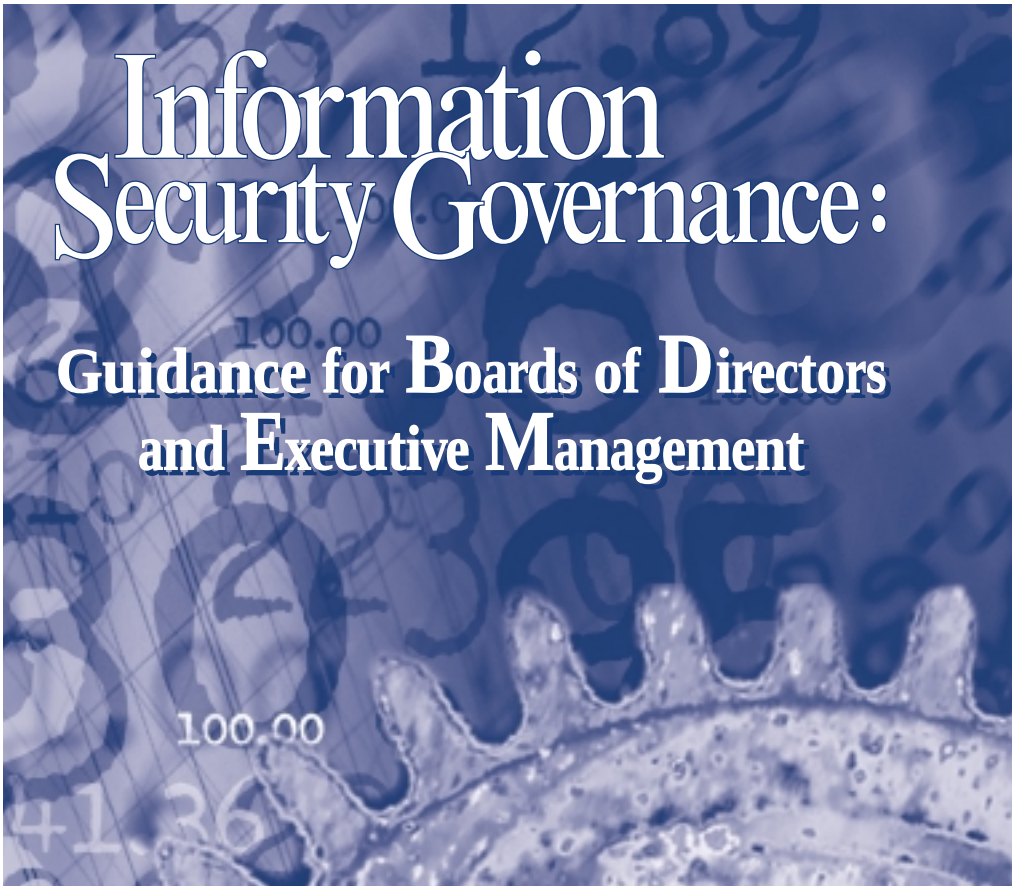


"Directors have a responsibility to protect shareholder value. This responsibility applies just as stringently to valued information assets as it does to any other asset. Boards must recognise that securing that information is not just an investment; it is essential for survival in all cases and for many it can even create competitive advantage."

— Ronald Saull, Chief Information Officer and Senior Vice President, Great-West Life Assurance Company/London Life/Investors Group

"IT security provides the management processes, technology and assurance to allow business management to ensure business transactions can be trusted; ensure IT services are usable and can appropriately resist and recover from failures due to error, deliberate attacks or disaster; and ensure critical confidential information is withheld from those who should not have access to it."

— Dr. Paul Dorey, Director, Digital Business Security, BP Plc

IT Governance Institute™

The IT Governance Institute appreciates the support the following organisations have provided to this project:

American Institute for Certified Public Accountants

Association Française de L'Audit et du Conseil Informatiques

The Canadian Institute of Chartered Accountants

The Center for Internet Security

The Gartner Group

International Federation of Accountants

Japanese Institute of Certified Public Accountants

The SANS Institute

Acknowledgements

The IT Governance Institute wishes to recognise:

- **The development team, for its leadership of the project**
  Erik Guldentops, CISA, SWIFTsc, Belgium (Leader, Development Team)
  John W. Lainhart IV, CISA, PricewaterhouseCoopers, USA (Chair, IT Governance Board)
  Gary Hardy, Arthur Andersen, UK
  Eddy Schuermans, CISA, PricewaterhouseCoopers, Belgium
  Marc Sel, CISA, PricewaterhouseCoopers, Belgium
  Dirk Steuperaert, CISA, PricewaterhouseCoopers, Belgium

- **The expert reviewers, whose comments helped shape the final document**
  Paul Dorey, Ph.D., BP Plc, UK
  William Malik, The Gartner Group, USA
  Donn B. Parker, CISSP, Atomic Tangerine, USA
  Fred Piper, Ph.D., Royal Holloway College, UK
  Daniel Fernando Ramos, CISA, CPA, SAFE Consulting Group, Argentina
  Robert S. Roussey, CPA, University of Southern California, USA

- **The Board of Directors/Trustees, for their support of the project**
  Paul A. Williams, FCA, MBCS, Arthur Andersen, UK, International President
  J. Manuel Aceves, CISA, CISSP, Cambridge Technology Partners, Mexico, Vice President
  Marios Damianides, CISA, CA, CPA, Ernst & Young, USA, Vice President
  Lynn C. Lawton, CISA, BA, FCA, FIIA, PIIA, KPMG, UK, Vice President
  Jae Woo Lee, Ph.D., Dongguk University, IAI, Korea, Vice President
  Michael J. A. Parkinson, CISA, CIA, KPMG, Australia, Vice President
  Robert S. Roussey, CPA, University of Southern California, USA, Vice President
  Ronald Saull, CSP, Great-West and Investors Group, Canada, Vice President
  Patrick Stachtchenko, CISA, CA, Deloitte & Touche, France, Past International President
  Akira Matsuo, CISA, CPA, Chuo Audit Corporation, Japan, Past International President
  Erik Guldentops, CISA, SWIFTsc, Belgium, Trustee
  Emil G. D'Angelo, CISA, Marsh and McLennan, Inc., USA, Trustee

- **The IT Governance Board, for its contributions to the development and review of the document**

IT Governance Institute™

The IT Governance Institute (ITGI), founded by the Information Systems Audit and Control Association and its affiliated foundation in 1998, strives to assist enterprise leadership in ensuring long-term, sustainable enterprise success and increased stakeholder value by expanding awareness of the need for and benefits of effective IT governance. The institute develops and advances understanding of the vital link between IT and enterprise governance, and offers best practice guidance on the management of IT-related risks.

Information Systems Audit and Control Foundation™

The Information Systems Audit and Control Foundation (ISACF™) was created in 1976 to undertake large-scale research efforts to expand the knowledge and value of the IT governance and control field. The role of the foundation is to evaluate the latest guidelines for implementation of emerging technologies and their applications. The research conducted by ISACF not only informs and guides the profession, it also forms the basis of many of the products and services—such as education, technical articles and publications, conferences, standards and professional certification—the association offers members and other constituents.

Information Systems Audit and Control Association®

The Information Systems Audit and Control Association (ISACA™) is an international professional, technical and educational organisation dedicated to being a single source provider for those concerned with the effective governance of information and its related technologies. With members in more than 100 countries, ISACA is uniquely positioned to fulfill the role of a central harmonising source of IT control practice standards the world over. Its strategic alliances with other organisations in the financial, accounting, auditing and IT professions ensure an unparalleled level of integration and commitment by business process owners.

This publication is based on the IT Governance Institute's *Control Objectives for Information and related Technology* (COBIT) 3rd Edition, which is an open standard and is available from the ISACA web site. This publication is considered one of the COBIT family of products, an international and generally accepted IT control framework enabling organisations to implement an IT governance structure throughout the enterprise.

Disclaimer

The IT Governance Institute, Information Systems Audit and Control Foundation, Information Systems Audit and Control Association and the authors of *Information Security Governance: Guidance for Boards of Directors and Executive Management* have designed this publication primarily as an educational resource for boards of directors, executive management and information technology control professionals. The IT Governance Institute, Information Systems Audit and Control Foundation and Information Systems Audit and Control Association make no claim that use of this publication will assure a successful outcome. This document should not be considered inclusive of any inquiries, proper procedures and tests or exclusive of other inquiries, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific inquiries, procedures or tests, the users should apply their own professional judgment to the specific control circumstances presented by the particular systems or information technology environment.

Disclosure

Information Systems Audit and Control Foundation

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: *jseago@isaca.org*
Web sites: *www.isaca.org* and *www.ITgovernance.org*

ISBN 1-893209-28-8 (*Information Security Governance: Guidance for Boards of Directors and Executive Management*)
Printed in the United States of America

Table of Contents

Purpose and Structure of Document

The growth and success of nearly all enterprises rely on harnessing information technology (IT) for secure, profitable use. All enterprises benefit from an integrated and comprehensive approach to risk management, security and control.

As organisations continue to take advantage of the opportunities available through global networking, and need to comply with existing or new security laws and regulations, difficult decisions arise about how much money to invest in IT security and control. Enterprises must consider the best ways to offer flexibility to customers and trading partners, yet ensure security of critical information and systems for all its users.

While executive management has the responsibility to consider and respond to these issues, boards of directors will increasingly be expected to make information security an intrinsic part of governance, preferably integrated with the processes they have in place to govern IT.

In this regard, governing boards and executive management should review:

- The scale and cost of the current and future investments in information
- The potential for technologies to dramatically change organisations and business practices, create new opportunities, and reduce costs

They should also consider the associated ramifications:

- The increasing dependence on information and the systems and communications that deliver the information
- The dependence on entities beyond the direct control of the enterprise
- The impact on reputation and enterprise value resulting from IT failures

To exercise effective enterprise and IT governance, boards of directors and executive management must have a clear understanding of what to expect from their enterprise's information security programme. They need to know how to implement an effective information security programme, how to evaluate their own status with regard to the security programme in place and how to decide what security programme is desired.

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

- What is information security?
- Why is it important?
- Who is responsible for it?

It also provides practical, pragmatic advice on:

- Questions to ask to uncover potential security weaknesses
- What information security governance should deliver
- How to implement information security
- How to measure your enterprise's maturity level relative to information security governance

Information Security Governance: Guidance for Boards of Directors and Executive Management

1. The Background to Information Security Governance

In today's global business environment, the significance of information is widely accepted, and information systems are truly pervasive throughout business and governmental organisations. The growing dependence of most organisations on their information systems, coupled with the risks, benefits and opportunities IT carries with it, have made IT governance an increasingly critical facet of overall governance. Boards and management alike need to ensure that IT is aligned with enterprise strategies, and enterprise strategies take proper advantage of IT.

Security breaches are an increasingly common occurrence. As early as 1996, the US General Accounting Office (GAO) reported that the US Department of Defense experienced as many as 250,000 attacks on 15,000 systems the previous year, of which 65 percent were successful, costing hundreds of millions of dollars. More sobering is that only 400 of these were detected and only 20 reported. In 1996 it was largely a vulnerability. Five years later it is a definite threat, as illustrated by the recent US Federal Bureau of Investigation (FBI) investigation into the extortion of more than 100 e-commerce sites by attackers not only threatening to disclose customer information, but actually carrying out their threats. Many national governments have recognised the importance of security, establishing initiatives to reinforce such measures as segregating infrastructures according to their sensitivity, investing in better authentication methods and making users of the infrastructure accountable for their actions.

Executive management has a responsibility to ensure that the organisation provides all users with a secure information systems environment. Furthermore, organisations need to protect themselves against the risks inherent in the use of information systems while simultaneously recognising the benefits that can accrue from having secure information systems.

Thus, as dependence on information systems increases, so too does the criticality of information security, bringing with it the need for effective information security governance.

2. What Is Information Security?

Security relates to the protection of valuable assets against loss, misuse, disclosure or damage. In this context, "valuable assets" are the information recorded on, processed by, stored in, shared by, transmitted or retrieved from an electronic medium. The information must be protected

against harm from threats leading to different types of vulnerabilities such as loss, inaccessibility, alteration or wrongful disclosure. Threats include errors and omissions, fraud, accidents and intentional damage. Protection arises from a layered series of technological and non-technological safeguards such as physical security measures, background checks, user identifiers, passwords, smart cards, biometrics and firewalls. These safeguards should address both threats and vulnerabilities in a balanced manner.

In the ever-changing technological environment, security that is state-of-the-art today is obsolete tomorrow. Security must keep pace with these changes. It must be considered an integral part of the systems development life cycle process and explicitly addressed during each phase of the process. Security must be dealt with in a proactive and timely manner to be effective.

The objective of information security is "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*." While emerging definitions are adding concepts like information usefulness and possession—the latter to cope with theft, deception and fraud—the networked economy certainly has added the need for trust and accountability in electronic transactions such that for most organisations, the security objective is met when:

- Information is available and usable when required, and the systems that provide it can appropriately resist attacks and recover from failures (*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 between enterprise locations or with partners can be trusted (*authenticity* and *non-repudiation*)

The relative priority and significance of availability, confidentiality, integrity, authenticity and non-repudiation vary according to the data within the information system and the business context in which they are used. For example, integrity is especially important relative to management information due to the impact that information has on critical strategy-related decisions.

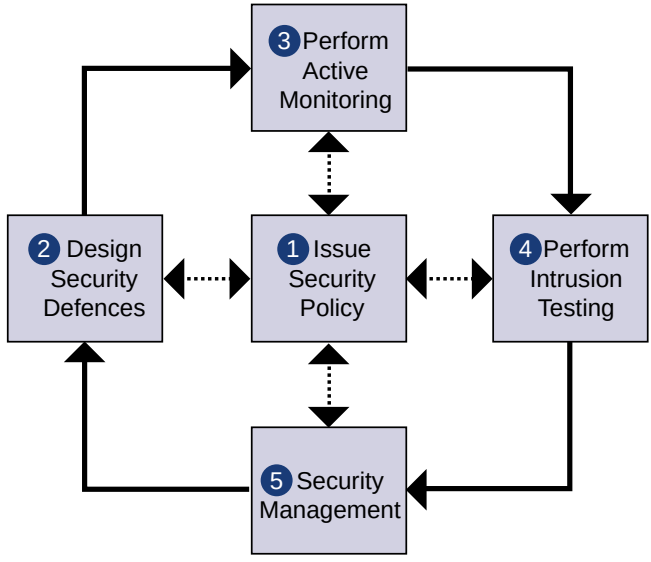
According to the International Guidelines for Managing Risk of Information and Communications Statement #1: *Managing Security of Information*, issued by the International Federation of Accountants, the six major activities involved in information security are:

- Policy Development—Using the security objective and core principles as a framework around which to develop the security policy
- Roles and Responsibilities—Ensuring that individual roles, responsibilities and authority are clearly communicated and understood by all
- Design—Developing a security and control framework that consists of standards, measures, practices and procedures
- Implementation—Implementing the solution on a timely basis, then maintaining it
- Monitoring—Establishing monitoring measures to detect and ensure correction of security breaches, such that all actual and suspected breaches are promptly identified, investigated and acted upon, and to ensure ongoing compliance with policy, standards and minimum acceptable security practices
- Awareness, Training and Education—Creating awareness of the need to protect information, providing training in the skills needed to operate information systems securely, and offering education in security measures and practices

To the latter should be added motivation, because people may be aware, but also need to be motivated to act. See Section 5 for an application of these activities against management level actions.

"The emerging approach to information security is not unlike the guard walking the corridors at night and testing the door handles."

However, the days of issuing a policy, educating users and then expecting that everyone will comply are gone. The speed with which risks emerge and the rate of change require a different and continuous approach, referred to as "test and patch." It implies continuous monitoring and testing of the infrastructure and environment for vulnerabilities and the required response in terms of security fixes through the security management function, improved defences and changed policies, as illustrated below.



3. Why Is Information Security Important?

Information systems can generate many direct and indirect benefits, and as many direct and indirect risks. These risks have led to a gap between the need to protect systems and the degree of protection applied. The gap is caused by:

- Widespread use of technology
- Interconnectivity of systems
- Elimination of distance, time and space as constraints
- Unevenness of technological change
- Devolution of management and control
- Attractiveness of conducting unconventional electronic attacks against organisations
- External factors such as legislative, legal and regulatory requirements or technological developments

This means that there are new risk areas that could have a significant impact on critical business operations, such as:

- Increasing requirements for availability and robustness
- Growing potential for misuse and abuse of information systems affecting privacy and ethical values
- External dangers from hackers, leading to denial-of-service and virus attacks, extortion and leakage of corporate information

Because new technology provides the potential for dramatically enhanced business performance, improved and demonstrated information security can add real value to the organisation by contributing to interaction with trading partners, closer customer relationships, improved competitive advantage and protected reputation. It can also enable new and easier ways to process electronic transactions and generate trust.

4. Who Should Be Concerned with Information Security Governance?

Too often information security has been dealt with as a technology issue only, with little consideration given to enterprise priorities and requirements. Responsibility for governing and managing the improvement of security has consequently been limited to operational and technical managers.

However, for information security to be properly addressed, greater involvement of boards of directors, executive management and business

process owners is required. For information security to be properly implemented, skilled resources such as information systems auditors, security professionals and technology providers need to be utilised. All interested parties should be involved in the process.

5. What Should the Board and Management Do?

Boards and management have several very fundamental responsibilities to ensure that information security governance is in force. They should:

"Adding security after the fact can cost up to 100 times more than doing it right from the start."

Understand Why Information Security Needs to be Governed

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

Ensure It Fits in the IT Governance Framework

As news of break-ins and losses related to hackers, computer viruses and other Internet-based threats grows more frequent, enterprise stakeholders are becoming concerned about the risks, regulatory requirements and investments associated with information security. Their need for assurance is putting the issue firmly in the lap of executive management and enterprise boards.

Effective security is not just a technology problem, it is a business issue. Related risk management must address the corporate culture, management's security consciousness and actions. Sharing of information with those responsible for governance is critical to success.

An information security programme is a risk mitigation method like other control and governance actions and should therefore clearly fit into overall enterprise governance. IT governance itself is emerging as a subject matter[1] and integral part of enterprise governance, with the goal of ascertaining that:

[1] See *Board Briefing on IT Governance*, also published by the IT Governance Institute.

- IT is aligned with the business, enables the achievement of business goals and maximises benefits
- IT resources are used responsibly
- IT related risks are managed appropriately

Within IT governance, information security governance becomes a very focused activity, with specific value drivers: integrity of information, continuity of services and protection of information assets.

For too long, information security was seen as a negative factor, creating value through nonoccurrence. However, as a result of global networking and extending the enterprise beyond its traditional boundaries, it is emerging as a value creator and opportunity builder in its own right, in particular through the instilling of trust among IT stakeholders.

Hence, information security should become an important and integral part of IT governance. Negligence in this regard will render the creation of IT value unsustainable in the long run.

Take Board Level Action

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

Take Management Level Action

- Write the security policy, with business input. (***Policy Development***[2])
- Ensure that individual roles, responsibilities and authority are clearly communicated and understood by all. This is imperative for effective security. (***Roles and Responsibilities***)
- Identify threats, analyse vulnerabilities and identify industry practices for due care.
- Set up a security infrastructure.
- Develop a security and control framework that consists of standards, measures, practices and procedures after a policy has been approved by the governing body of the organisation and related roles and responsibilities assigned. (***Design***)

[2] The key words highlighted in this sub-section refer to the International Federation of Accountants' statement on *Managing Security of Information*, described in Section 2.

"Don't treat security as an afterthought. Address it at every phase of the development life cycle."

- Decide what resources are available, prioritise possible countermeasures and implement the top priority countermeasures the organisation can afford. Solutions should be implemented on a timely basis, and then maintained. (***Implementation***)
- Establish monitoring measures to detect and ensure correction of security breaches, so that all actual and suspected breaches are promptly identified, investigated and acted upon, and to ensure ongoing compliance with policy, standards and minimum acceptable security practices. (***Monitoring***)
- Conduct periodic reviews and tests.
- Implement intrusion detection and incident response.
- Embed awareness of the need to protect information, and offer training in the skills needed to operate information systems securely and be responsive to security incidents. Education in security measures and practices is of critical importance for the success of an organisation's security programme. (***Awareness, Training and Education***)
- Ensure that security is considered an integral part of the systems development life cycle process and explicitly addressed during each phase of the process.

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

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

To Uncover Information Security Issues

- When was the last time top management got involved in security-related decisions? How often does top management get involved in progressing security solutions?
- Does management know who is responsible for security? Does the responsible individual know? Does everyone else know?
- Would people recognise a security incident when they saw one? Would they ignore it? Would they know what to do about it?
- Does anyone know how many computers the company owns? Would management know if some went missing?
- Has management identified all information (customer data, strategic plans, research results, etc.) that would cause embarrassment or competitive disadvantage if it were leaked?
- Did the company suffer from the latest virus attack? How many attacks did it have last year?
- Is the enterprise network being probed? Have there been intrusions? How often and with what impact?

- Does anyone know how many people are using the organisation's systems? Does anybody care whether they are allowed or not, or what they are doing?
- Is security considered an afterthought or a prerequisite?
- What would be the consequences of a serious security incident in terms of lost revenues, lost customers and investor confidence?

To Find Out How Management Addresses the Information Security Issues

- Is the enterprise clear on its position relative to IT and security risks? Does it tend toward risk-avoidance or risk-taking?
- How much is being spent on information security? On what? How were the expenditures justified? What projects were undertaken to improve security last year?
- How many staff had security training last year? How many of the management team received training?
- How does management decide who has access to the organisation's information and systems?
- How does the organisation detect security incidents? How are they escalated and what does management do about them?
- Is management prepared to recover from a major security incident?
- Is there a security programme in place that covers all of the above questions? Is there clear accountability about who carries it out?

To Self-assess Information Security Governance Practices

- Is management confident that security is being adequately addressed in the company?
- Is management aware of the latest IT security issues and best practices?
- What are other people doing, and how is the enterprise placed in relation to them?
- What is industry best practice and how does the enterprise compare?
- Does management regularly articulate and communicate the enterprise requirement for IT security?
- Does management have a view on how much the enterprise should invest in IT security improvements?
- Are IT security issues considered when developing business and IT strategy?
- Does the company keep abreast of security risks and available technical solutions?
- Does management obtain regular progress reports on the state of security and security improvement projects?
- Has management set up an independent audit of IT security? Does management track its own progress on recommendations?

7. What Should Information Security Governance Deliver?

Information security governance, when properly implemented, should provide four basic outcomes:

Strategic Alignment

- Security requirements driven by enterprise requirements
- Security solutions fit for enterprise processes
- Investment in information security aligned with the enterprise strategy and agreed-upon risk profile

Value Delivery

- A standard set of security practices, i.e., baseline security following best practices
- Properly prioritised and distributed effort to areas with greatest impact and business benefit
- Institutionalised and commoditised solutions
- Complete solutions, covering organisation and process as well as technology
- A continuous improvement culture

Risk Management

- Agreed-upon risk profile
- Understanding of risk exposure
- Awareness of risk management priorities

Performance Measurement

- Defined set of metrics
- Measurement process with feedback on progress made
- Independent assurance

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

The following questions provide the board of directors and executive management a sound way to begin implementing effective information security governance. These are the questions those responsible for governance should ask:

Questions for Directors

- Is information and information security critical to the entity? If so, does the board understand the criticality of information security?
- Has management issued a policy statement on information security? If it has, is the policy statement subject to continual updating? If it is not, why not?

- What are the top three critical information assets of the enterprise? What confidence does managment have regarding information *availability, confidentiality* and *integrity* over these critical information assets?
- Does management know where the enterprise is most vulnerable within the IT infrastructure?
- Can the entity continue to operate if the critical information is *unavailable, compromised* or *lost*? What would be the consequences of a security incident in terms of lost revenues, lost customers and investor confidence? What would be the consequences if the infrastructure became inoperable?
- What are the information assets subject to laws and regulations? What has management instituted to assure compliance with them?
- Does the information security policy address the concern of the board and management on information security ("tone at the top"), cover identified risks, establish an appropriate infrastructure to manage and control the risks, and establish appropriate monitoring and feedback procedures?
- Has the organisation ever had its network security checked by a third party?
- Does the organisation provide information security awareness training to all and is security part of staff and management's appraisals?
- Is management confident that security is being adequately addressed in the company?

Questions for Management

- How is the board kept informed of information security issues? When was the last briefing made to the board on security risks and status of security improvements?
- When was the last risk assessment made on the criticality of information security assets? When is the next risk assessment scheduled?
- Does the risk assessment consider whether the entity can continue to operate if the critical information is *unavailable, compromised* or *lost*? Does it cover the consequences of a security incident in terms of lost revenues, lost customers and investor confidence? Does it determine what the consequences would be if the infrastructure became inoperable?
- Does the risk assessment consider what information assets are subject to laws and regulations? Does it result in adequate procedures to assure compliance with these laws and regulations?
- Is IT security risk assessment a regular agenda item on IT management meetings and does management follow through with improvement initiatives?
- What are other people doing, and how is the enterprise placed in relation to them? What is industry best practice and how does the enterprise compare?

- When was the latest policy statement issued on information security?
- Does this policy statement adequately cover:
  - The critical information security assets?
  - The importance placed on information security by the board and by management ("tone at the top")?
  - The identified risks?
  - The control mechanisms established to address these risks?
  - The monitoring and feedback procedures?
- When was the last performance review made of the person responsible for information security (i.e., the information security officer)? Is the process to keep management informed on security issues by the information security officer adequate?
- What safeguards have been established over systems connected to the Internet to protect the entity from virus and other attacks? Are the systems being actively monitored and is management kept informed of the results?
- What information security awareness training has been established and does it appear adequate considering the assessed risks? Does it reach all parties involved in IT?
- What safeguards have been established over the physical security over computer assets and do they appear adequate?
- When was the last time an information security audit was performed? Does management track its own progress on recommendations?
- Is there a security programme in place that covers all of the above questions? Is there clear accountability about who carries it out?

There are some fundamental steps boards and management can take to ensure that effective information security governance is implemented in their enterprise. Those steps are:

Adopt Best Practices

<u>At the Board of Director Level</u>

- Establish ownership for security and continuity with enterprise managers.
- Create an audit committee that clearly understands its role in information security and how it will work with management and auditors.
- Ensure that internal and external auditors agree with the audit committee and management how information security should be covered in the audit.
- Require that the head of security report progress and issues to the audit committee.
- Develop crisis management practices, involving executive management and the board of directors from pre-agreed thresholds onward.

<u>At the Executive Management Level</u>

- Establish a security function that assists management in the development of policies and assists the enterprise in carrying them out.

- Create a measurable and management-transparent security strategy based on benchmarking, maturity models, gap analysis and continuous performance reporting.
- Conduct an annual executive risk brainstorming session, prepared by security and audit professionals (internal and external), resulting in actionable conclusions and followed up until closure.
- Develop what-if scenarios on information security and risk, leveraging the knowledge of the specialists.
- Establish clear, pragmatic enterprise and technology continuity programmes, which are continually tested and kept up-to-date.
- Conduct information security audits based on a clear process and accountabilities with management tracking closure of recommendations.
- Develop clear policies and detailed guidelines, supported by a repetitive and assertive communications plan that reaches every employee.
- Constantly assess vulnerabilities through monitoring system weaknesses (CERT), intrusion and stress testing, and testing of contingency plans.
- Make business processes and supporting infrastructures resilient to failure, especially targeting single points of failure.
- Establish security baselines and rigorously monitor compliance.
- Run security responsiveness programmes and conduct frequent penetration tests.
- Harden all security and critical server and communications platforms by appling a high level of control.
- Base authorisation on business rules and match the authentication method to the business risk.
- Include security in job performance appraisals and apply appropriate rewards and disciplinary measures.

Consider Critical Success Factors

Make sure that:

- There is awareness that a good security programme takes time to evolve.
- The corporate security function reports to senior management and is responsible for executing the security programme.
- Management and staff have a common understanding of security importance, requirements, vulnerabilities and threats, and understand and accept their own security responsibilities.
- Third-party evaluation of security policy and architecture is conducted periodically.
- The security function has the means and ability to administer security and especially to detect, record, analyse significance, report and act upon security incidents when they do occur, while minimising the probability of occurrence by applying intrusion testing and active monitoring.
- There are clearly defined roles and responsibilities for risk management ownership and management accountability.
- 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 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 are used to raise awareness and increase co-operation with suppliers for security and continuity needs.
- Policy enforcement is considered and decided upon 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 that employees perform their duties in an ethical and secure manner.
- Management is leading by example.

Introduce Performance Measures

To Determine If Information Security Is Succeeding

- No incidents causing public embarrassment
- Reduced number of new implementations delayed by security concerns
- Number of critical business processes relying on IT that have adequate continuity plans
- Number of critical infrastructure components with automatic availability monitoring
- Measured improvement in employee awareness of ethical conduct requirements, system security principles and performance of duties in an ethical and secure manner

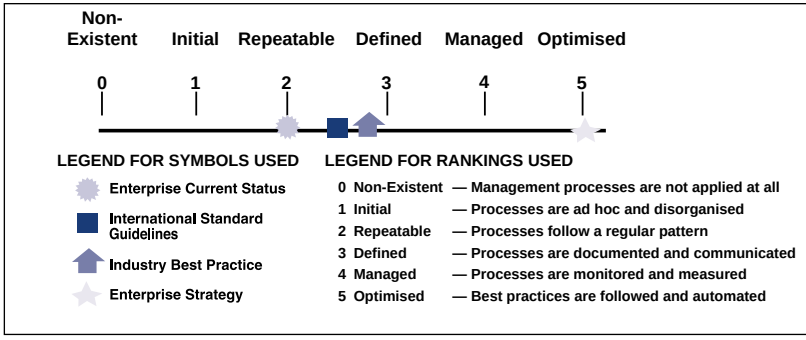
To Determine If Information Security Governance Is Succeeding

- Full compliance, or agreed-upon and recorded deviations from minimum security requirements
- Percent of IT-related plans and policies developed and documented covering IT security mission, vision, goals, values and code of conduct
- Percent of IT security plans and policies communicated to all stakeholders

9. How Does My Organisation Compare?

Boards of directors and executive management can use an information security governance maturity model to establish rankings for security in an 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, which is not necessarily at the top level
- 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



Maturity Level	Description
0	**Non-Existent** • Risk assessment for processes and business decisions does not occur. The organisation does not consider the business impacts associated with security vulnerabilities and with 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 IT security. Responsibilities and accountabilities are not assigned for ensuring security. Measures supporting the management of IT security are not implemented. There is no IT security reporting and no response process to IT security breaches. There is a complete lack of a recognisable system security administration process. • There is no understanding of the risks, vulnerabilities and threats to IT operations or the impact of loss of IT services to the business. Service continuity is not considered as needing management attention.

Maturity Level	Description
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 IT security, but security awareness depends on the individual. IT security is addressed on a reactive basis and not measured. IT security breaches invoke "finger pointing" responses if detected, because responsibilities are unclear. Responses to IT 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. • Responsibilities and accountabilities for IT security are assigned to an IT security co-ordinator with no management authority. Security awareness is fragmented and limited. IT security information is generated, but not analysed. Security tends to respond reactively to IT 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. IT 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. IT security procedures are defined and fit into a structure for security policies and procedures. Responsibilities for IT security are assigned, but not consistently enforced. An IT security plan exists, driving risk analysis and security solutions. IT security reporting is IT-focused, rather than business-focused. Ad hoc intrusion testing is performed. • Management communicates consistently the need for continuous service. High-availability components and system redundancy are being applied piecemeal. An inventory of critical systems and components is rigorously maintained.

Maturity Level	Description
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 IT security are clearly assigned, managed and enforced. IT 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. IT security processes are co-ordinated with the overall organisation security function. IT 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 where a structured, organisation-wide process is enforced, followed regularly and managed well. • IT security is a joint responsibility of business and IT management and is integrated with corporate security business objectives. IT 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. IT 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 is the basis for continuous improvements. Security processes and technologies are integrated organisation-wide. • Continuous service plans and business continuity plans are integrated, aligned and routinely maintained. Buy-in for continuous service needs is secured from vendors and major suppliers.

10. What Do Regulatory and Standards Bodies Say?

Financial regulators are instructing the banking industry to focus on operational risk within which security and IT are very significant. All major past risk issues—they claim—have been caused by breakdowns in internal control, oversight or IT.

Organisation for Economic Co-operation and Development, Guidelines for the Security of Information Systems (1992)

The OECD's *Guidelines for the Security of Information Systems* are designed to assist countries and enterprises to construct a framework for security of information systems. The guidelines are intended to:

- Raise awareness of risks to and safeguards for information systems
- Offer a general framework to aid in the development and implementation of effective measures, practices and procedures for the security of information systems and encourage co-operation between the public and private sectors regarding same
- Promote confidence in information systems, their implementation and use
- Facilitate national and international development, use and security of information systems

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

International Federation of Accountants, Managing Security of Information (1998)

The objective of information security is "the protection of the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality, and integrity." Any organisation may consider the security objective met when those three criteria are satisfied, that is, when information systems are available and usable when required (availability); data and information are disclosed only to those who have a right to know it (confidentiality); and data and information are protected against unauthorised modification (integrity).

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

Information security is taking on increased importance because of the expanding incidences and types of risks existent. Threats to information systems may result from intentional or unintentional acts and may generate from internal or external sources. They may emanate from technical conditions, natural disasters, environmental conditions, human factors, unauthorised access or viruses. In addition, business dependencies (reliance on third-party communications carriers, outsourced operations, etc.) can potentially result in a loss of management control and oversight.

International Organisation for Standardisation Standard 17799 (2000)

ISO 17799 (based on part one of BS 7799) is intended to serve as a single reference point for identifying the range of controls needed for most situations where information systems are used in industry and commerce. It is suitable for use by any size organisation. It treats information as an asset that, like other important business assets, has value to the organisation and consequently needs to be suitably protected.

Information security is characterised within ISO 17799 as the preservation of:

- Confidentiality—Ensuring that information is accessible only to those authorised to have access to it
- Integrity—Safeguarding the accuracy and completeness of information and processing methods
- Availability—Ensuring that authorised users have access to information and associated assets when required

Information security protects information from a wide range of threats in order to ensure business continuity, minimise business damage, maximise return on investments and capitalise on business opportunities. Security is achieved by implementing a suitable set of controls, which consist of policies, practices, procedures, organisational structures and/or software functions.

American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants, SysTrust™ Principles and Criteria for Systems Reliability V2.0 (2001)

The SysTrust service is an assurance service designed to increase the comfort of management, customers and business partners with the systems that support a business or a particular activity. The SysTrust service entails the certified public accountant providing an assurance

service in which he or she evaluates and tests whether a system is reliable when measured against four essential principles: availability, security, integrity and maintainability.

- Availability—The system is available for operation and use at times set forth in service-level statements or agreements.
- Security—The system is protected against unauthorised physical and local access.
- Integrity—System processing is complete, accurate, timely and authorised.
- Maintainability—When necessary, the system can be updated in a way that does not interfere or conflict with its availability, security and integrity.

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

Because the SysTrust framework is scalable, enterprises have the flexibility to choose any or all of the SysTrust standards for verification. An opinion rendered on all four standards constitutes an opinion on the overall reliability of the system. The certified public accountant can also render an opinion on an individual standard, such as availability or security, where the opinion applies only to the particular standard, not the overall reliability of the system.

Information Systems Audit and Control Foundation/IT Governance Institute, Control Objectives for Information and related Technology (COBIT®)

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

COBIT further divides IT into 34 processes belonging to four domains (Planning and Organisation, Acquiring and Implementing, Delivery and Support, Monitoring). The three processes most directly related to information security are:

- Planning and Organisation Process 9—Assess risks
- Delivery and Support Process 4—Ensure continuous service
- Delivery and Support Process 5—Ensure systems security

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

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

The more detailed elements of COBIT provide some 300 detailed control objectives for management and IT practitioners who are looking for best practices in control implementation, and extensive audit guidelines building on these objectives. The latter are geared toward those needing to evaluate and audit the degree of control and governance over IT processes.

Recent COBIT developments added a management and governance layer, providing management with a toolbox containing:

- Performance measurement elements (outcome measures and performance drivers for all IT processes)
- A list of critical success factors that provides succinct non-technical best practices for each IT process
- A maturity model to assist in benchmarking and decision-making for control over IT

References

IT Governance Institute, COBIT (*Control Objectives for Information and related Technology*) 3rd Edition, 2000, *www.ITgovernance.org* and *www.isaca.org*

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

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

International Organisation for Standardisation, *Standard 17799*, 2000

US General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, 1996 (*www.fas.org/irp/gao/aim96084.htm*)

British Standards Institution, *BS 7799-2—Code of Practice for Information Security Management*, 1999