Information Security Management Systems and Standards

Lim Thow-Chang, Kwan Siew-Mun and Alvin Foo
Sun Professional Services, Singapore

Mr Lim and Mr Kwan participate in the Security and Privacy Standards Technical Committee (SPSTC) while Mr Foo participates in the Information Security Management Working Group (ISM WG) under SPSTC.

Abstract

This article provides an appreciation of the different considerations and involvement for an effective security management of an organisation's core assets, principally information. It describes the process involved in developing an Information Security Management System (ISMS) as well as some background on the development of the ISMS standards.

1. Introduction

Information is a vital asset in any organisation. The protection and security of this information is of prime importance to many aspects of an organisation's business. It is important that an organisation should not only implement a set of security policy, standards, and procedures for information security but also manage and maintain them.

Increasingly, organisations and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Sources of damage such as computer viruses, computer hacking and denial of service attacks have become more common, more ambitious and increasingly sophisticated.

Traditionally, companies merely used the Internet as another channel to cast their net to a wider audience. Nowadays, more organisations differentiate themselves by providing value-added services such as target marketing, customer relationship management, electronic commerce, payment aggregation, and other innovative services. Organisations also use the public networks to establish business relationships and transactions, for example, supply and order chain and application service provisions. IT security thus becomes the focal and strategic component for these companies and corporation to value add their business and to develop new business models.

For business relationship to thrive on the public network, there must be certain standards and trust that all wishing to do business should abide. There is the critical need of establishing IT security standards, whic h corporations and companies can safeguard information assets and well as relationship on a somewhat equal footing.

2. ISMS Standards Development

In the early 1990s, the UK Department of Trade and Industry (DTI) in response to demands from industry set up an Industry Working Group, which comprised of experienced information security managers. They produced a Code of Practice for Information Security Management, which was published in September 1993. This Code formed the basis of the British Standard BS7799, which was published in 1995. Part 2 of the standard, which provides the specifications of the ISMS, was published in 1998. The standard was later revised in 1999.

The BS7799 Part 2 standard is organised into 10 major categories, 36 control objectives and 127 general controls which are appropriate to their particular business or specific area of responsibility. It describes detailed security controls for computers and networks, provides guidance on security policies, staff security awareness, business continuity planning, and legal requirements.

BS7799 is being fast-tracked as an International Standard. ISO/IEC 17799:2000 was formally approved by the October 2000 International Standards Organisation (ISO) JTC1/SC27/WG1 meeting in Tokyo. ISO/IEC 17799:2000 is based on the BS7799 Part 1 1999 standard.

ISO/IEC has other security management guidelines like the TR 13335 Part 1 to 5. Although TR 13335 is not a formal standard, it represents a set of security management practices and techniques that have been developed and agreed by many leading international companies and organisations.

3. Information Security Requirements

The purpose of information security is to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents. Information security is characterised here as the preservation of:

- Confidentiality: ensuring that information is accessible only to those authorised to have access;
- 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.

As information is increasingly being processed and stored in a technological environment, the following security issues pertaining to IT are also important:

- Non-repudiation: ability to prove an action or event has taken place, so that this event or action cannot be repudiated later

- Accountability: the property that ensures that the actions of an entity may be traced uniquely to the entity
- Authenticity: the property that ensures that the identity of a subject or resource is the one claimed
- Reliability: the property of consistent intended behaviour and results

As information is continually being processed, stored, transmitted via technological means, so has the protection of the information, which now leans heavily towards a technological flavour. This, however, does not negate that traditional security such as physical, environmental, personnel etc. are no longer necessary. Instead, security vigilance in these areas is ever more important now that technology has forced the weakest link onto such areas.

Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organisational structures and software functions. These controls need to be established to ensure that the specific security objectives of the organisation are met.

To have an effective information security process in place, the following success factors have been identified [2]:

- security policy, objectives and activities that reflect business objectives;
- an approach to implementing security that is consistent with the organisational culture;
- visible support and commitment from management;
- a good understanding of the security requirements, risk assessment and risk management;
- effective marketing of security to all managers and employees;
- distribution of guidance on information security policy and standards to all employees and contractors;
- providing appropriate training and education;
- a comprehensive and balanced system of measurement, which is used to evaluate performance in information security management and feedback suggestions for improvement.

4. Information Security Management Systems

Information security planning and management is the overall process of establishing and maintaining an information security programme within an organisation. Figure 1 shows the possible main activities within this process. It is important that all of the

activities and functions identified in Figure 1 are addressed within the culture and structure of the organisation, and its manner of conducting their business. It is implicit that management reviews are conducted as part of all these activities and functions.

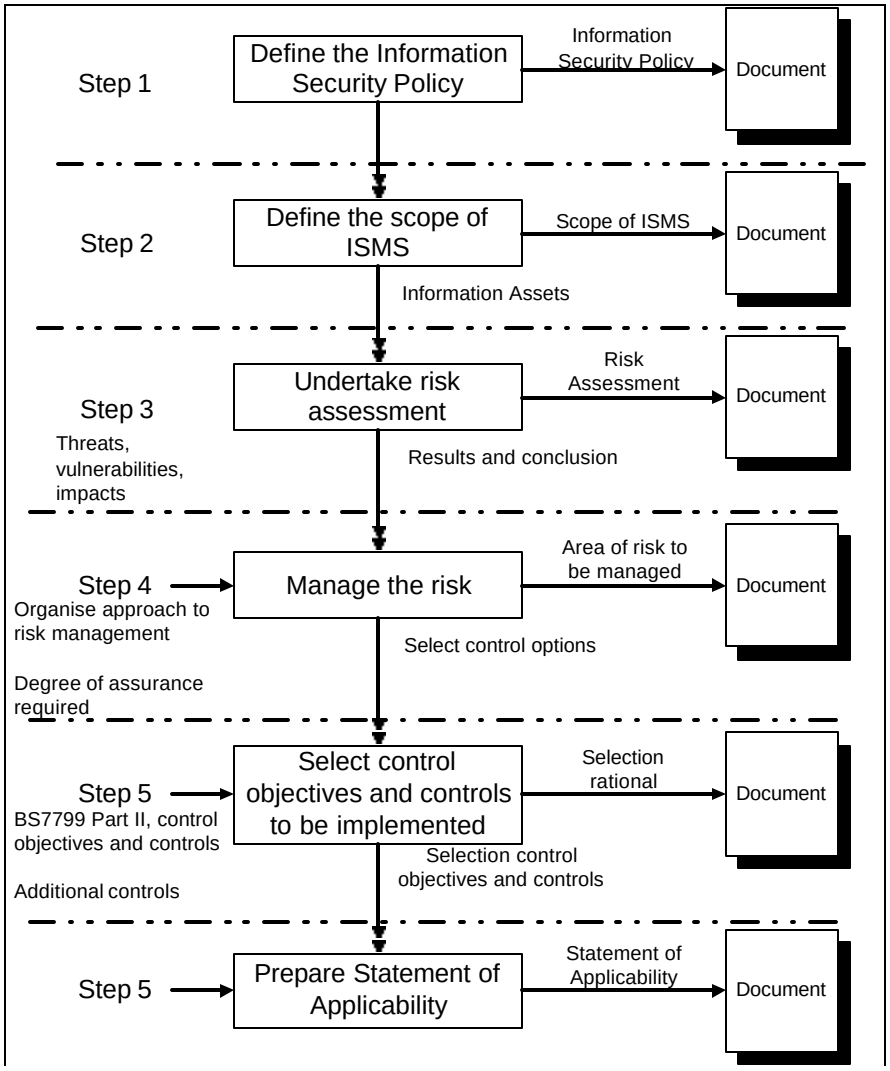

Figure 1: Overview of the Information Security Management Systems (ISMS)

4.1 Corporate Information Security Policy

The objective of the Corporate Information Security Policy is to provide management direction and support for information security. Therefore, management should set a clear policy direction and demonstrate support for, and commitment to, information security across the entire organisation.

The policy document should be approved by the senior management, published and communicated, as appropriate, to all employees. It should state management commitment and set out the organisation's approach to managing information security.

4.2 Scope of the ISMS

The scope of an ISMS can be defined in terms of the organisation as a whole, or parts of the organisation, covering the relevant assets, systems, applications, services, networks and technology. It should clearly define the boundaries. The ISMS could encompass:

- All of an organisation's information systems
- Some of an organisation's information systems or
- A specific information system.

An organisation may need to define different ISMS for different parts or aspects of its business as the organisation has different business units with disparate business goals and requirements. For example, an ISMS may be defined solely for an organisation's EDI environment for its procurement business unit.

4.3 Risk Analysis

Risk analysis is to:

- identify the threats and vulnerabilities of the information and information processing facilities and
- assess the likelihood of their occurrence and the impact to the business goals.

There are four basic options for a corporate risk analysis strategy [3]:

- **Baseline Approach**. Use the same baseline approach for all information processing, transmission and storage mechanisms, irrespective of risks facing the systems, and accept that the level of security may not always be appropriate,
- **Informal Approach**. Use an informal approach to perform risk analysis and concentrate on those mechanisms which are perceived as being exposed to high risks,
- **Formal Approach**. Conduct detailed risk analysis using a formal approach for all information processing, transmission and storage mechanisms, or
- **Hybrid Approach**. Carry out an initial 'high level' risk analysis to identify all information processing, transmission and storage mechanisms that are

exposed to high risks and those which are critical for the business, followed by a detailed risk analysis for these mechanisms, and applying baseline security to all other systems.

Information assets should be classified appropriately to reflect the sensitivity, importance and impact to business goals and requirements. The classification of information assets can ensure that the right focus and priority is placed on the more important information assets.

4.4 Risk Management

Different organisations have different risk tolerance level as well as risk appetite. Risk management consists of the process of identifying, controlling and minimising or eliminating security risks that may affect information systems, at an acceptable cost.

Appropriate and justified controls should be identified and selected to reduce the assessed risks to an acceptable level. The organisations must take the following factors into account when selecting controls:

- Existing and planned controls;
- IT architecture and infrastructure;
- IT security architecture and infrastructure;
- Business and operational requirements;
- Technology and budgetary constraints.

In order to select controls that effectively protect against the assessed risks, the results of the risk analysis should be considered. The vulnerabilities with associated threats indicate where additional protection may be needed, and what form it should take.

When the controls are selected, setting up a management forum to ensure that there is a clear direction and visible management support for security initiatives should therefore be considered. That forum should promote security within the organisation through appropriate commitment and adequate provision of resources. Roles and responsibilities should be clearly assigned, communicated and documented.

The forum may be part of an existing management body. Typically, such a forum undertakes the following:

- reviewing and approving information security policy and overall responsibilities;
- monitoring significant changes in the exposure of information assets to major threats;
- reviewing and monitoring information security incidents;
- approving major initiatives to enhance information security.

4.5 Selection of Controls

Once the risk areas have been identified, controls should be selected and implemented to ensure risks are reduced to an acceptable level.

One of the key considerations in this selection process is the cost of implementation in relation to the perceived impacts and losses if a security breach occurs. Non-monetary factors such as loss of reputation should also be taken into account.

The BS7799 standard describes a number of general controls that can be considered as good guiding principles for implementing information security. The controls can be categorised into the following focus areas: -

- Security policy
- Security organisation
- Assets classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- System development and maintenance
- Business continuity management
- Compliance

These focus areas are either based on essential legislative requirements or considered to be common best practice for information security.

4.6 Statement of Applicability

The statement of applicability is an important document stating the reasons for the selection of the controls for the ISMS. It is recognised that certain controls may not be available or suitable and there are good reasons for excluding them. These exclusions must also be documented in the statement of applicability citing the reasons and how the risk is managed.

5. Conclusion

Information and the supporting processes, systems and networks are important business assets. Confidentiality, integrity and availability of information are essential to maintain competitive edge, cash flow, profitability, legal compliance and commercial image.

In addition, reliance on technology to facilitate the flow of information have become more complex and harder to manage. Though technology is increasingly aligning towards more open integration and stronger security functions, the same technology has permitted greater ease to deny, disable, collect illegally, and the decipherment of information. This has placed greater emphasis on organisation to continually monitor, reassess, and strengthen defence against these threats.

The correct implementation of security controls relies heavily upon a well-structured and documented information security plan. Security awareness and training associated with each IT system should take place in parallel. For the implementation of controls, all the necessary steps described in an information security plan should be carried out.

Together, the formulation of an information security process and its implementation requires heavily the visible support of management. Strong management leadership and support should be established to approve the information security policy, assign security roles and co-ordinate the implementation of security across the organisation. Its key participation cannot be understated

References

[1] ISO/IEC 17799:2000 Information Technology – Code of practice for information security management.

[2] Guidelines for the Management of IT Security (GMITS): Part 1 to 3 - Techniques for the Management of IT Security, ISO/IEC JTC 1/SC27.

[3] BS 7799-1 Information security management – Part 1: Code of practice for information security management.

[4] BS 7799-2 Information security management – Part 2: Specification for information security management systems