review and advise on the adequacy of security initiatives to serve business functions.	Review and advise whether security initiatives meet business objectives.	Review processes for knowledge capture and dissemination.	• Identify critical business processes and assurance providers. • Direct assurance integration efforts.
CISO/information security management	Develop the security strategy, oversee the security programme and initiatives, and liaise with business process owners for ongoing alignment.	• Ensure that risk and business impact assessments are conducted. • Develop risk mitigation strategies. • Enforce policy and regulatory compliance.	Monitor utilisation and effectiveness of security resources.	Develop and implement monitoring and metrics approaches, and direct and monitor security activities.	Develop methods for knowledge capture and dissemination, and develop metrics for effectiveness and efficiency.	• Liaise with other assurance providers. • Ensure that gaps and overlaps are identified and addressed.
Audit executives	Evaluate and report on degree of alignment.	Evaluate and report on corporate risk management practices and results.	Evaluate and report on efficiency.	Evaluate and report on degree of effectiveness of measures in place and metrics in use.	Evaluate and report on efficiency or resource management.	Evaluate and report on effectiveness of assurance processes performed by different areas of management.

6. Information Security Metrics and Monitoring

Information Security Metrics

Managing any activity that cannot be measured is generally difficult or impossible. Operational security is not readily measured in any absolute sense; rather, attributes, effects and consequences are normally the gauge. In some organisations, probability is assigned to risks and occurrences, and an estimate is made of likely annual loss expectancy (ALE). These often wildly speculative numbers are then used as a basis for allocating or justifying resources for security activities.

Standard information security metrics include such items as downtime due to viruses or Trojans, number of penetrations of systems, impacts and losses, recovery times, number of vulnerabilities uncovered with network scans, and percentage of servers patched. While these measures can be indicative of aspects of security, none provides information about how 'secure' the organisation is overall.

Often, an effort is made to determine the maximum impacts of potential adverse events as a yardstick of security. Measuring 'security' by consequences and impacts is like gauging how tall a tree is by how loud a noise it makes when it falls. In other words, adverse events are necessary to determine whether security is working. An absence of adverse events provides no information on the state of information security. It may mean that defences worked, or it may mean that no one attacked, or it may mean that a vulnerability was not discovered.

Of course, simulated attacks with penetration testing will provide only some measure of the effectiveness of defences against those specific attacks performed. Unless a statistically relevant percentage of all possible attacks are attempted, no prediction can be made about the state of security and the organisation's ability to resist attack.

All that can be stated with certainty about information security is that:
- Some organisations are attacked more frequently and/or suffer greater losses than others
- There is a strong correlation between good information security management and practices, and relatively fewer incidents and losses

Good management is arguably one result of good governance. Measuring effective information security governance and management with any precision may be more difficult than measuring 'security', and metrics will, in most respects, be based on attributes, costs and subsequent outcomes of the security programme.

A sensible notion suggests that a well-governed information security programme can be characterised as one that efficiently, effectively and consistently meets expectations and attains defined objectives. This is, however, of little help to most organisations since it is unclear what the expectations or objectives of information security are in any specific sense.

Commercial efforts to 'measure' good governance by organisations such as Institutional Shareholder Services (ISS) and Governance Metrics International (GMI) have not stood up well to scrutiny, according to a Yale report titled 'Good Governance and the Misleading Myths of Bad Metrics'.[6] The report details studies showing that many, but not all, apparently sound governance notions are not supported by fact. However, the converse is also true; many governance 'notions' are, indeed, supported by fact.

Because governance, in general, and information security governance, in particular, is difficult to measure by a set of objective metrics, there is a tendency to use metrics that are available regardless of demonstrated relevancy. A typical example apparent in most organisations is vulnerability scans. Arguably, if it were possible to eliminate all or most vulnerabilities (which it is not), most risks could be avoided. The fallacy is the assumption that something can be determined about risk, threat or impact by measuring technical vulnerabilities.

It is obvious that there is no universal objective scale for information security or information security governance. For an organisation that has determined the goal or objectives of information security, as discussed previously, the problem of metrics becomes somewhat simpler. Metrics can be reduced to any measure of the results of the information security programme progressing toward the defined objectives. With this approach, useful guidance to developing organisation-specific metrics is possible from organisations such as ISACA, CERT, Information Security Forum (ISF), ISO and NIST.

Governance Implementation Metrics

Implementing an effective information security governance strategy and framework usually requires significant effort and commitment of resources; therefore, it is important that some form of metrics be in place during the implementation of the governance programme. Performance of the overall information security programme will be too far downstream to provide timely information on implementation; therefore, another approach must be used. Key goal indicators (KGIs) and key performance indicators (KPIs) can be useful in providing information about the achievement of process or service goals and can determine whether organisational milestones and objectives are being met.

Strategic Alignment

Strategic alignment of information security in support of organisational objectives is a highly desirable goal that is often difficult to achieve. It should be clear that the cost-effectiveness of the information security programme inevitably is tied to how well it supports the objectives of the organisation and at what cost. Without organisational objectives as a reference point, any other gauge, including so-called 'best practices', may be overkill, inadequate or misdirected. From a business perspective, 'adequate and sufficient' practices proportionate to the requirements are likely to be more cost-effective than 'best' practices. They are also likely to be received better by cost-conscious management.

[6] Sonnenfeld, Jeffrey; 'Good Governance and the Misleading Myths of Bad Metrics', *Academy of Management Executive*, Academy of Management, vol. 18, no.1, 2004

The best overall indicator of information security activities in alignment with business (or organisational) objectives is the development of an information security strategy that defines information security objectives in business terms and ensures the objectives are directly articulated from planning through implementation of policies, standards, procedures, processes and technology. The acid test is the ability to conduct a reverse-order evaluation of a specific control to track it to a specific business requirement. Any control that cannot be tracked directly back to a specific business requirement is suspect and should be analysed for relevancy and possible elimination.

Indicators of alignment can include:
- The information security programme demonstrably enables specific business activities.
- The information security organisation is responsive to defined business requirements.
- The organisational and information security objectives are defined and clearly understood by all involved in information security and related assurance activities.
- The information security programme is mapped to the organisational objectives, and executive management has validated this mapping.
- There is an information security steering committee consisting of key executives with a charter to ensure ongoing alignment of information security activities and business strategy.

Risk Management

Risk management is the ultimate objective of all information security activities and, indeed, all organisational assurance efforts. While risk management effectiveness is not subject to direct measurement, there are indicators that correlate well with a successful approach. A successful risk management programme can be defined as one that efficiently, effectively and consistently meets expectations and attains defined objectives.

Once again, it is a requirement that expectations and objectives of risk management be defined; otherwise, there is no basis for determining whether the programme is succeeding or heading in the right direction, or resource allocations are appropriate.

Indicators of appropriate risk management include:
- Organisational 'risk appetite' or risk tolerance is defined in terms relevant to the organisation.
- An overall information security strategy and programme for achieving acceptable levels of risk exist.
- Mitigation objectives for identified significant risks are defined.
- Processes for management or reduction of adverse impacts exist.
- Systematic, continuous risk management processes exist.
- Trends of periodic risk assessment indicate progress towards defined goals.
- Impacts are reviewed for trends.
- A tested business continuity plan (BCP)/disaster recovery plan (DRP) exists.
- Complete asset valuation and assignment of ownership exist.
- Recovery time objectives (RTOs) for all critical systems are developed.

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

The key goal of information security is to reduce adverse impacts on the organisation to an acceptable level and ensure the preservation of the business. Therefore, key metrics are the extent and number of adverse impacts of information security incidents experienced by the organisation. An effective security programme will show a trend in impact reduction. Quantitative measures can include trend analysis of impacts over time.

Value Delivery

Value delivery occurs when information security investments are optimised in support of organisational objectives. Value delivery is a function of the strategic alignment of the information security strategy and business objectives—in other words, when a business case can be convincingly made for all information security activities. Optimal investment levels arise when strategic goals for information security are achieved, and an acceptable risk posture is attained at the lowest possible cost.

Key indicators include:

- Information security activities are designed to achieve specific strategic objectives.
- The cost of security is proportional to the value of assets.
- Information security resources are allocated by degree of assessed risk and potential impact.
- Protection costs are aggregated as a function of revenues or asset valuation.
- Controls are designed well, based on defined control objectives, and are fully utilised.
- The number of controls to achieve acceptable risk and impact levels is adequate and appropriate.
- Control effectiveness is determined by periodic testing.
- Policies are in place that require all controls to be re-evaluated periodically for cost, compliance and effectiveness.

Resource Management

Information security resource management is the term used to describe the processes to plan, allocate and control information security resources, including people, processes and technologies for improving the efficiency and effectiveness of business solutions.

As with other organisational assets and resources, information security resources must be managed properly. Knowledge must be captured, disseminated and available when needed. Providing multiple solutions to the same problem is obviously not efficient and indicates a lack of resource management. Controls and processes must be standardised, when possible, to reduce administrative and training costs. Problems and solutions must be well documented, referenced and available.

Indicators of effective resource management include:
- Problem recurrence is infrequent.
- Knowledge capture and dissemination are effective.
- Processes are standardised.
- Roles and responsibilities for information security functions are clearly defined.
- Information security functions are incorporated into every project plan.
- Information assets and related threats are covered by security resources.
- The appropriate location in the organisational structure, level of authority and number of personnel for the information security function exist.

Performance Measurement

Measuring, monitoring and reporting on information security processes are requirements to ensure that organisational objectives are achieved. The maxim states 'you cannot manage what you cannot measure'. Methods to monitor information security-related events across the organisation must be developed, and metrics that provide an indication of the performance of the security 'machinery' must be designed. The ideal of a 'security dashboard' has not yet been realised, and most measures are indirect indicators of the state of information security and performance of the information security programme.

Indicators of effective performance measurement may include the:
- Time it takes to detect and report information security-related incidents
- Number and frequency of subsequently discovered unreported incidents
- Benchmarks with comparable organisations for costs and effectiveness
- Ability to determine the effectiveness and efficiency of controls
- Clear indication that information security objectives are being met
- Absence of unexpected information security events
- Knowledge of impending threats
- Effective means of determining organisational vulnerabilities
- Methods of tracking evolving risks
- Consistency of log review practices
- Results of BCP/DRP tests

Assurance Process Integration (Convergence)

An area of emerging conceptual interest related to a suggested outcome of information security governance is business process assurance or assurance integration.

Most organisations utilise numerous assurance processes in unintegrated 'silos'. These activities are often related to information security but operate more or less independently. This lack of integration demonstrably and needlessly creates a number of often unidentified risks that should be addressed. An approach to information security governance that includes an effort to integrate these disparate assurance functions should be considered to ensure that processes operate as intended from end to end, thereby minimising hidden risks.

In the past, management of the risk inherent in a business was a function embedded within the individual roles of the 'C-suite'. The traditional approach was to treat individual risks separately and assign responsibility to an individual or small team. Managing a singular kind of risk became a distinct job, and performing that job well meant focusing exclusively on that one particular area. The problem with this stovepiped approach is that it not only ignores the interdependence of many business risks but also suboptimizes the financing of total risk for an enterprise.

Breaking stovepipes and addressing the suboptimizing of investments requires a new way of thinking about the problem. This new thinking brings together the various stakeholders in the problem set to work closely together. A major objective of this study is to understand how leading organizations bring together diverse elements and get them to orient on a common objective.[7]

Indicators for integration of diverse security-related functions may include:
- 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.
- All assurance functions are identified and considered in the strategy.

[7] Booz Allen Hamilton, 'Convergence of Enterprise Security Organizations', USA, 2005, page 3

7. Establishing Information Security Governance

The notion that information security governance is of sufficient importance to warrant senior management attention is becoming more common in organisations. A 2006 ISACA survey indicated that 72 percent of the organisations surveyed had either completed or initiated an information security governance programme. This same survey demonstrated why information security governance is important, and the benefits that can be obtained. In relation to strategic alignment, resource management, risk management, performance measurement, value delivery and regulatory compliance, those organisations that had implemented information security governance performed markedly better than those who had not.[8]

For organisations with a robust, effective information security programme in place, a significant amount of the work most likely has already been accomplished. The primary efforts will be in developing a strategy and road map aligned with and supportive of the organisation's business objectives and attempting to integrate existing programmes into the strategy.

For organisations in the initial phases of developing an information security programme, implementing well-developed information security governance makes the information security programme more effective. It can optimise alignment with and support of the organisation's business objectives.

An Information Security Strategy

There are many definitions of 'strategy'. While they all point in the same direction, they vary widely in scope, emphasis and detail. One representative statement of what is required for an information security strategy is:

> *Corporate strategy is the pattern of decisions in a company that determines and reveals its objectives, purposes, or goals, produces the principal policies and plans for achieving those goals, and defines the range of business the company is to pursue, the kind of economic and human organization it is or intends to be, and the nature of the economic and non-economic contribution it intends to make to its shareholders, employees, customers and communities.*[9]

A recent report from McKinsey[10] poses the caution that often the 'approach to strategy involves the mistaken assumption that a predictable path to the future can be paved from the experience of the past'. It goes on to suggest that strategic outcomes cannot be predetermined, given today's turbulent business environment.

---

[8] Pironti, John; 'Information Security Governance: Motivations, Benefits and Outcomes', *Information Systems Control Journal*, vol. 4, ISACA, USA, 2006

[9] Andrews, Kenneth; *The Concept of Corporate Strategy, 2nd Edition*, Dow-Jones Irwin, USA, 1980

[10] McKinsey & Company, 'Strategy: Executive Insight', USA, *www.mckinsey.com/clientservice/strategy/insight.asp*

As a result, McKinsey proposes defining strategy as a 'coherent and evolving portfolio of initiatives to drive shareholder value and long-term performance'. This change in thinking requires management to develop a 'you are what you do' perspective, as opposed to 'you are what you say'. In other words, companies are defined by the initiatives they prioritise and drive, not merely by mission and vision statements.

According to the report, 'Strategy approached in this way is by its very nature more adaptive and less dependent upon big bets'. By creating a portfolio of initiatives around a unifying theme and reinforcing it by branding, an engaging value proposition for customers and solid operational skills, a company can successfully set the stage to drive shareholder value.

Whichever definition or approach is appropriate to a particular organisation, the implementation steps remain essentially the same. The 'adaptive' McKinsey model may be more appropriate to organisations experiencing a great deal of change. The more traditional model may achieve the same adaptability by increasing the monitoring of key performance indicators and reviewing strategy suppositions more frequently.

The arguably more important criteria for good outcomes from a successful strategy are strong, ongoing senior management leadership and their commitment to achieving effective information security governance.

CIOs are coming to the conclusion that the biggest benefit of IT governance is that no one has gone to prison yet. There is no doubt that complying with the US Sarbanes-Oxley Act and keeping senior executives out of trouble are key drivers behind many IT governance projects. Nevertheless, 'the greatest operational payback often comes from improving asset and resource management', says Melinda Bailou, an analyst at IDC, an IT research firm in Framingham, Massachusetts (USA). 'There is a lot of politicisation around resource allocation, with different groups vying for the same constrained resources', she explains. 'Unfortunately, most organisations barely have an inventory of their applications'.[11]

[11] Hildreth, Sue; 'IT Governance: Business in the Driver's Seat', *Computerworld*, 2005

8. Information Security Objectives

The Goal

The first, and often surprisingly difficult, question that must be answered by an organisation seeking to develop an information security strategy is, what is the goal?

While this seems a trivial question, most organisations fail to define the objectives of information security with any specificity. This may be because it seems obvious that the goal of information security is to protect the organisation's information assets. However, that answer assumes knowledge of two things:

- Information assets are known with a degree of precision, which for most organisations is not the case.
- There is an accepted understanding of what it means 'to protect'.

While the goal of information security is generally understood, it is considerably more difficult to state which assets need how much protection against what. In part, this is because organisations typically have little knowledge of what information exists within the enterprise. There is generally no process to purge useless, outdated, or potentially dangerous information, data or unused applications. It is extremely rare to find a comprehensive catalogue or index of information or a process to define what is important and what is not, or even who 'owns' it. As a result, everything typically gets saved under the assumption that storage is cheaper than data classification, ownership assignment and the identification of users. For large organisations, this can amount to terabytes of useless data and literally thousands of outdated and unused applications accumulated over decades.

This situation makes it difficult to devise a rational data protection plan since it arguably makes little sense to expend resources protecting useless or dangerous data and information or unused applications. Dangerous data in this context constitute information that might be used to the detriment of the organisation, such as damaging evidence obtained in litigation that could have been destroyed subject to a legal and appropriate retention policy.

Classification and Valuation

Assuming current relevant information is located and identified, it must be catalogued or classified as to criticality and sensitivity. A great deal of a typical organisation's data and information is neither critical nor sensitive and it is wasteful to expend substantial resources to protect it. For many organisations, cataloguing and classifying information may be a significant undertaking, and management may be reluctant to allocate the resources necessary. However, it must be considered a crucial step in developing a practical and useful information security strategy and a cost-effective security programme.

For most organisations, asset classification poses a daunting task that will grow exponentially more onerous over time, unless addressed.

Just as values are assigned to an organisation's physical resources, values must be assigned to information to prioritise budget-constrained protection efforts and determine required levels of protection. Valuation of information is, in most cases, difficult to do with any precision. For some information, it can be the cost of creating or replacing it. In other cases, information in the form of knowledge or trade secrets is difficult or impossible to replace and may literally be priceless. It is obviously prudent to provide excellent protection for 'priceless' information.

One approach that has been used is to create a few rough levels of value, for example, from zero to five, with zero signifying no value and five signifying a critical value. A zero value would be assigned where no owner can be determined and no use has been evidenced for a period of time. Information of zero value can be archived for a specified period, notices can be sent to business owners and, if there are no objections, the zero value information can be destroyed. Information deemed a five, or critical, obviously becomes the priority for protection efforts.

Another approach that may be useful and substantially easier to perform is a business dependency evaluation as an indication of value. This process starts by defining critical business processes and then determines which information is used and created. This provides a measure of the level of criticality of information resources that can be used as a guide for protection efforts.

Regardless of the methods used, the level of sensitivity must be defined at the same time to determine a classification level needed to control access and limit disclosure. Typically, most organisations use three or four sensitivity classifications such as confidential, internal use and public.

For most organisations, asset classification poses a daunting task that must be undertaken for existing information, if security governance is to be effective and relevant. It is also a task that will grow exponentially more onerous over time, unless addressed. Concurrently, policies, standards and processes must be developed to mandate classification moving forward to prevent the problem from getting worse.

In summary, it will not be possible to develop a cost-effective information security strategy that is aligned with business requirements prior to:
- Determining the objectives of information security
- Locating and identifying information assets and resources
- Assigning value to information assets and resources
- Classifying information assets as to criticality and sensitivity

Deferred Information Maintenance

Most organisations have taken years or decades to create terabytes of data, and the problem of useless, outdated or dangerous information is unlikely to be resolved quickly. However, delaying resolution will only compound the problem and increase the ultimate cost. The deferred maintenance should be recorded as a liability on the books. Gartner estimates that, within the next decade, businesses will need to deal with 30 times as much information as they do now.

One approach to resolve the problem is to have the information security strategy include the goal of clearing out the 'information attic' over time. In conjunction with this goal, the strategy should set the additional goal of not compounding the problem by allowing these practices, or lack of them, to continue. This includes creating and implementing information ownership policies as well as data retention and destruction policies.

From the perspective of making a business case for getting data under control, it may be useful to realise that a number of organisations have suffered significant financial losses in the course of legal actions when the opposing side located incriminating e-mails and other data that should have been subject to a data destruction policy.

9. Strategy

Defining Objectives

It is axiomatic that if you do not know where you are going, you cannot find a way to get there and will not know if you have arrived.

If an information security strategy is the basis for a plan of action to achieve security objectives, it obviously is necessary to define those objectives. Defining long-term objectives in terms of a 'desired state' of security is necessary for a number of reasons. Without a well-articulated vision of desired outcomes for an information security programme, it will not be possible to develop a meaningful strategy. It is axiomatic that if you do not know where you are going, you cannot find a way to get there and will not know if you have arrived.

Without a strategy, it also is not possible to develop a meaningful plan of action and the organisation will continue to implement *ad hoc* tactical point solutions. As a result, there is no way to provide overall integration, and the resulting unintegrated systems will become increasingly difficult to manage, more costly, and difficult or impossible to secure.

Unfortunately, many organisations do not allocate adequate resources to address these issues until a major incident occurs. Experience shows that these incidents often end up far more costly than addressing them would have been.

Many business objectives related to information protection are stated in terms of mitigating or managing risks. Information security strategy objectives should also be stated in terms of specific goals directly aimed at supporting business activities. Some risk mitigation will apply to the organisation generally, such as virus and other malware protection. Such protection is usually not considered a specific business enabler; rather, it supports the overall health of the organisation by reducing adverse impacts that hinder business.

A review of the organisation's strategic business plan is likely to uncover opportunities for information security activities to be directly supportive of, or to enable, a particular avenue of business. For example, the implementation of a public key infrastructure (PKI) can enable high-value transactions with trusted trading partners or customers. Deploying virtual private networks (VPNs) may provide the sales force with secure remote connectivity, enabling improved performance. In other words, information security can enable business activities that would otherwise be too risky to undertake or, as more frequently happens, are undertaken with the hope that nothing goes wrong.

> *Developing and maintaining an information security strategy is essential to the success of your program. This strategy serves as the road map for establishing your program and adapting it to future challenges. By following a consistent methodology for developing your strategy, you are more likely to achieve high-quality results during the process and complete the project in a timely manner.*[12]

> *Security's rising profile is encouraging. According to the global* State of Information Security Study 2007 *conducted by PricewaterhouseCoopers and* CSO *and* CIO *magazines, 57 percent of respondents now say that their organization has an overall security strategy in place. This is up from 37 percent in 2006.*[13]

The Desired State

The term 'desired state' is used to denote a complete snapshot of all relevant conditions at a particular point in time. This includes people, processes and technologies.

Defining a 'state of security' in purely quantitative terms is not possible. Consequently, a 'desired state of security' must be defined qualitatively in terms of attributes, characteristics and outcomes. It can include high-level objectives such as:

> *Protecting the interests of those relying on information, and the systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality and integrity.*[14]

Qualitative elements such as desired outcomes should be defined as precisely as possible to provide guidance to strategy development. For example, if specific regulatory compliance is a desired outcome, a significant number of technical and process requirements become apparent.

If characteristics include a non-threatening compliance enforcement approach consistent with the organisation's culture, strategy development will define limits on the types of enforcement methods to consider.

A number of useful approaches are available to provide a framework to achieve a well-defined desired state for security. These, and perhaps others, should be evaluated to determine which provides the best form, fit and function for the organisation. It may be useful to combine several different frameworks to provide a multidimensional view into the desired state.

Several of the most accepted approaches are described briefly in the following sections.

---

[12] Mather, Tim; Mark Egan; *Developing Your Information Security Program*, Prentice Hall PTR, USA, 10 December 2004, *www.phptr.com/index.asp?rl=1*

[13] *CIO*, *CSO* and PricewaterhouseCoopers, *op. cit.*

[14] IT Governance Institute, *op. cit*., *COBIT Security Baseline*

CobiT

CobiT defines 34 processes for information and the technology that supports it. The processes are divided into four domains: Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate. Although there is a specific focus on information technology, the elements are generally relevant to information security governance and should be considered a powerful approach.

ITGI and CobiT Maturity Scale

The desired state of security may also be defined as achieving a specific level in the maturity scale. It consists of grading each defined area of security on a scale of zero to five based on the 'maturity' of processes. This approach is presented in detail in appendix B, Self-assessment and maturity model. The maturity levels are described in **figure 3**.

Figure 3—ITGI and CobiT Maturity Scale

Maturity Level	Description
0	Non-existent—No recognition by organisation of need for security
1	Initial/*ad hoc*—Risks considered on an *ad hoc* basis; no formal processes
2	Repeatable but intuitive—Emerging understanding of risk and need for security
3	Defined process—Company-wide risk management policy/security awareness
4	Managed and measurable—Risk assessment standard procedure; roles and responsibilities assigned; policies and standards in place
5	Optimised—Organisation-wide processes implemented, monitored and managed

Balanced Scorecard

As shown in **figure 4**, the balanced scorecard (BSC) uses four perspectives. The BSC develops metrics, collects data and analyses the data relative to each of these perspectives:

- Learning and growth
- Business process
- Financial
- Customer

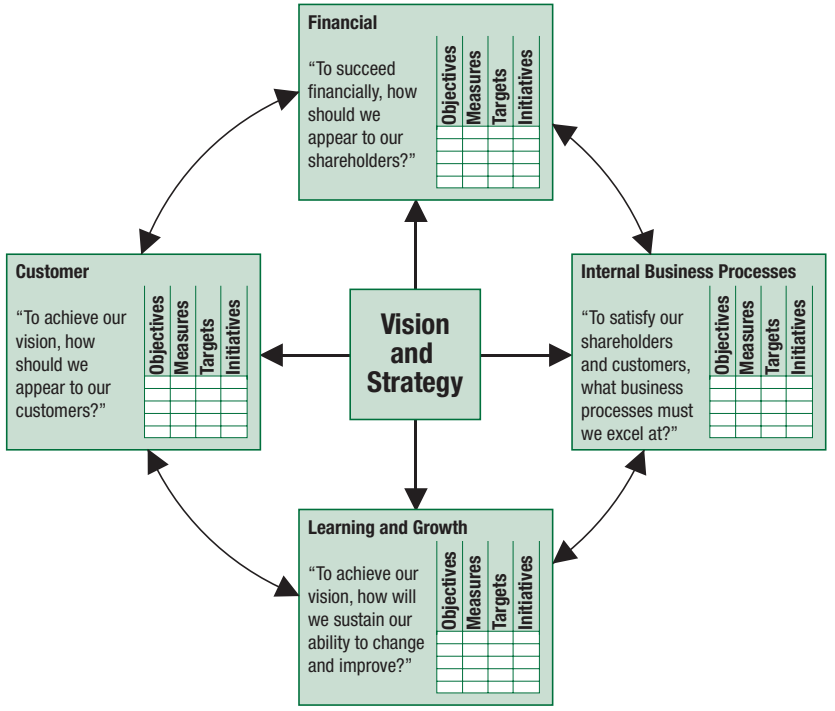
> *The balanced scorecard is a management system (not only a measurement system) that enables organizations to clarify their vision and strategy and translate them into action. It provides feedback around both the internal business processes and external outcomes in order to continuously improve strategic performance and results. When fully deployed, the balanced scorecard transforms strategic planning from an academic exercise into the nerve center of an enterprise.*[15]

Sherwood Applied Business Security Architecture

The key to success in the Sherwood Applied Business Security Architecture (SABSA®) methodology is to be business-driven and business-focused. The business strategy, objectives, relationships, risks, constraints and enablers tell much about what sort of security architecture the organisation needs. This analysis and the description of the business itself are called the contextual security architecture.

[15] Balanced Scorecard Institute, Washington DC, USA, *http://balancedscorecard.org/basics/bsc1.html*

Figure 4—Balanced Scorecard Perspectives[16]



Reprinted with permission from the Balanced Scorecard Institute and Pavel Arveson

As shown in **figure 5**, SABSA uses a matrix of business drivers and attributes to describe the objectives of security from an architectural perspective. Architecture should be an expression of strategy and, therefore, the attributes apply to both. This approach also emphasises traceability from strategy through execution.

ISO/IEC 27002

To ensure that all relevant elements of information security are addressed in an organisational security strategy, the 11 areas of ISO/IEC 27002 can provide a useful framework to gauge comprehensiveness. Similarly, policies and standards must be created that can track directly to each element of the standard.

The 11 major headings of ISO/IEC 27002 are:
- Information security policy
- Organising information security
- Asset management
- Human resources (HR) security
- Physical and environmental security
- Communications and operations management

[16] *Ibid*.

Figure 5—SABSA Matrix

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The business	Business risk model	Business process model	Business organisation and relationships	Business geography	Business time dependencies
Conceptual	Business attributes profile	Control objectives	Security strategies and architectural layering	Security entity model and trust framework	Security domain model	Security-related lifetimes and deadlines
Logical	Business information model	Security policies	Security services	Entity schema and privilege profiles	Security domain definitions and associations	Security processing cycle
Physical	Business data model	Security rules, practices and procedures	Security mechanisms	Users, applications and the user interface	Platform and network infrastructure	Control structure execution
Component	Detailed data structures	Security standards	Security products and tools	Identities, functions, actions and ACLs*	Processes, nodes, addresses and protocols	Security step timing and sequencing
Operational	Assurance of operational continuity	Operational risk management	Security service management and support	Application and user management and support	Security of sites, networks and platforms	Security operations schedule

*Access control lists
© 1995 to 2008 Sherwood Applied Business Security Architecture. All rights reserved. Used with permission.

- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance

Other Approaches

Other approaches and methods exist that may be useful, such as some of the other ISO standards on quality (9001-2000), publications from NIST, the ISF, US Federal Information Security Management Act (FISMA), and IDEAL from the Software Engineering Institute (SEI) of Carnegie Mellon University. Some of these approaches and methods focus more on management processes than on strategic information security objectives, although a valid argument could be made that if the objective of a security strategy is to fully implement relevant components of ISO/IEC 27002, all security requirements are likely to have been met. That would likely be a needlessly expensive approach and the standard itself suggests that it be carefully tailored to the specific requirements of the adopting organisation. Other methodologies will undoubtedly emerge in the future that may prove more effective than the ones mentioned. Those outlined are not meant to constitute an exhaustive list; they are merely some of the more widely accepted approaches used to arrive at well-defined information security objectives.

It may be useful to employ a combination of methods to describe the desired state to assist in communications with others and as a way to cross-check the objectives to ascertain that all relevant elements are considered. For example, a combination of CobiT control objectives, CMM, BSC and SABSA would make a powerful combination. While it may seem like overkill, each approach presents a different viewpoint. In combination, they are likely to ensure that no significant aspect is overlooked. Since it is unlikely that an effective security programme will evolve from a faulty strategy, this may be a prudent approach.

It is unlikely that an effective information security programme will devolve from a faulty strategy.

Risk Objectives

A major input into defining the desired state is the organisation's approach to risk and its risk appetite, that is, what management considers acceptable risk. It is vital to define acceptable risk, although often difficult to do without thorough consideration. This is, however, another critical step, since defined acceptable risk will evolve into the control objectives or other risk mitigation measures employed. Control objectives will, in turn, be instrumental in determining the type, nature and extent of controls and countermeasures the organisation will employ to manage risk.

It must be remembered that risk is a complex subject and often difficult to ascertain with precision.

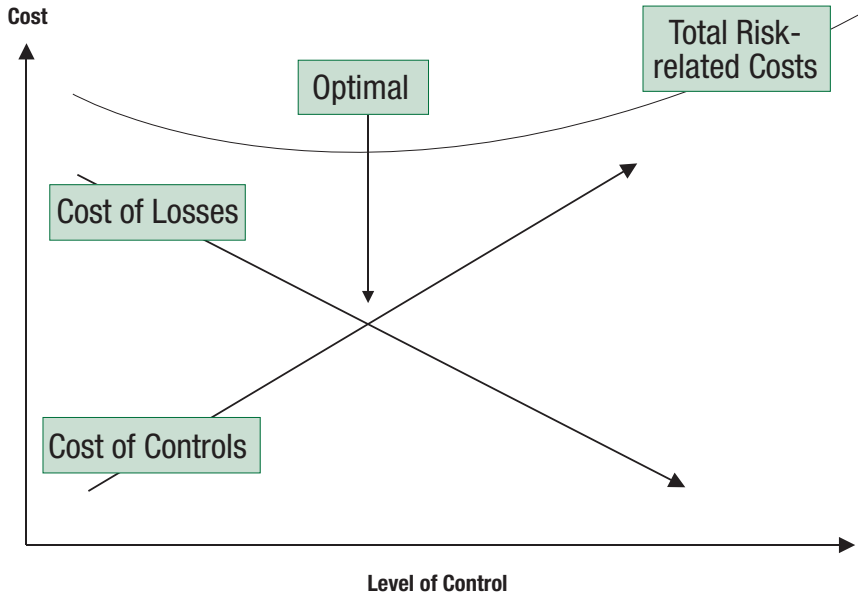
> *Operational risk management is a trade-off—if there is a risk associated with taking a particular course of action, there is also a risk of not doing so. Furthermore, individual risks interact in complex ways, and if you mitigate one risk you almost certainly increase at least one other risk in response.*
>
> *Risks always carry a cost, whether controlled or not. Risk cost can be expressed as annual loss expectancy (ALE). ALE is calculated as the amount of potential loss times the likelihood of occurrence. [ALE will equal the (cost of controls) + (residual risk cost × likelihood).]* ***Figure 6*** *illustrates the balance of the cost of controls against the cost of losses.*[17]

Number of Controls

One way to approach the acceptable-risk question is to develop RTOs for critical business systems. A broad-brush approach may provide input needed for strategy development. This can be an informal determination by business process owners of the amount of time critical systems can be inoperative without serious business consequences. This, in turn, will provide the basis for approximating costs of achieving the desired recovery times. If this estimate is considered too costly, iteration of the process will arrive at an acceptable recovery time at an acceptable cost. This, then, may be considered the acceptable risk at an acceptable cost.

[17] Sherwood, John; Andrew Clark; David Lynas; *SABSA Enterprise Security Architecture*, CMP, USA, 2005

Figure 6—Optimising Risk Costs



© 2005 Sherwood Applied Business Security Architecture. All rights reserved. Used with permission

Developing most elements of the right strategy objectives requires an iterative approach based on analysis of costs, to achieve the desired state and achieve acceptable risk levels. It is likely that lowering the level of acceptable risk will be more costly, but that is not always the case. The approaches used in treating risk and achieving the desired state will have a significant bearing on the costs of implementing and maintaining the information security programme.

For example, some risks may exist because of certain practices that are not necessary or useful to the organisation or are, in fact, detrimental to its operation. This could include practices that might be considered discriminatory or contrary to law and pose the risk of a lawsuit—practices that, when examined, may be determined to have resulted from outmoded attitudes or approaches that could have been changed at low cost, resulting in elimination or mitigation of the risk. In other words, the approach to addressing or treating specific risks will have a significant impact on costs.

From a strategy point of view, all options for treating risks should be considered. These include controls and countermeasures, changes in risky behaviours, transferring risks where appropriate, and accepting certain risks. It must be understood that technical controls (e.g., firewalls, IDSs) are merely one dimension to be considered. Physical, process, and procedural controls or countermeasures may be more effective and less costly. In most organisations, process risks pose the greatest hazard. Failures of process are inevitably failures of management and normally cannot be addressed by technical means.

Once risk objectives have been defined, there are a number of ways to architect solutions that will vary significantly in cost and complexity. Whichever process is used, the requirement is to define in meaningful, concrete terms the desired overall state of security at some future point. The desired state must be meaningful and concrete in the sense that the process is reasonable and can be achieved and effectively monitored, and progress and the results can be measured in a useful way.

Current State of Security

A current-state evaluation of information security must also be determined using the same methodologies or combination of methodologies employed to determine strategy objectives, or desired state. In other words, whichever combination of COBIT, CMM, BSC, etc., is used to define the desired state must also be used to determine the current state. This will provide an apples-to-apples comparison between the two, providing the basis for a gap analysis, which will delineate what is needed to achieve the objectives.

Using these same methodologies periodically will also provide the metrics on progress toward meeting the objectives as well as an information security baseline. As has been stated previously, one cannot manage what one cannot measure.

The current state of risk must also be assessed through a comprehensive risk assessment. Just as risk objectives must be determined as a part of the desired state, the current state of risk must be determined to provide the basis for a gap analysis that addresses risks by the strategy and the extent. A full risk assessment includes threat and vulnerability analysis, which individually provides useful information in building a strategy as well. Since risks can be addressed in different ways—such as altering risky behaviour, developing countermeasures to threats, reducing vulnerabilities or developing controls—this information will provide the basis for determining the most cost-effective strategy to address risks. Additional periodic assessments likewise will provide the needed metrics to determine progress.

The current-state evaluation should also include a thorough business impact analysis (BIA) to help round out the current-state picture. Since the ultimate objective of information security is to provide business process assurance and minimise the impacts of adverse events, an impact analysis provides some of the information needed to develop an effective strategy. The difference between acceptable levels of impact and the current level of potential impacts must be addressed by the strategy.

10. The Strategy

Re-engineering a process can mitigate or eliminate a risk without the need for controls.

The original meaning of 'strategy', a military term, is the plan to achieve an objective. For the purpose of implementing an information security programme strategy, this is a straightforward working definition. At this juncture, the current state and the desired state of security have been determined using one or more methodologies. The desired state has been defined by attributes and characteristics. Current risk has been assessed and an approach to determine acceptable risk, or desired state of risk, has been defined. In other words, the information security programme objectives can now be coupled with available processes, methods, tools and techniques to create the means to construct an information security programme strategy.

A good information security strategy should address and mitigate risks while complying with the legal, contractual and statutory requirements of the business; provide demonstrable support for the business objectives of the organisation; and maximise value to the stakeholders. The strategy should provide a sound basis for resource allocation and address how the organisation will embed good security practices into every business process and area of the enterprise. Often, those responsible for developing an information security strategy think in terms of controls as the means to establish security. Controls, while important, are not the only element available to the strategist. Countermeasures may, in many cases, be a more cost-effective treatment. In some cases, re-engineering a process can mitigate or eliminate a risk without the need for controls. Potential impacts may be reduced by architectural modifications rather than controls. It should also be considered that, in some cases, mitigating risks can reduce opportunities to the extent of being counterproductive.

Information is an asset to an organisation only to the extent that it supports the business objectives.

Ultimately, the goal of information security is business process assurance, regardless of the business. While the business of a government agency may not result directly in profits, it is, nevertheless, in the business of providing cost-effective services to its constituency and must protect the assets for which it has custodial care. Whatever the business, its primary operational goal is to maximise the success of business processes and minimise impediments to those processes.

Some might argue that the primary goal of information security is to protect information assets. However, information is an asset only insofar as it supports the primary purpose of the business, generating revenues (or cost-effective services) through value-add processes. All other information is, to some extent, a liability. As some organisations have discovered, information that should have been subject to a retention and destruction policy turned out to be a major liability when incriminating e-mails were discovered by the opposition in a lawsuit. Even if not incriminating, useless data consume resources and are a liability.

Elements of a Strategy

What should go into an information security strategy? The starting point and the destination have been defined. The next consideration must be what resources are available and what constraints must be considered when developing the road map. The resources are the mechanisms that will be used to achieve various parts of the strategy.

The available resources need to be enumerated and considered. They typically include:
- Policies
- Standards
- Processes
- Methods
- Controls
- Technologies
- People
- Skills
- Training
- Education
- Other organisational support and assurance providers

There will also be constraints to a strategy and subsequent action plan. Constraints typically include:
- **Law**—Legal and regulatory requirements
- **Physical**—Capacity, space and environmental constraints
- **Ethics**—Appropriate, reasonable and customary
- **Culture**—Both inside and outside the organisation
- **Costs**—Time and money
- **Personnel**—Resistance to change; resentment against new constraints
- **Resources**—Capital, technology and people
- **Capabilities**—Knowledge, training, skills and expertise
- **Time**—Window of opportunity; mandated compliance
- **Risk tolerance**—Threats, vulnerabilities and impacts

Some of the constraints, such as ethics and culture, may have been dealt with in developing the desired state. Others may arise as a consequence of developing the road map and action plan.

The typical road map to achieve a defined, secure desired state includes numerous people, processes and technologies. The interaction and relationships amongst these elements are likely to be complex. As a consequence, it is prudent to consider the initial stages of developing a security architecture. A method of developing an architecture such as SABSA, mentioned previously, can provide a structured approach to defining resource relationships and process flows. It can help ensure that contextual and conceptual elements such as business drivers and consequences are considered in the strategy development stage.

It is likely a misnomer to state that there will be a single strategy. Rather, there may be a variety of connected strategies required to achieve various objectives that cumulatively result in attaining the desired state of information security over time.

Achieving the desired state will be a long-term project or series of projects. Like most large, complex projects, it will be necessary to break it down into a series of shorter-term projects that can be accomplished in a reasonable time period, given the inevitable resource constraints. The entire road map can, and should, be charted with the understanding that there is no steady state for information security and some objectives will need to be modified over time. Some objectives, such as attaining a particular maturity level, re-engineering high-risk processes or achieving specific control objectives, may not require modification.

Shorter-term projects aligned with the long-range objectives serve to provide checkpoints and opportunities for corrections. They also provide metrics to validate the overall strategy.

For example, one long-term objective defined in the strategy may be data classification according to sensitivity and criticality. Because of the sheer magnitude of the effort required for this in a large organisation, it is likely to require a number of years to accomplish. The strategy to achieve this goal may be to determine that a certain percentage will be targeted for completion each fiscal year, utilising a variety of tactical approaches.

A second component of the strategy may be to create policies and standards that preclude the practices that originally gave rise to the problem, so it does not get worse while the remediation process is underway.

Development of a strategy to achieve long-term objectives and the road map to get there, coupled with shorter-term intermediate goals, will provide the basis for sound policy and standards development in support of the effort.

Gap Analysis—Basis for an Action Plan

Establishing a strategy will require one or more actions, projects or plans. An analysis of the gap between the current state and the desired state for each defined metric will identify the requirements and priorities for a plan of action. Gap analysis will be required for various components of the strategy previously discussed, such as maturity levels, control objectives, and risk and impact objectives. This exercise may need to be repeated annually, or more frequently, to provide performance and goal metrics and information on possible corrections needed in response to changing environments or other factors. A typical approach to gap analysis is to work backward from the end point to the current state and determine the intermediate steps needed to accomplish the objectives.

11. Action Plan

One of the most important aspects of the action plan to execute the strategy is to create or modify policies and standards as needed. Policies are the constitution of governance; standards are the law. Policies must capture the intent, expectation and direction of management. As a strategy evolves, it is vital that supporting policies be developed to articulate the strategy. For example, if the objective is to become ISO/IEC 27001-compliant over a three-year period, the strategy must consider which elements are addressed first, what resources are allocated, how the elements of the standard can be accomplished, etc. The road map will show the steps and the sequence, dependencies and milestones. The action plan is essentially a project plan to implement the strategy following the road map.

If the objective is ISO/IEC 27001 certification, each of the relevant 11 domains and major subsections must be the subject of a policy. In practice, this can be effectively accomplished with specific policies. Each policy is likely to have a number of supporting standards, typically divided by security domains. In other words, a set of standards for a high-security domain is more stringent than the standards for a low-security domain. Other standards may need to be developed for different business units depending on their activities and regulatory requirements.

Since policies are the primary instrument of governance, it is important that clarity and a consistent set of definitions be used in their creation. One of the first standards that should be considered is the standard for policies and standards. The next section details ISACA's definitions of policy, standards, procedures and guidelines, as used in this publication.

Policies

There is a broad range of interpretation of policy, standards, procedures and guidelines. The definitions used in this document are consistent with the definitions provided by major standards bodies and should be adopted to preclude miscommunication. Policies and standards are considered tools of governance and management, respectively; procedures and guidelines are primarily the purview of operations. Obviously, there are procedures and guidelines for security 'operations' as well as other management functions. In this document, the following definitions are used:

- **Policies**—High-level statements of management intent, expectations and direction. An example of a policy statement on access control is: 'Information resources shall be controlled in a manner that effectively prevents unauthorised access'. Policy can be considered the 'constitution' of security governance.
- **Standards**—Metrics, allowable boundaries or the process used to determine whether procedures meet policy requirements. An example of a standard for passwords used for access control is: 'Passwords for medium- and low-security domains must be comprised of no fewer than eight characters consisting of a mixture of upper- and lower-case letters, at least one number and one punctuation mark'.

The standard for access control for employees on the premises can include password composition requirements, minimum and maximum password length, frequency of password changes, and rules for reuse. Generally, a standard must provide sufficient parameters or boundaries that a procedure or practice can be unambiguously determined to meet the requirements of the relevant policy. Standards must change as requirements and technologies change. Policies in a mature organisation can, for the most part, remain fairly static. Multiple standards usually exist for each policy, depending on the security domain, e.g., the password standard would be more restrictive when accessing high-security domains.

- **Procedures**—The portion of an information security policy that states the general process that will be performed to accomplish a security goal. Procedures can be the responsibility of operations but can also include security-specific activities intended to support operational aspects of the information security programme. Procedures must be unambiguous and include all necessary steps needed to accomplish specific tasks. Procedures must define expected outcomes and displays as well as dependencies and conditions required for execution. Procedures must also contain the steps required when unexpected results occur. Procedures must be clear and unambiguous and terms must be exact. For example, the words 'must', 'shall' and 'will' shall be used for any task that is mandatory. The word 'should' must be used only to mean a preferred action that is not mandatory. The terms 'may' or 'can' must be used only to denote a purely discretionary action. Procedures for passwords should include the detailed steps required for setting up password accounts and for changing or resetting passwords.
- **Guidelines**—A description of a particular way of accomplishing something that is less prescriptive than a procedure. Guidelines are often the responsibility of operations but can also be used within business units to provide guidance for management, who is defining department-specific procedures. Guidelines should contain information that will be helpful in executing procedures. Information can include suggestions and examples, narrative clarifying the procedures, useful background information, and tools.

The completed strategy provides the basis for creation or modification of existing policies. The policies should be directly traceable to strategy elements. If the policies are not traceable to strategy, either the strategy is incomplete or the policy is incorrect. Obviously, a policy that contradicts the strategy will be counterproductive. The strategy is the statement of intent, expectations and direction of management. The policies must, in turn, be consistent with and support the intent and direction of the strategy.

Most organisations today have some information security policies. Typically, they have evolved over time, usually in response to a security problem or regulation, and are often inconsistent and sometimes contradictory. These policies generally have no relationship to an information security strategy (if one exists) and only a coincidental relationship to business activities.

Policies are one of the primary elements of governance. They must be properly created, accepted and validated by the board and executive management, and communicated broadly throughout the organisation. There may be occasions that subpolicies must be created to address unique situations separate from the bulk of the organisation. An example is a part of the organisation that is performing highly classified military work. Policies that reflect the specific security requirements for classified defence work may exist as a separate set.

There are several attributes of good policies that should be considered:
- Information security policies should be an articulation of a well-defined information security strategy and capture the intent, expectations and direction of management.
- Each policy should state only one general security mandate.
- Policies must be clear and easily understood by all affected parties.
- Policies should rarely be more than a few sentences long.

Most organisations have created information security policies prior to developing an information security strategy. Indeed, most organisations still have not developed an information security strategy. In many cases, policy development has not followed the approach defined here and has been *ad hoc* in a variety of formats. Often, these policies have been written to include standards and procedures in lengthy, detailed documents compiled in large, dusty volumes relegated to the stockroom.

In many cases, especially in smaller organisations, effective practices have been developed that may not be reflected in written policies. Existing practices that adequately address security requirements may usefully serve as the basis for policy and standards development. This approach will minimise organisational disruptions, facilitate communications of new policies, and quell resistance to new or unfamiliar constraints.

Standards

Standards are a powerful information security management tool. They set the permissible bounds for procedures and practices of technology and systems and for people and events. Properly implemented, they are the law to policy's constitution. They provide the measuring stick for policy compliance and a sound basis for audits. They govern the creation of procedures and guidelines.

Standards serve to create information security baselines, i.e., the minimum level of security across the enterprise. It is, therefore, important that all information security policies be expressed through a complete set of standards to ensure there are no significant gaps or 'weak links'.

Regular, systematic standards, compliance monitoring and enforcement processes are critical to ensure that the intentions of policies are met, and should themselves be the subject of a set of policies and standards.

Standards are the predominant tool for establishing effective information security governance and must be 'owned' by the information security manager. They must be carefully crafted to provide only necessary and meaningful boundaries without unnecessarily restricting operations or procedural options. Standards serve to interpret policies and define the limits of acceptability that will satisfy the policy requirements. Therefore, it is important that they reflect the intent of policy. Standards must be unambiguous, consistent and precise as to scope and audience.

There may be more than one standard per policy, divided by security domain and operational levels. For example, the access control standards for high-security domains will be more stringent than those for public areas or low-security domains. Standards for supervision and management functions will be different from those for operational activities.

Specific technical standards will exist for critical IT operations such as firewall and server configurations. These may be developed as a subset under a general configuration standard that specifies adherence to a particular set of protocols developed by the manufacturer, standards bodies or other organisations. For example, the Australian IT security organisation, AusCERT, has developed comprehensive UNIX server hardening configurations that could be mandated by the organisation's general configuration standard. Internal security audit standards may be developed specifying the type, nature and scope of audits required under compliance standards.

Standards should also exist for the creation of standards and policies, including format, content and required approvals.

Once created, standards must be disseminated to those governed by them as well as those impacted. Regular review and modification processes also must be developed since standards must be changed in response to changing circumstances such as new threats, environmental changes or revised baselines.

Exception processes must be developed for standards not readily attainable for technological or other reasons. A process for implementing compensatory controls must also be developed for out-of-compliance situations.

12. Action Plan Intermediate Goals

For most organisations, a variety of specific near-term tactical goals that align with the overall information security strategy can be defined readily. If the objectives of the security strategy ultimately require compliance with defined portions of ISO/IEC 27002, an example of a near-term action (or tactical) plan may state, for the first 12 months:

- Assign each business unit to identify current applications in use and their criticality and sensitivity
- Review 25 percent of stored information to determine ownership, criticality and sensitivity
- Assign each business unit to complete a BIA to identify critical resources
- Develop metrics and a reporting system tied to business objectives
- Define and document all security roles and responsibilities
- Develop a process to ensure business process linkages
- Perform a comprehensive risk assessment for each business unit
- Educate all users on the acceptable use policy
- Review all policies for strategic alignment and revise as necessary
- Develop standards for all policies for each business unit

Near-term goals and milestones will be required as part of the action plans. However, all the desired state objectives should be defined for the long term to maximise potential synergies and ensure that no short- or intermediate-term action plans ultimately fail to align with end goals. For example, a tactical solution that needs to be replaced, because it does not integrate into the overall plan, is likely to be more costly than one that does integrate.

It is important that the strategy and long-range plan serve to integrate near-term tactical activities. This will counter the tendency to implement tactical point solutions that are typical of the fire-fighting/crisis mode of operation in which many security departments find themselves. As many information security managers have discovered, numerous unintegrated solutions implemented in response to a series of crises over a period of years become increasingly costly and difficult to manage.

Action Plan Metrics

The plan of action to implement the strategy will require methods to monitor and measure progress and the achievement of milestones. As with any project plan, progress and costs must be monitored on an ongoing basis to determine conformance with the plan and to implement corrections on a timely basis. There are likely to be a variety of near-term goals, each requiring resources and a plan of action to achieve it.

There are many approaches that can be used for ongoing monitoring and measurement of progress. One or more of the methods used to determine current state can be used on a regular basis to determine and chart how it changes. For example, a BSC might be used effectively by itself as an ongoing means of tracking progress. Another commonly used approach is to utilise the CMM to define the current state and the objectives. CMM is a straightforward approach that is easily implemented and used extensively by COBIT, and provides a basis for performing ongoing gap analysis to determine progress toward achieving the goals.

In addition, however, each plan of action will benefit from an appropriate set of KPIs, defining critical success factors (CSFs) and setting KGIs.

Example
For example, the plan of action to achieve regulatory compliance for Sarbanes-Oxley may require, amongst other inputs:
- A detailed analysis by competent legal personnel to determine regulatory requirements for affected business units
- Knowledge of the current state of compliance
- Definition of the required state of compliance

Possible monitoring and metrics might include the following:
- KGIs—Defining clear objectives and achieving consensus on the goals are essential to developing meaningful metrics. For this particular plan, the key goals could include:
  – Achieving Sarbanes-Oxley controls testing compliance mandates
  – Completing independent controls testing, compliance validation and attestation
  – Preparing a required statement of control effectiveness

  Sarbanes-Oxley requires that, for organisations publicly traded in the US, all financial controls be tested for effectiveness within 90 days of reporting. The results of testing must be signed by the CEO and CFO, and be attested to by the organisation's auditors. The results then must be included in the organisation's public filings to the US Securities Exchange Commission (SEC).
- CSFs—To achieve Sarbanes-Oxley compliance, certain steps must be accomplished to achieve the required objectives:
  – Identifying, categorising and defining controls
  – Defining appropriate tests to determine effectiveness
  – Committing resources to accomplish required testing

  Large organisations may have hundreds (or more) of controls that usually have been developed over a period of time. In many cases, these controls are *ad hoc* and have not been subject to formal processes. It is necessary to identify control processes, procedures, structures and technologies so that an appropriate testing regime can be developed. Determining the necessary resources and testing procedures is critical to accomplish the required tests.
- KPIs:
  – Control effectiveness testing plans
  – Progress in control effectiveness testing
  – Results of testing control effectiveness

  For management to track progress in the testing effort, appropriate testing plans must be developed, consistent with the defined goals and encompassing the CSFs. Because of the limited time (90 days) available to perform the required tests, management needs reports on the progress and results of testing.

General Metrics Considerations

Considerations for information security metrics include ensuring the relevance of what is being measured. Because information security is difficult to measure in any objective sense, relatively meaningless metrics are often used simply because they are readily available. Different metrics will be more or less useful for different parts of the organisation and should be determined in collaboration with business process owners.

Senior management typically is not interested in detailed technical metrics such as the number of virus attacks thwarted or passwords reset. While these may be of significance to the IT security manager, senior management typically wants a summary or 'roll up' of information important from a management perspective—information that typically excludes detailed technical data. This summary may include:

- Progress according to plan and budget
- Significant changes in risk and possible impacts to business objectives
- Results of disaster recovery testing
- Audit results
- Regulatory compliance status

The information security manager may want more detailed information, including such data as:

- Policy compliance metrics
- Significant process, system or other changes that may affect risk profile
- Patch management status
- Exceptions and variances to policy or standards

In organisations that have an IT security manager, it is likely that all available technical security data can be useful. These data may include:

- Vulnerability scan results
- Server configuration standards compliance
- IDS monitoring results
- Firewall log analysis

Summary

Useful information security metrics are often difficult to design and implement. Since a standard predictive security yardstick does not exist, most measures are just indicative of possible risks and potential impacts.

The lack of predictive value often results in the collection of vast amounts of data to try to ensure nothing significant is overlooked. The result can be that the sheer volume of data makes it difficult to see the big picture, and efforts should be made to develop processes to distil data into useful information. A collaborative effort with various constituencies may help determine which security information is useful and what it means.

The focus is often on IT vulnerabilities, regardless of whether a threat exists or the potential impact is significant. Simply knowing the number of open vulnerabilities provides no information on risk, threats or impacts, and, by itself, is of little use.

Improvements in overall monitoring can be achieved by careful analysis of available metrics to determine their relevancy. For example, it may be interesting to know how many packets were dropped by the firewalls, but this sheds little light on risks to or potential impacts on the organisation. It may be useful to the IT department, but it is of no value to information security management. On the other hand, knowing the amount of time it takes to recover critical services after a major incident is likely to be extremely useful to all parties.

Metrics design and monitoring activities should take into consideration:
- What is important to information security operations
- The requirements of IT security management
- The needs of business process owners
- The requirements of senior management

Communication with each constituency may be helpful in determining the kinds of information security reports that would be useful. Reporting processes then can be devised to provide each group with the security information it requires.

13. Establishing Information Security Governance: An Example Using the ITGI and CobiT Maturity Scale

This chapter demonstrates an approach to establishing information security governance utilising the ITGI and CobiT maturity scale to define objectives (KGIs), determine a strategy and measure progress.

See appendix B, Self-assessment and Monitoring Model, for the six stages of the ITGI and CobiT maturity scale.

As an example, attaining a level 4 is a typical organisational goal and may comprise a statement of the objectives of information security, or the desired state.

These statements may not serve to delineate all attributes and characteristics of the desired state of information security; additional elements may need to be added. However, the statements do provide the required basics and an adequate description of the desired state of security for most organisations.

Level 4, managed and measurable:[18]
- 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 have become 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.

Breaking out the individual elements of level 4 for information security generates the following list:
- The assessment of risk is a standard procedure and exceptions to following the procedure would be noticed by information security management.
- Information security risk management is a defined management function with senior-level responsibility.
- Senior management and information security management have determined the levels of risk the organisation will tolerate and have standard measures for risk/return ratios.

[18] IT Governance Institute, *op. cit*., *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*

- 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 have become 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 information 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.

Depending on the structure of the organisation, each significant area or process of the organisation needs to be evaluated separately. For example, accounting, HR, operations, IT, business units and subsidiaries need to be evaluated to determine whether the current state meets the requirements of the 15 (or more) elements. In most organisations, the typical results for each of the 15 defined characteristics range across the maturity levels from one to four.

Policies need to be reviewed to determine whether they address each of the elements. Suggestions for policies that address each of the requirements of level 4 follow.

One objective that should be stated is to achieve consistent maturity levels across specific security domains, mindful of the notion that ‘security is only as good as the weakest link’. For example, all processes in critical financial processes should be at a similar maturity level.

After selecting a particular department, business unit or area of the organisation, the maturity level of the first statement in level 4 can be considered. The first statement is ‘The assessment of risk is a standard procedure and exceptions to following the procedure would be noticed by information security management’.

If the organisation is not at this maturity level, the approach to achieving this element must be considered. Several requirements are implicit in this statement. One is that risk assessments are a standard, formal procedure performed on a regular basis and as a result of changes in systems, processes, threats or vulnerabilities. These assessments are based on good practices and are performed on entire processes, whether physical or electronic.

In addition, the statement implies that there is effective monitoring in place to ensure the assessments are performed as required by policy. First, there must be a policy that sets forth the requirement. If one exists that states it, the requirement is addressed. Otherwise, a policy may need to be created or an existing policy may need to be modified.

An appropriate policy to address this requirement is stated in the following sample.

Sample Policy Statement

The following is a sample policy:

- Information security risks must be assessed on a regular basis or as changes in conditions warrant, utilising standardised procedures, and must include all relevant technologies and processes. Corporate security must be advised prior to commencement of such assessments, and the results of such assessments must be provided to corporate security on completion.

This policy addresses the level 4 recommendation for a standard procedure and a process to keep security management informed. A subsequent set of standards may need to be created to define the allowable boundaries and risk assessment requirements for various operational domains.

Sample Standard

The following is a sample standard:

- High-security domains comprising business-critical systems and/or confidential or protected information shall be assessed for risk annually, or more often if there are:
  - Material changes in threats
  - Changes in hardware or software
  - Changes in business or objectives
- Such assessments shall be the responsibility of the system or data owner, and shall be provided to corporate security for review on a timely basis. When possible, assessments shall be performed prior to implementing changes and provided to corporate security for approval of consistency with applicable policy.

The second statement in level 4 is ‘Information security risk management is a defined management function with senior level responsibility’. This requirement may necessitate an organisational change. Often, information security is relegated to low-level managers who do not meet the objective. Based on the information in this document and its companion guidance publication,[19] a strong business case can be made for implementing this structural change.

The third level 4 criterion states ‘Senior management and information security management have determined the levels of risk the organisation will tolerate and have standard measures for risk/return ratios’. A policy to address this criterion might state that risks must be managed to levels that prevent serious interruptions to critical business operations and limit control impacts to levels defined as acceptable.

[19] IT Governance Institute, *op. cit.*, *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*

Related standards would define limits of serious interruption and specify how the acceptable levels of impact would be determined. They may also set forth other definitions such as declarations criteria (who has the authority to declare an incident or disaster that requires appropriate responses) and severity criteria (who has authority to determine the severity of the event).

Additional Sample Policy Statements

The following are samples of policies that might be created to address some of the other level 4 statements:

- **Clear assignment of roles and responsibilities**—Roles and responsibilities of XYZ Corporation shall be unambiguously defined and all required security functions formally assigned to ensure accountability. Acceptable performance shall be ensured by appropriate monitoring and metrics.
- **Information assets identified and classified by criticality and sensitivity**—All information assets must have an identified owner and be catalogued, and the value must be determined and classified as to criticality and sensitivity throughout its life cycle.
- **Effective controls designed, implemented and maintained**—Risks and potential impacts must be managed, utilising appropriate controls and countermeasures to achieve acceptable levels at acceptable costs.
- **Effective monitoring processes in place**—All risk management, assurance and security activities must have processes to provide continuous monitoring necessary to ensure control objectives are achieved.
- **Effective compliance and enforcement processes**—Monitoring and metrics must be implemented, managed and maintained to provide ongoing assurance that all security policies are enforced and control objectives are met.
- **Tested, functional incident and emergency response capabilities**—Incident response capabilities sufficient to ensure that impacts do not materially affect the ability of the organisation to continue operations must be implemented and managed.
- **Tested BCPs/DRPs**—BCPs/DRPs shall be developed, maintained and tested in a manner that ensures the ability of the organisation to continue operations under all conditions.

Conclusions

Most organisations have not achieved a consistent level 4 across the enterprise, although this level is usually sufficient to address the security needs of most organisations in most circumstances. It is also a difficult standard to achieve and may take a number of years to accomplish, but it can serve as the objective or the desired state.

It should be noted that the foregoing sample policies may or may not be appropriate for a particular organisation. They are provided as samples consistent with the action plan in chapter 11 in terms of simple, clear construction setting forth management intent and direction at a high level.

As has been previously stated, complete policies are necessary for effective information security governance. Construction as provided in the samples has proven in practice to be a preferable approach for achieving management buy-in and general consensus. It must be remembered that policy construction must be consistent with and reflect the information security strategy and the desired state of security. The policies should also be reviewed and approved in writing by senior management.

The sample standards in this chapter are typical examples, but they must be tailored for the needs of individual organisations and are generally not complete. Usually, multiple standards are required for each policy in each security domain.

Standards construction must be undertaken with care. Properly constructed, they provide consistent security baselines and a powerful tool for implementing information security governance.

Draft standards should be reviewed by the audit department and affected organisational units. While line managers are responsible for policy compliance, audits are critical for ensuring that management fulfils this responsibility and accountability for performing security tasks is established. Audit, because of its assurance role, is one of the primary policy enforcement and compliance mechanisms. Auditors' input into standards may be helpful in developing complete and effective standards that assist them in performing their function. Collaboration with affected process owners is likely to generate better co-operation with implementing proposed changes and can help ensure that the standards do not needlessly interfere with the performance of process owners' functions. While it may entail considerable give and take to achieve consensus on appropriate standards, the end result will be greater alignment with business activities and better results in terms of ensuring compliance.

14. Conclusion

For most organisations, establishing effective information security governance is a major initiative, given the often fragmented, tactical nature of typical security efforts. It requires committed support of senior management and adequate resources. It necessitates the elevation of information security management to positions of authority commensurate to the required responsibilities. This has been the trend in recent years as organisations grow increasingly dependent on their information assets and resources, while threats and disruptions continue to escalate in frequency and cost.

It is clear from numerous recent studies that organisations that have taken the steps described in this publication and have implemented effective information security governance have achieved significant results in reduced losses and improved resource management. Given the demonstrable benefits, it is surprising that there have not been greater strides in effectively managing information assets.

Although regulatory compliance has been a major driver in improving information security overall, recent studies have also shown that nearly half of all companies are failing to initiate meaningful compliance efforts.

Appendix A—Critical Success Factors for Effective Information Security

To achieve successful information security, it is critical to ensure the following:

- There is awareness that a good information security programme takes time to evolve.
- The corporate information security function reports to senior management and is responsible for executing the information security programme.
- Management and staff have a common understanding of information security importance, requirements, vulnerabilities and threats, and understand and accept their own security responsibilities.
- Third-party evaluation of information security policy and architecture is conducted periodically.
- The information security function has the means and ability to administer security, especially to detect, record and analyse significance, and report and act on security incidents when they do occur, while minimising the probability of occurrence by applying intrusion testing and active monitoring.
- Clearly defined roles and responsibilities for risk management ownership and management accountability are in place.
- A policy is established to define risk limits and risk tolerance.
- Responsibilities and procedures for defining, agreeing on and funding risk management improvements exist.
- A reality check of the information security strategy is conducted by a third party to increase objectivity and is repeated at appropriate times.
- Critical infrastructure components are identified and continuously monitored.
- Service level agreements (SLAs) are used to raise awareness of and increase co-operation with suppliers relative to security and continuity needs.
- Policy enforcement is considered and decided on at the time of policy development.
- A confirmation process is in place to measure awareness, understanding and compliance with policies.
- Applications are secured well before they are deployed.
- Information control policies are aligned with the overall strategic plans.
- Management endorses and is committed to the information security and control policies, stressing the need for communication, understanding and compliance.
- There is a consistently applied policy development framework that guides formulation, roll-out, understanding and compliance.
- There is awareness that, although insiders continue to be the primary source of most security risks, attacks by organised crime and other outsiders are increasing.
- Proper attention is paid to data privacy, copyright and other data-related legislation.
- There is senior management support to ensure employees perform their duties in an ethical and secure manner.
- Management is leading by example.

Performance Measures

To Determine Whether Information Security Is Succeeding
The performance measures to determine whether information security governance is succeeding are:
- No incidents causing public embarrassment
- Reduced number of new implementations delayed by information security concerns
- Number of critical business processes that have adequate continuity plans
- Number of critical infrastructure components with automatic availability monitoring
- Measured improvement in employee awareness of information security responsibilities

To Determine Whether Information Security Governance Is Succeeding
The performance measures to determine whether information security governance is succeeding are:
- Full compliance, or agreed-on and recorded deviations from minimum security requirements
- Percentage of plans and policies developed and documented covering information security mission, vision, goals, values and code of conduct
- Percent of information security plans and policies communicated to all stakeholders
- Consistent, predictable levels of security and impacts at acceptable levels

Appendix B—Self-assessment and Maturity Model

Self-assessment for Information Security Governance

Information security management can utilise the ITGI and COBIT Maturity Scale to create an information security governance profile of the organisation.

This model can be progressively applied as:

- A method for self-assessment against the scales, deciding where the organisation is
- A method for using the results of the self-assessment to set targets for future development based on where the organisation wants to be on the scale
- A method for planning projects to reach the targets based on an analysis of the gaps between those targets and the present status
- A method for prioritising project work based on project classification and an analysis of its beneficial impact against its cost

The information that follows—the maturity scale and a description for each of the major elements of information security relative to maturity—can be used to develop a comprehensive profile of the current state of information security governance:

- An information security strategy with senior management acceptance and support
- An information security strategy intrinsically linked to business objectives
- Information security policies that are complete and consistent with strategy
- Complete standards for all relevant policies that are consistently maintained
- Complete and accurate procedures for all important operations
- Clear assignment of roles and responsibilities
- Organisational structure ensuring appropriate authority for information security management without inherent conflicts of interest
- Information assets identified and classified as to criticality and sensitivity
- Effective controls designed, implemented and maintained
- Effective security metrics and monitoring processes in place
- Effective compliance and enforcement processes
- Tested functional incident and emergency response capabilities
- Tested BCP/DRP
- Appropriate security approval in change management processes
- Risks properly identified, evaluated, communicated and managed
- Adequate security awareness of all users, and training as needed
- Development and delivery of activities that can positively influence an information security orientation of the enterprise's culture and staff's behaviour
- Regulatory and legal issues understood and addressed
- Information security issues with third-party service providers addressed
- Timely resolution of non-compliance issues and other variances

Maturity Levels—Detailed Descriptions[20]

The maturity levels described in COBIT 4.1 (based on CMM) are depicted in **figure 7** and described as follows:

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.
- 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. Information security reporting and a response process to information security breaches do not exist. 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 the loss of IT services to the business. Service continuity is not considered as needing management attention.

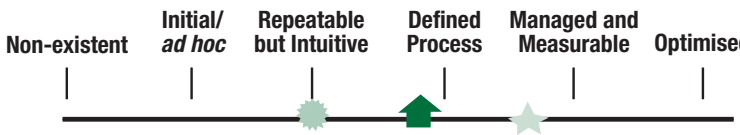
1 Initial*/ad hoc*

- 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 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. Some approach to risk assessment exists, but the process is still immature and developing.

Figure 7—ITGI and COBIT Maturity Scale



LEGEND FOR SYMBOLS USED

- Enterprise current status
- Industry average
- Enterprise target

LEGEND FOR RANKINGS USED

0—Management processes are not applied at all.
1—Processes are *ad hoc* and disorganised.
2—Processes follow a regular pattern.
3—Processes are documented and communicated.
4—Processes are monitored and measured.
5—Good practices are followed and automated.

[20] Adapted from IT Governance Institute, COBIT 4.1, USA, 2007

- Responsibilities and accountabilities for information security are assigned to an information security co-ordinator 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 organisation-wide 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 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 consistently communicates 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 have become 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 organisation's overall 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 assessment has developed to the stage that a structured, organisation-wide process is enforced, followed regularly and managed well.
- Information security is a joint responsibility of business and IT management and is integrated with corporate 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 pro-active identification of risk are the basis for continuous improvements. Security processes and technologies are integrated organisation-wide.
- Continuous service plans and BCPs are integrated, aligned and routinely maintained. Buy-in for continuous service needs is secured from vendors and major suppliers.

Appendix C—A Generic Approach to Information Security Initiative Scoping

Scoping is the process of determining the various inputs, outputs and technologies related to an initiative as well as the business processes and organisational units involved or affected. It also includes the identification of any standards, methodologies, and other tools and techniques used to guide the initiative; estimates of financial and other resources; and the time frame within which the initiative is to be completed.

Planning the implementation of an information security governance implementation is important as it will invariably touch every business unit and impact every user. The goals for such projects are more global in nature than other security projects and the boundaries for the project much broader. This generic scoping document may assist in identifying the resources, time frames and other resources required for the implementation project. More important, it will help in documenting the outcomes that are expected and the performance metrics that will be necessary in determining the success of the project.

Figure 8 lists the steps, activities and deliverables to define the initiative.

Figure 8—Step 1: Define the Initiative

Steps	Activities	Deliverables
Step 1.1 Define objectives. Identify the primary objectives and goals of the initiative. Develop the value proposition and indicate how the objectives support and enhance the goals of the enterprise.	• Identify reasons and objectives for undertaking the project and review with management. • Research and document key issues and concerns. • Learn from similar projects that have been undertaken. • Identify and obtain relevant documents. • Identify expected outcomes and deliverables of the initiative (high level). • Identify competitive landscape.	• Documented business values • Documented objectives of the initiative • Documented expected outcomes
Step 1.2 Define boundaries. Define the project and its boundaries: what is included and what is excluded. Identify the organisational units, business activities and processes that are included and those that are excluded from the project scope.	• Identify key activities, business units, organisational entities, operations, etc. to be included within the scope of the project. • Identify and document items that are normally within the scope of such projects but are to be excluded. • Identify any scope issues such as partially owned entities, foreign jurisdictions and exclusions. • Ensure the scope is sufficient to make certain that the results obtained will meet the objectives and expected deliverables. • Establish a liaison with affected entities to ensure co-ordination.	• Documented scope of the initiative • Documented scope of the boundary issues and their treatment • Communication of the boundaries with key stakeholders

Figure 8—Step 1: Define the Initiative (*cont.*)		
Steps	**Activities**	**Deliverables**
Step 1.3 Define standards. Identify key standards, reference frameworks, policies and/or contracts in undertaking the project with which the initiative needs to comply. Standards may include industry requirements, regulatory standards and entity policies. Identify indicators for measuring, and establish key success factors for achieving, compliance.	• Identify contractual, legislative, regulatory, industry or other standards with which the entity and the project must comply. • Identify any standards or frameworks that the project/initiative should consider. • Document success factors to enable, and key metrics to evidence, compliance with standards.	• Documented standards that will be used • Documented key success factors and metrics for use in assessing project results
Step 1.4 Define risks. Identify and assess risks associated with the project, including business risks and project risks. The degree of risk assessment and mitigation depends on the project's size, value delivered and impact.	• Identify potential reasons for failure or delay of the initiative in meeting objectives. • Identify important scenarios that may endanger the initiative's objectives and the negative impacts this initiative may have on other enterprise objectives. • Identify the significance of risks and the likelihood of occurrence. • Create plans to manage and mitigate the risks.	• Documented risk assessment • Risk mitigation plan (as needed) and estimated costs
Step 1.5 Define a change process. Identify internal and external factors that could cause changes to the project and define how changes will be made to the project's objectives, scope, risks and success factors.	• Identify and analyse internal and external factors that could cause changes to the project. • Define and document the processes and procedures for authorising, accepting and communicating changes of the drivers and outcomes. • Identify appropriate tools and techniques to manage the change process.	• Change process description • Change management guidance, including the use of tools and techniques

Figure 8—Step 1: Define the Initiative (*cont.*)		
Steps	**Activities**	**Deliverables**
Step 1.6 Define success. Identify the conditions that must exist for the project to be considered complete, including the specific activities, tasks and deliverables required to complete the project. Define the exit criteria of the initiative, i.e., the conditions that determine whether the objectives have been achieved.	• Identify post-project acceptance activities. • Identify evidence required to indicate that the project deliverables have been provided and accepted by the project owner and by those taking responsibility for the ongoing activities the project may create.	• Evidence (e.g., metrics, quality criteria) required to indicate the project has been successfully completed • Evidence that post-completion activities have been identified and provided to appropriate organisational units
Step 1.7 Define resources. Identify the resources required to successfully complete the initiative, including people, technology, funding and skills.	• Define the number and level (skills) of resources needed to achieve the objectives of the initiative. • Assess the need for technology and equipment to support the initiative.	• Resource model • Resource cost plan
Step 1.8 Define deliverables. Define the specific deliverables that are to be produced during the initiative.	• Identify the external deliverables that will result from the initiative. • Create an illustrative sample deliverable.	• List of project deliverables • Sample of selected deliverables

Figure 9 lists the steps, activities and deliverables to plan the initiative.

Figure 9—Step 2: Plan the Initiative		
Steps	**Activities**	**Deliverables**
Step 2.1 Obtain executive support. Identify and appoint the appropriate project sponsor for the initiative.	• Determine the suitability of potential sponsors. • Assess the availability of potential sponsors to fulfil the requirements. • Develop executive presentation material based on project objectives and benefits.	• Initiative sponsor/owner identification • Completed project documentation and charter
Step 2.2 Finalise resource requirements. Acquire the necessary funding and resources as defined in the resource model.	• Review the expected resource model and cost plan. • Prepare a detailed acquisition timeline. • Prepare a detailed calendar-based project budget, including resource consumption/use and funding requirements.	• Updated resource model • Detailed resource acquisition timeline • Detailed project budget

Figure 9—Step 2: Plan the Initiative (*cont.*)		
Steps	**Activities**	**Deliverables**
Step 2.3 Define the organisational structure for the initiative. Define and implement the organisational structure required to make this initiative successful. This should include leadership, staffing and key sponsor, and may include a project management office.	• Document roles and responsibilities. • Define leadership expectations. • Create and establish the organisational structure. • Initially populate the organisation with key personnel. • Create position descriptions, roles and responsibilities.	• Organisation model • Reporting authority • Roles and responsibilities
Step 2.4 Define a timeline. Define the specific timeline for the initiative to be completed to meet stated goals and objectives given the expected resources and deliverables defined for the initiative. Include key milestones and identify the critical path.	• Review goals, objectives and the expected resource model. • Based on the review, define key milestones for deliverables and major initiative checkpoints with project sponsors. • Prepare a high-level diagram and identify the potential critical path and dependent activities. • Prepare Gantt charts for each major phase of the sub-projects, including critical and slack path analysis, skill requirements and resource plans. • Ensure the timing will meet critical external reporting, financing and other deadlines within the business cycle. • Define ongoing status reporting within the project to key external stakeholders and affected staff.	• Documented timelines integrated with the resource planning information • Project timeline document indicating: – Activities and tasks – Activity dependence – Major milestone dates – Major project checkpoints – Key deliverable dates – Status and reporting dates – Business activities and other key dates • Detailed communications documents
Step 2.5 Define an approach and methodology. Determine the methodologies to be used and develop detailed plans, complete with phases, sub-phases, activities and tasks to enable the project to successfully meet its objectives.	• Develop project phases and sub-phases, each with objectives, activities and deliverables. • Determine the approach and methodologies to be used and the information to be obtained. • Develop detailed work plans for each phase, sub-phase and activity.	• Detailed project plan

Figure 9—Step 2: Plan the Initiative (*cont.*)		
Steps	**Activities**	**Deliverables**
Step 2.6 Create a communication plan. Design a plan to communicate information about the initiative, manage expectations and support the objectives of the initiative throughout its life cycle. Consider the key milestones and different audiences.	• Communicate project status, resource plans and costs, as appropriate. • Communicate the status of the risk management plan. • Communicate changes in project goals and objectives. • Communicate project progress.	• Documented communications plan, including timelines and key milestones

Appendix D—An Approach to Information Security Metrics

Figure 10—NIST SP 800-55

NIST special publication 800-55 provides an approach to security metrics (**figure 10**). It states:

> *The foundation of strong upper-level management support is critical, not only for the success of the security program, but also for the implementation of a security metrics program. This support establishes a focus on security within the highest levels of the organization. Without a solid foundation (i.e., proactive support of those persons in positions that control IT resources), the effectiveness of the security metrics program can fail when pressured by politics and budget limitations.*
>
> *The second component of an effective security metrics program is practical security policies and procedures backed by the authority necessary to enforce compliance. Practical security policies and procedures are defined as those that are attainable and provide meaningful security through appropriate controls. Metrics are not easily obtainable if there are no procedures in place.*
>
> *The third component is developing and establishing quantifiable performance metrics that are designed to capture and provide meaningful performance data. To provide meaningful data, quantifiable security metrics must be based on IT security performance goals and objectives, and be easily obtainable and feasible to measure. They must also be repeatable, provide relevant performance trends over time, and be useful for tracking performance and directing resources.*

Finally, the security metrics program itself must emphasize consistent periodic analysis of the metrics data. The results of this analysis are used to apply lessons learned, improve the effectiveness of existing security controls, and plan future controls to meet new security requirements as they occur. Accurate data collection must be a priority with stakeholders and users if the collected data is to be meaningful to the management and improvement of the overall security program. The success of an information security program implementation should be judged by the degree to which meaningful results are produced. A comprehensive security metrics analysis program should provide substantive justification for decisions that directly affect the security posture of an organization. These decisions include budget and personnel requests and allocation of available resources. A security metrics program should provide a precise basis for preparation of required security performance-related reports.[21]

[21] National Institute of Standards and Technology, 'Security Metrics: Guide for Information Technology Systems', SP 800-55, USA, 2003

Glossary

Acceptable use policy—A policy that establishes an agreement between users and the organisation and defines for all parties the ranges of use that are approved before gaining access to a network or the Internet

Access control—Refers to the processes, rules and deployment mechanisms that control access to information systems, resources and physical access to the premises

Access rights—Permission or privileges granted to users, programs or workstations to create, change, delete or view data and files within a system as defined by rules established by data owners and the information security policy

Accountability—The ability to map a given activity or event back to the responsible party

Administrative controls—The rules, procedures and practices dealing with operational effectiveness, efficiency and adherence to regulations and management policies

Application controls—Manual or programmed activities intended to ensure the completeness and accuracy of records and the validity of entries made. The objectives of application controls are to ensure the completeness and accuracy of the records and the validity of the entries made therein resulting from manual and programmed processing.

Audit trail—A visible trail of evidence enabling one to trace information contained in statements or reports back to the original input source

Authentication—1. The act of verifying a user, 2. The user's eligibility to access computerised information

Availability—Relates to information being available when required by the business process, now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.

CISO—Chief information security officer, an executive position charged with responsibility for managing and protecting information assets

CobiT—*Control Objectives for Information and related Technology*, a complete, internationally accepted process framework for IT that supports business and IT executives and management in their definition and achievement of business goals and related IT goals by providing a comprehensive IT governance, management, control and assurance model. CobiT describes IT processes and associated control objectives, management guidelines (activities, accountabilities, responsibilities and performance metrics) and maturity models. CobiT supports enterprise management in the development, implementation, continuous improvement and monitoring of good IT-related practices.

Confidentiality—The protection of sensitive or private information from unauthorised disclosure

Corporate governance—The system by which organisations are directed and controlled. Boards of directors are responsible for the governance of their organisations. It consists of the leadership and organisational structures and processes that ensure the organisation sustains and extends strategies and objectives.

Corporate strategy—The pattern of decisions in a company that determines and reveals its objectives, purposes or goals; produces the principal policies and plans for achieving those goals; and defines the range of business the company is to pursue, the kind of economic and human organisation it is or intends to be, and the nature of the economic and non-economic contribution it intends to make to its shareholders, employees, customers and communities

COSO—The Committee of Sponsoring Organisations of the Treadway Commission; provides guidance and a comprehensive framework of internal control for all organisations

Data classification—The assignment of a level of sensitivity to data (or information) that results in the specification of controls for each level of classification. Levels of sensitivity of data are assigned according to predefined categories as data are created, amended, enhanced, stored or transmitted. The classification level is an indication of the value or importance of the data to the organisation.

Decentralisation—The process of distributing computer processing to different locations within an organisation

Dual control—A procedure that uses two or more entities (usually persons) operating in concert to protect a system resource such that no single entity acting alone can access that resource

Guidelines—A description of a particular way of accomplishing something that is less prescriptive than a procedure

Information security governance—The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly

Information security programme—The overall combination of technical, operational and procedural measures, and management structures implemented to provide for the confidentiality, integrity and availability of information based on business requirements and risk analysis

Integrity—The accuracy, completeness and validity of information

ISO/IEC 27001:2005—A standard from the International Organisation for Standardisation (ISO)/International Electrotechnical Commission (IEC) that covers all types of organisations (e.g., commercial enterprises, government agencies, not-for-profit organisations). ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system within the context of the

organisation's overall business risks. ISO/IEC 27001:2005 specifies requirements for the implementation of security controls customised to the needs of individual organisations or parts thereof. (Source: International Organisation for Standardisation.)

ISO/IEC 27002—A standard from the International Organisation for Standardisation (ISO)/International Electrotechnical Commission (IEC) that defines information's confidentiality, integrity and availability controls in a comprehensive information security management system

Mandatory access control (MAC)—A means of restricting access to data based on varying degrees of security requirements for information contained in the objects and the corresponding security clearance of users' programs acting on their behalf

Monitoring policy—The rules outlining or delineating the way in which information about the use of computers, networks, applications and information is captured

Non-repudiation—The assurance that a party cannot later deny originating data, that is, the provision of proof of the integrity and origin of the data that can be verified by a third party. A digital signature can provide non-repudiation.

Policies—High-level statements of management intent, expectations and direction. An example of a policy statement on access control is: 'Information resources shall be controlled in a manner that effectively prevents unauthorised access'. Policy can be considered the 'constitution' of security governance.

Privacy—Freedom from unauthorised intrusion or disclosure of information about individuals

Procedures—The portion of a security policy that states the general process that will be performed to accomplish a security goal

Security metrics—Any form of measurement used to determine any aspect of the operation of any security-related activity

Standards—Metrics, allowable boundaries or the process used to determine whether procedures meet policy requirements. An example of a standard for passwords used for access control is: 'Passwords for medium- and low-security domains must be comprised of no fewer than eight characters consisting of a mixture of upper- and lower-case letters, at least one number and one punctuation mark'.

Steering committee—A management committee assembled to sponsor and manage various projects, such as an information security programme

References

American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants, *Privacy Framework Principles and Criteria*, USA and Canada, 2004

American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants, *SysTrust Principles and Criteria for Systems Reliability V2.0*, USA and Canada, 2001

Andrews, Kenneth; *The Concept of Corporate Strategy, 2nd Edition*, Dow-Jones Irwin, USA, 1980

Asian School of Cyber Laws, *www.asianlaws.org/infosec/archives/08_02_oecd.htm* (contains references to cyberlaws that are in force in Asia)

Australian Computer Emergency Response Team, *www.auscert.org.au* (contains security guidelines from this Australian emergency organisation)

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

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

Carnegie Mellon University, *Governing for Enterprise Security*, USA, June 2005

CIO, *CSO* and PricewaterhouseCoopers, 'The State of Information Security 2007: A Worldwide Study by *CIO*, *CSO* and PricewaterhouseCoopers', USA, 2007

The Corporate Governance Task Force, 2004, *www.cyberpartnership.org/InfoSecGov4_04.pdf*

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

Fiedler, Andreas E.; *On the Necessity of Management of Information Security: The Standard ISO 17799 as International Basis*, Northwest Controlling Corporation Ltd., 2002, *www.noweco.com/wp_iso17799e.htm* (contains an overall description of ISO 17799)

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

Hallawell, Arabella; *Gartner Global Security and Privacy Best Practices*, Gartner Analyst Reports, 16 March 2004, *www.csoonline.com/analyst/report2332.html*

Information Security Forum, *The Forum's Standard of Good Practice*, 2001, *www.isfsecuritystandard.com/index_ie.htm* (includes information security good practices published by this organisation)

Information Security Forum, *The Standard of Good Practice for Information Security*, *Version 4*, UK, March 2003

Information Systems Security Association (ISSA), *The Generally Accepted Information Security Principles* (GAISP), in preparation

International Federation of Accountants, *Managing Security of Information*, 1998

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

IT Governance Institute, COBIT 4.1, USA, 2007, *www.itgi.org*

IT Governance Institute, *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*, 2005, *www.itgi.org*

Kahnerman, Daniel; Amos Tversky; *Judgment Under Uncertainty: Heuristics and Biases*, 1982

Kiely, Laree; Terry Benzel; *Systemic Security Management*, Libertas Press, USA, 2006

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

Mather, Tim; Mark Egan; *Developing Your Information Security Program*, Prentice Hall PTR, USA, 10 December 2004, *www.phptr.com/index.asp?rl=1*

National Cyber Security Partnership, *www.cyberpartnership.org/init-governance.html*

National Institute of Standards and Technology (NIST), *www.csrc.nist.gov/pcig/ppsp.html*

National Institute of Standards and Technology (NIST), NIST 800-53, *Recommended Security Controls for Federal Information Systems*, USA, 2005

Organisation for Economic Co-operation and Development, *Guidelines for the Security of Information Systems*, France, 2002

Organisation for Economic Co-operation and Development, *Guidelines for the Security of Information Systems and Networks—Toward a Culture of Security*, France, 2003

Pironti, John; 'Information Security Governance: Motivations, Benefits and Outcomes', *Information Systems Control Journal*, ISACA, USA, 2006

Sherwood, John; Andrew Clark; David Lynas; SABSA *Enterprise Security Architecture*, CMP 2005, *www.sabsa.org*

US Computer Emergency Readiness Team, *www.us-cert.gov/resources.html*

Other Publications

Many publications issued by ITGI and ISACA contain detailed assessment questionnaires and work programmes. For further information, please visit *www.isaca.org/bookstore* or e-mail *bookstore@isaca.org*.

CobiT and Related Publications

- CobiT® 4.1, 2007
- *CobiT® Control Practices, Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition,* 2007
- *CobiT® Security Baseline, 2nd Edition*, 2007
- *CobiT® Quickstart, 2nd Edition*, 2007
- *IT Assurance Guide: Using CobiT®,* 2007
- *IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance,* 2007
- *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition,* 2006
- *IT Governance Implementation Guide: Using CobiT® and Val IT™, 2nd Edition,* 2007

CobiT Mapping Series:

- *Aligning CobiT®, ITIL and ISO 17799 for Business Benefit*
- *CobiT® Mapping: Mapping of CMMI® for Development V1.2 With CobiT® 4.0*
- *CobiT® Mapping: Mapping of ISO/IEC 17799:2000 With CobiT®, 2nd Edition*
- *CobiT® Mapping: Mapping of ISO/IEC 17799:2005 With CobiT® 4.0*
- *CobiT® Mapping: Mapping of ITIL With CobiT® 4.0*
- *CobiT® Mapping: Mapping of NIST SP800-53 With CobiT® 4.1*
- *CobiT® Mapping: Mapping of PMBOK With CobiT® 4.0*
- *CobiT® Mapping: Mapping of PRINCE2 With CobiT® 4.0*
- *CobiT® Mapping: Mapping of SEI's CMM for Software With CobiT® 4.0*
- *CobiT® Mapping: Mapping of TOGAF 8.1 With CobiT® 4.0*
- *CobiT® Mapping: Overview of International IT Guidance, 2nd Edition*

IT Governance Publications

- *Board Briefing on IT Governance, 2nd Edition*, 2003
- *IT Governance Global Status Report—2008*, 2008

IT Governance Domain Practices and Competencies series:

- *Information Risks: Whose Business Are They?*, 2005
- *Optimising Value Creation From IT Investments*, 2005
- *Measuring and Demonstrating the Value of IT*, 2005
- *Governance of Outsourcing*, 2005
- *IT Alignment: Who Is in Charge?*, 2005

Val IT series:

- *Enterprise Value: Governance of IT Investments: The Val IT™ Framework*, 2006
- *Enterprise Value: Governance of IT Investments: The Business Case*, 2006
- *Enterprise Value: Governance of IT Investments: The ING Case Study*, 2006

Security Publications

- *Cybercrime: Incident Response and Digital Forensics,* 2005
- *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition,* 2006
- *Information Security Governance—Top Actions for Security Managers,* 2005
- *Information Security Harmonisation—Classification of Global Guidance,* 2005
- *Managing Information Integrity: Security, Control and Audit Issues,* 2004
- *Security Awareness: Best Practices to Serve Your Enterprise,* 2005
- *Stepping Through the InfoSec Program*, 2007

E-commerce Security series:

- *Securing the Network Perimeter*, 2002
- *Business Continuity Planning*, 2002
- *Trading Partner Authentication, Registration and Enrollment*, 2000
- *Public Key Infrastructure*, 2001
- *A Global Status Report*, 2000
- *Enterprise Best Practices*, 2000

Assurance Publications

- *Stepping Through the IS Audit, 2nd Edition*, 2004

ERP Series:

- *Security, Audit and Control Features Oracle® E-Business Suite: A Technical and Risk Management Reference Guide, 2nd Edition*, 2006
- *Security, Audit and Control Features PeopleSoft®: A Technical and Risk Management Reference Guide, 2nd Edition*, 2006
- *Security, Audit and Control Features SAP®R/3®: A Technical and Risk Management Reference Guide, 2nd Edition*, 2005

Specific Environments

- *Electronic and Digital Signatures: A Global Status Report,* 2002
- *Enterprise Identity Management: Managing Secure and Controllable Access in the Extended Enterprise Environment,* 2004
- *ITAF™: A Professional Practices Framework for IT Assurance*, 2008
- *Linux: Security, Audit and Control Features*, 2005
- *Managing Risk in the Wireless LAN Environment: Security Audit and Control Issues*, 2005
- *Oracle® Database Security, Audit and Control Features,* 2004
- *OS/390—z/OS: Security, Control and Audit Features,* 2003
- *Peer-to-peer Networking Security and Control,* 2003
- *Risks of Customer Relationship Management: A Security, Control and Audit Approach,* 2003
- *Security Provisioning: Managing Access in Extended Enterprises,* 2002
- *Virtual Private Network—New Issues for Network Security,* 2001

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*

ISBN 978-1-933284-73-6