# CHAPTER 3

## INFORMATION SECURITY MANAGEMENT SYSTEM

In recent years, apart from the familiar 'Quality Management System' (QMS), much has been talked about the term 'Information Security Management System' (ISMS) or 'Information Security Management Framework', especially in enterprises where information is a mission-critical asset. Whilst expanding their business activities online, enterprises also face with the need to strengthen their information security practices and to make them more effective and systematic. In that case, developing ISMS appears to be a timely, good solution. There have, here and there, been few successful models in implementing ISMS. Given this context, this chapter aims at exploring ISMS models by seeking the following answers:

- What is an ISMS? What's about its history?
- What are some approaches to modern ISMS?
- What are ISO/IEC 17799:2000 & BS 7799-2:2002?
- Why to develop an ISMS based on ISO/IEC 17799:2000 & BS 7799-2:2002? How to develop?

*"Without a deep change in security culture & practices, buying technology will bring little safety".*
*Raymond R. Panko[7], Professor of Information System*
*University of Hawaii, Manoa.*

## 1. INTRODUCTION TO INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

To many people, the word 'information' is not so unfamiliar. People hear it and think of something related to advanced technology. More impressive is 'security'. It makes people cast back the 'hot' stories in which hackers successfully intruded into computer system protected at the highest level or FBI used state-of-the-art technologies tracing back to the 'hiding' places of those hackers over the network. Adding 'management', people think further about the way to control or deal with those adverse actions, whereat protecting computing infrastructure. Yet, there must have been some confusion that what is an 'Information Security Management System'.

Information Security Management System (ISMS) is a systematic approach to managing sensitive organization's information so that it remains secure. It strives to create a foolproof system to protect the availability, integrity and confidentiality of organization's most vital asset information. It encompasses people, processes and IT systems (URL:http://www.tqmi.com/nl/is.pdf[48]). In the 1990s, for instance, the British Standards Institution (BSI) has published a code of practice, namely BS 7799 for these systems.

The Ministry of Information Technology of India (MIT/India) – the world's top software production power – provided another point of view, which is, in my opinion, is more concrete than the previous one. According to them, Information Security Management System is the means by which senior management monitor and control their security, minimizing the residual business risk and ensuring that security continues to fulfill corporate, customer and legal requirements (URL:http://stqc.nic.in/itservices/overview.htm[49]). In order to build an appropriate ISMS, the first step of an organization should do is to assess and define specific security requirements, design a solution meeting those unique requirements, deploy the necessary policies, technology and procedures and continuously maintain, adapt and improve that solution to the changing requirements.

Given those definitions, I would summarize that an ISMS is a mechanism in which people, processes and computing infrastructure interact each other, aiming at securing organization's most critical information assets in terms of availability, integrity and confidentiality.

## 2. A GLANCE AT HISTORY OF ISMS

Like Internet, ISMS models historically derived from the military operation. Protecting strategic information was, and still is, the main priorities of military functions. Throughout the years, military took care mostly of espionage and connected with ISMS, loosing confidentiality or integrity of strategic information.

ISMSs were developed uniquely to work out those challenges. One of the most common ISMS called "Department of Defense Trusted Computer System Evaluation Criteria" – or shortly titled "Orange Book", composes of several books full of criteria (TCSEC[28]. In 1991, TCSEC was replaced with FIPS - Federal Information Processing Strategy as a result of common work of National Institute of Standards & Technology - NIST and National Security Agency - NSA (Schell & Brinkley[29]). Other popular models are Clark-Wilson (Clark and Wilson[30]) or Bell La Padula model, which are published by the Commission of European Community and based on DoD criteria – ITSEC Information Technology Security Evaluation Criteria (ITSEC[31]). Besides these models, more and more security-related standards, controls and regulations for ISMS models were set up to meet the ever-increasing needs of information security practices (Vigilinx[14]). Inheriting distinct advantages from their origins, those newly-developed ISMSs are now of a wide range of concerning areas, up-to-date and well-designed. Such examples are ISO 17799:2000 and BS 7799-2:2002, which will be intimately presented in section 4.

## 3. SOME APPROACHES TO MODERN ISMSs

Before developing an ISMS, I find it useful to review three approaches to ISMS models, which are typical in terms of modern viewpoint and high feasibility. Throughout this section, readers may realize that though they are different in structures and practices, all these models, overally, arrive at one common philosophy – PDCA (Plan, Do, Check and Act), whose father is Dr. Deming William Edwards (Module Note WMG QMT[32]). For reading convenience, three models will be named after the organizations whose devised them.

### 3.1 The CERT/CC model

Christopher and Audrey[8], along with presenting the OCTAVE$^{SM}$ method, also explain how to develop an ISMS.

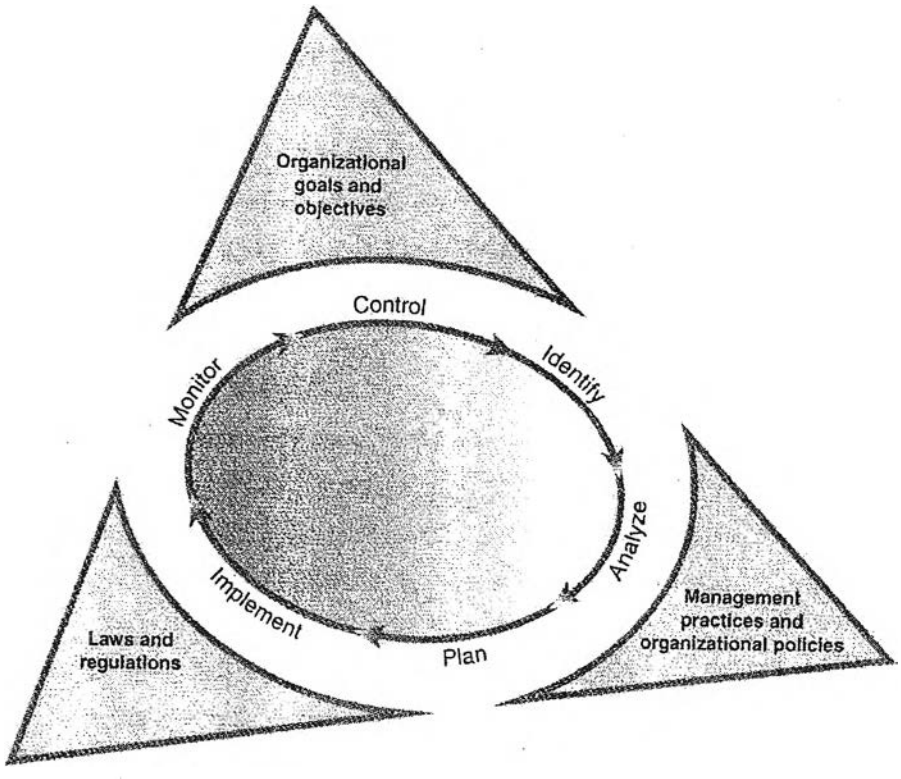


***FIGURE 3-1:*** *Information Security Risk Evaluation in relation to an Information Security Management Framework - Adapted from Figure 14-3, p.278, Christopher and Audrey[8].*

As we can see from Figure 3-1, the information security risk evaluation, presented in Chapter 2, is just a 'piece', containing two main processes – identify and analyze, of the whole framework. The post activities of risk evaluation are nothing more than a *Plan-Do-Check-Act* cycle, ensuring that the selected aspects of the organization's protection strategy and mitigation plans are implemented. To build on the risk assessment results, it's required to address the following operations:

- *Plan (Plan)* for implementation by developing detail action plans for key aspects of the organization's protection strategy and risk mitigation plans
- *Implement (Do)* action plans as specified
- *Monitor (Check)* the execution of action plans for schedule and effectiveness
- *Control (Act)* any variations in action plans by implementing corrective measure

What's worth mentioning in figure 3-1 is that the whole framework, as described by Christopher and Audrey[8], must be put in a triangle context with three angles concerning three aspects – (1) supporting organizational goals and objectives; (2) complying with laws and regulations; and (3) being integrated with management practices and

organizational policies. Doing this way, an organization is able to properly integrate its information security management system with its business processes.

The above figure also reveals the fact that information security management system is the ongoing process of identifying and addressing information security risks. To be more specific, Figure 3-2 illustrates the operations required by the information security risk management framework as well as the major tasks completed during each operation.

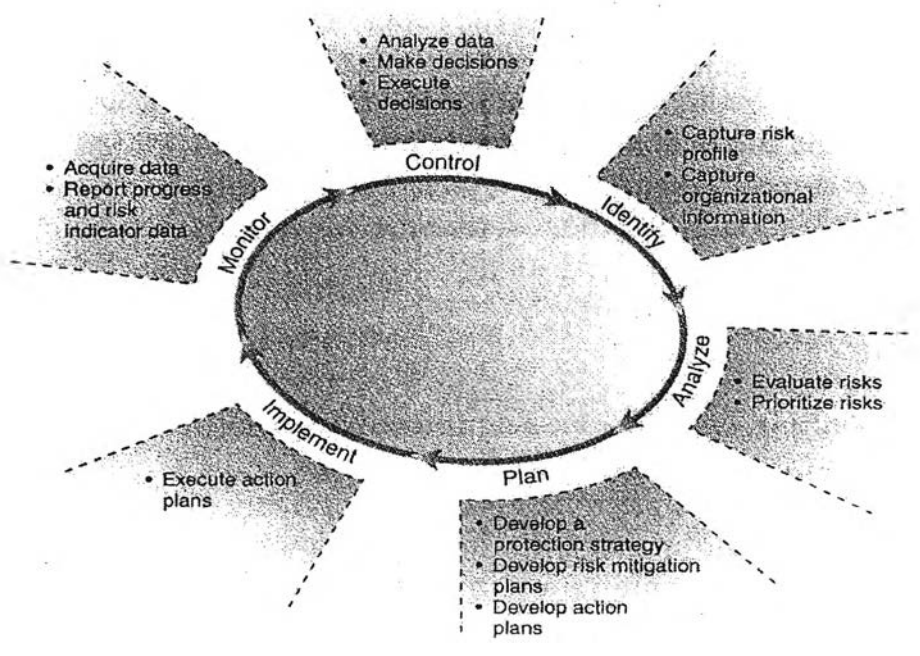


***FIGURE 3-2:*** *Operations & Tasks of the Information Security Management Framework – Adapted from Figure 14-4, p.280, Christopher and Audrey*[8].

➢ ***Identify***

Identification is the process of transforming uncertainties and issues related to how well an organization's assets are being protected into distinct risks. The objective of this activity is to anticipate risks before they occur and to incorporate this information into the organization's information security process. Overall, when implemented, risk identification should:

- enable staff members throughout the organization to identify and communicate risk-related information periodically or as needed
- provide a means for documenting all risk-related information in a consistent format

The output of this identification process is a documented set of risks, including information about the organization's critical assets, the threat to those assets and applicable vulnerabilities (both organizational and technological).

➢ ***Analyze***

Analysis is the process of projecting how extensive risks are and using those projections to set priorities. The objective of risk analysis is to gain a better understanding of risks by examining all risk-related data in relation to a set of organizational evaluation criteria (like those presented in processes 1 to 3 of the OCATVE$^{SM}$ method). CERT/CC suggested that risk analysis should include techniques for setting priorities based on established evaluation criteria (Christopher and Audrey[8]). The criteria define aspects of impact (and probability, if used) that are most important to the organization's business objectives (This issue will be mentioned in relation to performing OCATVE$^{SM}$ in Chapter 4). The analysis process should:

- enable staff members to evaluate or re-evaluate risks for impact and probability (if used)
- provide personnel who analyze risks with sufficient guidance to set or revise priorities

The output of this analyze process is information to determine which risks to mitigate actively and after setting priorities, to decide what the organization can do to address those risks.

➢ ***Plan***

Planning is the process of determining which actions to take to improve the organization's security posture and protect its critical assets. The objectives of planning are developing and maintaining the following three security requirements:

- A protection strategy to improve the organization's overall security posture
- Mitigation plans designed to reduce risks to the organization's critical assets
- Detailed action plans to implement key aspects of the protection strategy and risk mitigation plans

The planning process should include the following specifications:

- Require planners to review existing plans and strategies for common actions
- Provide planners with established methods for incorporating return on investment, dealing with limited resources and prioritizing corrective actions
- Enable the use of technological and organizational solutions

- Require planners to select measures for monitoring plans against their schedules and success criteria
- Afford planners the authority to allocate or reallocate resources
- Incorporate all necessary reviews and approvals

➢ ***Implement***

Implementation is the process of taking planned action to improve an organization's security posture. The objective is to execute all action plans according to the schedules and critical success factors defined during the planning process. Implementation is tightly linked to the monitoring and control processes to follow and correct the implementation progress.

The implementation process should:

- communicate to organizational personnel that staff members are authorized to implement their assigned action plans
- enable staff members to reprioritize existing work tasks to incorporate their action plan activities
- provide staff members with sufficient funds, equipment and other required resources to complete the action plans

➢ ***Monitor***

This process tracks action plans to determine their status quo and reviews organizational data for indications of new risks or changes to existing risks. The objectives are to collect accurate, timely and relevant information about the progress of action plans being implemented and any major changes to the organization's operational environment that could indicate the existence of new risks or significant changes to existing risks.

➢ ***Control***

Controlling risk is a process, where designated personnel adjust the course of action plans and determine whether changing organizational conditions indicate the presence of new risks. The objectives of controlling risks are to make informed, timely and effective decisions about corrective measures for action plans and about whether to identify new risks to the organization.

Continuous control of risks should be tightly integrated into the organization's management practices. The control process should:

- ensure that responsibility for making control decisions is formally assigned and accepted
- provide personnel with guidance for weighing alternatives and making trade-offs
- provide a mechanism for elevating sensitive issues to an appropriate organizational level
- be integrated with general business risk planning, implementation and identification activities in the organization.

In sum, I have some remarks on this model:

- The model actively adopts the Deming's philosophy, which has proven its effectiveness throughout the years in the industry.
- Organizations, after conducting the OCTAVE[SM] method, may find it convenient and ready to go on with this model.
- However, the plan process emphasizes much on details of mitigation plan such as how to mitigate the risk immediately or soon without paying much attention to develop organizational policies, which is the core of the risk mitigation plan in the long-term. In other words, this model is just targeting at 'curing' syndromes rather than targeting at root of those syndromes.
- This model follows the top-down approach. It starts from with top management and ends with down technology.
- Business continuity planning and how it is incorporated into the entire framework are not clearly mentioned.
- There is no high attention paid to training and awareness program on security issues, which are indispensable in effective detecting and responding.

### 3.2 The PricewaterhouseCoopers model (PWCs Thailand)

Eralp Gullep, a senior manager of Global Risk Management Solutions at PricewaterhouseCoopers Thailand, introduced an Information Security Management Framework, which have been successfully implemented in some enterprises in Bangkok such as Serm Suk Public Company Ltd., Bank of Thailand and Assumption University, to name but a few (Gullep[33]).

According to this framework, the security model is built upon policies and controls, which are the sum of output of three processes:

- *Business initiatives and processes:* The organization should identify its mission and business objectives and put the security-related issues into that business context to consider.
- *Technology strategy and usage:* The organization should identify the purpose, plan and function of its computing infrastructure in relation to the business context. They should explore with due care the relationship among the adopted technology, business processes and security issues.
- *Vulnerability and risk assessment:* The organization must identify both organizational and technological vulnerabilities. This information is of utmost significance in determining the risk impact on their organization.

PricewaterhouseCoopers Thailand puts much emphasis on enterprise security policy since it is a preventive means of protecting valuable corporate data and business processes. It codifies management's view of security behavior in an easy-to-understand language and then communicates these rules to the groups involved in corporate information (printed or electronic type) management. This audience includes senior executives, business function users and technical and audit staff. Such a framework is ended with three processes that help to prevent known threats and vulnerabilities, detect potential risks and decide and act upon that detection to effectively control the enterprise information system.

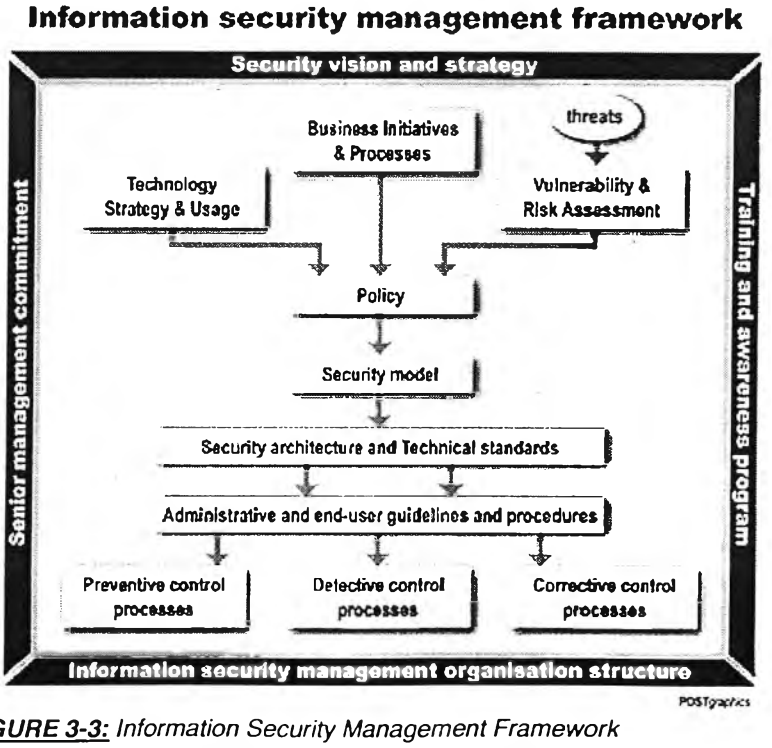


***FIGURE 3-3:*** *Information Security Management Framework*

*Source:* *Eralp Gullep*[33]

Still, the entire framework may stand instably without the firm support of the four fundamental "pillars" as it can be seen from the diagram:

- ***Security vision and strategy*** – Senior management must create an information security mission statement that clearly defines guiding principles and a philosophy about the importance of information in the organization, plus a broad strategy for implementation. The mission statement should be distributed throughout the organization and should highlight that information security is a priority for senior management.

- ***Senior management commitment*** – Achieving a consistent standard for information requires clear vision and direction from senior management. Top executives must be specific about how the program is packaged and communicated to all individuals (internally and externally) with access to the organization's information and systems. Communications should also include direction on how to implement the program.

- ***Information security management organization structure*** – Information security is a management issue that cuts straight to the core of an enterprise. Following a proper organizational assessment, a dedicated information security function should be created to possess and direct security matters. Depending on industry, size and corporate culture, this function could be centralized, decentralized or a mixture of both.

- ***Training and awareness program*** – This final component, stressing security awareness and education, must imbed the importance of information security in an organization's culture. Training must be provided to all staff and should focus on security aspects relevant to each organization's business. It should be persuasive, continually provided and be an integral part of required training.

In a word, the information security management framework underpins with these four pillars would establish a continuous process that includes *assessment (Check)*, *design (Plan)*, *implementation (Do)* and *maintenance (Act)* phases.

I have some remarks on this model:

- As it can be seen from the diagram, the model is built in such a way that the organizational policies drive the computing infrastructure, procedures and testing. This is to ensure that security activities within the organization *'stay on track'*.
- This model also adopts the PDCA and 'top-down' approach.
- The selected controls for the ISMS are quite efficient. They start with administrative and end-users guidelines and end with detective, corrective and preventive processes. Understandably, such mechanism is critical for large, complex organization such as banks, multinational corporations, who are generally customers of PWCs Thailand.

### 3.3 The EWEEK ISMS

EWEEK Labs, a leading website in consulting enterprise information technology, based on their experience as well as surveys from customers, described five steps upon which an organization may follow to ensure a 'secure' computing infrastructure (Peter, Timothy, Cameron and Jim[34]:

- ***Assessment***


***FIGURE 3-4:*** *5-STEPS TO ENTERPRISE SECURITY - Security Step 1: Assessment Adapted from Peter Coffee*[34]

This step is dedicated to risk assessment on both organizational and technological vulnerabilities. As similar as other known risk assessment methods, the primary concerns of enterprises should be threats (and impact) that occur to information (data), technology (hardware and software). However, throughout this section, I do not see anywhere mentioning about evaluation on people – an information asset. As great as risk assessment is concerned, the paper suggested to adopt a specific approach that is

quite familiar to financial institutions. Like OCTAVE[SM], the authors reveal the point of view that a successful risk evaluation requires multidisciplinary perspectives.

➢ ***Prevention***

This step concerns how to structure computing system to minimize the risks of security compromises. The authors tie the success of a security system to two points: (1) intimate knowledge of deployed technical configuration (in terms of hardware and software) and (2) meticulous attention to how information assets might fail upon the occurrence of breaches and incidents.

In this section, I find it interesting with the principle of preventing information security violations and incidents by designing an ISMS for failure. Old truth says "better safe than sorry" or "prevention is better than cure". Thus, organizations can make their most sensitive or irreplaceable information assets be as far away from vulnerabilities as possible.


***FIGURE 3-5:*** *5-STEPS TO ENTERPRISE SECURITY - Security Step 2: Prevention Adapted from Timothy Dyck*[34]

➢ ***Detection***

There is no lack of system for detecting security breaches. Still, there's a huge lack of proper management of those computing facilities. Indeed, according to Cameron, technology is just a piece of complete solution to managing risk and exposure. Therefore, organizations should:

- Routinely assess and review vulnerabilities
- Prioritize assets based on their value and focus detection efforts accordingly
- Know the computing infrastructure and how it behaves under normal circumstances so abnormal activities are noticeable

Rely on people to detect new attacks and make sure they have resources to fully defend their computing infrastructure


***FIGURE 3-6:*** *5-STEPS TO ENTERPRISE SECURITY - Security Step 3: Detection Adapted from Cameron Sturdevant*[34]

- ***Response***

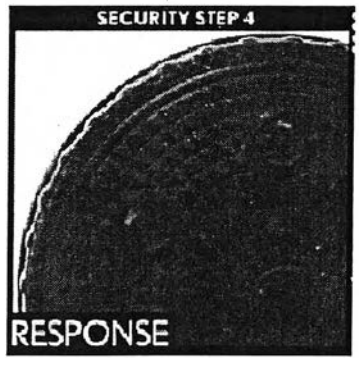


***FIGURE 3-7:*** *5-STEPS TO ENTERPRISE SECURITY - Security Step 4: Response Adapted from Jim Rapoza*[34]

The best management practice to respond to information security breaches as well as incidents is not only stopping them but, more importantly, is learning from them. The simple principle, usually overlooked or underestimated in many enterprises, should become a motto guiding how to protect organization's information system against future incidents.

➢ ***Vigilance***


***FIGURE 3-8:*** *5-STEPS TO ENTERPRISE SECURITY - Security Step 5: Vigilance Adapted from Peter Coffee*[34].

Peter Coffee believed that when driven by top-down commitment from enterprise management, the resulting culture of vigilance will leave fewer vulnerabilities to find, repair and monitor and will drastically reduce the costs that arise during and after the occurrence of breaches and incidents. This can be propelled by consistent attention to the principles below:

- Identify information security involvement of every enterprise department; share information on policies, responsibilities, incidents and lessons learned.
- Evaluate insurance policies with regard to information security threats; resolve any questions of coverage or response.
- Setup positive programs to reinforce good security practices; promulgate specific consequences for negligence or misconduct threatening information assets.
- Integrate security considerations into all project proposals to avoid higher cost
- Design security systems for robustness and economy; reflect organization roles in security arrangements, rather than give information administration undue control of business operations.

Some thoughts of this model come across my mind:

- Like other models, this models is also built up as a continuos process starting with assessment – prevention (Plan) – Detection (Check) – Response (Act) – Vigilance (Do).
- Unlike other models, in this model, each step is developed based on good security practices and principles. The advantage of this approach is realistic, pertinent and ready-to-use. The disadvantage, also the different point from other models, is that it is not systematic and thus, difficult to implement in complex and large information

system. In other words, they just focus on what to do instead of how to do or how to organize the management system.

- Another limitation is that this model does not put emphasis on understanding organizational and business structure. This is very important to detect and prevent organizational vulnerabilities. I would think that this model is quite suitable for small and simple information system.

## 4. AN INSIGHT INTO ISO/IEC 17799:2000 & BS 7799-2:2002

### 4.1 What is ISO/IEC 17799:2000 & BS 7799-2:2002

ISO/IEC 17799:2000 (Guidance Standard) is the standard code of practice for information security management and can be regarded as a comprehensive catalogue of good security practices to follow. It describes 10 security domains containing 36 security control objectives, which are either essential requirements or considered to be fundamental building blocks for information security. These security domains are:

*1. Business Continuity Planning:*

The objectives of this section are to counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters.

*2. System Access Control*

The objectives of this section are: 1) To control access to information 2) To prevent unauthorized access to information systems 3) To ensure the protection of networked services 4) To prevent unauthorized computer access 5) To detect unauthorized activities. 6) To ensure information security when using mobile computing and tele-networking facilities

*3. System Development and Maintenance*

The objectives of this section are: 1) To ensure security is built into operational systems; 2) To prevent loss, modification or misuse of user data in application systems; 3) To protect the confidentiality, authenticity and integrity of information; 4) To ensure IT projects and support activities are conducted in a secure manner; 5) To maintain the security of application system software and data.

*4. Physical and Environmental Security*

The objectives of this section are: To prevent unauthorized access, damage and interference to business premises and information; to prevent loss, damage or compromise of assets and interruption to business activities; to prevent compromise or theft of information and information processing facilities.

*5. Compliance*

The objectives of this section are: 1) To avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements 2) To ensure compliance of systems with organizational security policies and standards 3) To maximize the effectiveness of and to minimize interference to/from the system audit process.

*6. Personnel Security*

The objectives of this section are: To reduce risks of human error, theft, fraud or misuse of facilities; to ensure that users are aware of information security threats and concerns and are equipped to support the corporate security policy in the course of their normal work; to minimize the damage from security incidents and malfunctions and learn from such incidents.

*7. Security Organization*

The objectives of this section are: 1) To manage information security within the Company; 2) To maintain the security of organizational information processing facilities and information assets accessed by third parties. 3) To maintain the security of information when the responsibility for information processing has been outsourced to another organization.

*8. Computer & Network Management*

The objectives of this section are: 1) To ensure the correct and secure operation of information processing facilities; 2) To minimize the risk of systems failures; 3) To protect the integrity of software and information; 4) To maintain the integrity and availability of information processing and communication; 5) To ensure the safeguarding of information in networks and the protection of the supporting infrastructure; 6) To prevent damage to assets and interruptions to business activities; 7) To prevent loss, modification or misuse of information exchanged between organizations.

*9. Asset Classification and Control*

The objectives of this section are to maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection.

*10. Security Policy*

The objectives of this section are to provide management direction and support for information security.

What's worth mentioning here is that *not all of these may be applicable to an organization and additional ones may be required for more security sensitive areas* (ISO Bulletin, 2000). In other words, based on the risk assessment results, an organization must select appropriate control and control objectives to minimize the impact of identified risks.

ISO/IEC 17799 is an internationally recognized Information Security Management Standard. It was first published by the International Organization for Standardization (ISO) in December 2000. Whilst there are other "Guidelines" and "Best Practices", ISO 17999 is *the only standard for Information Security Management*.

BS 7799-2: 2002 (certification standard), released in December 2002, is the specification document against which an organization is measured for compliance and subsequent certification. BS7799 tells organizations how to apply ISO/IEC 17799 and how to design, implement and operate, monitor and review, maintain and improve an ISMS. This standard can be used by internal and external parties including certification bodies to assess an organization's ability to meet its own requirements as well as any customer or regulatory demands.

BS 7799-2 is based on "Plan-Do-Check-Act" approach and is aligned with ISO 9001:2000 and ISO 14001:1996 in order to support consistent and integrated implementation and operation with related management system standards.

### 4.2 A Condensed history

The origin of ISO/IEC 17799 goes back to the days of the UK Department of Trade and Industry's (DTI) Commercial Computer Security Centre (CCSC). Founded in May 1987, the CCSC had two major tasks. The first was to help vendors of IT security products by establishing a set of internationally recognized security evaluation criteria and an associated evaluation and certification scheme. This ultimately gave rise to the information security and the establishment of the UK ISMS Scheme. The second task was to help users by producing a code of good security practice and resulted in a "Users Code of Practice" that was published in 1989. This was further developed by the National Computing Center (NCC) and later a consortium of users, primarily drawn from British Industry, to ensure that the Code was both meaningful and practical from a user's point of view.

The final result was first published as a British Standard's guidance document PD 0003, a code of practice for information security management and following a period of further public consultation recast as British Standard BS 7799: 1995.

A second part BS 7799-2: 1998 was added in February 1998. Following an extensive revision and public consultation period, beginning in November 1997, the first revision of the standard, BS 7799: 1999 was published in April 1999. Part 1 of the standard was proposed as an ISO standard via the "Fast Track" mechanism in October 1999. The international ballot closed in August 2000 and received the required majority voting. In October 2000, eight minor changes to the BS text were approved and the standard was published as ISO/IEC 17799:2000 on 1st December 2000.

Meanwhile "BDD/2" (the BSI/DISC committee responsible for the development of BS 7799), is preparing to upgrade Part 2 in readiness for it to be proposed as an ISO standard.

The birth of BS 7799-2:2002 is ultimately significant. As presented above, ISO 17799 is just a code of practice and additional controls could be added to fit the specific organizational context. But yet, there emerged some problems such as how an assessor could associate a pass or fail verdict; how an assessor would know which safeguards or controls were to apply and which were not. The answer lay in the creation of BS 7799-2:2002, which spells out precisely what an organisation and the assessor need to do in order to ensure a successful certification. Almost by accident, this creation has led some people to conclude that the concept of an ISMS is perhaps far greater important than the

original *Code of Practice*. By the inclusion of a variety of feedback loops, an ISMS allows managers to monitor and control their security systems, thereat minimizing the residual business risk and ensuring that security continues to fulfil the corporate, customer and legal requirements.

### 4.3 Why to develop an ISMS based on ISO 17799:2000 & BS 7799-2:2002

In addition to some benefits identified above, there are also other important properties of different ISMSs. Various systems differ in their approaches to the sphere of information security. Models like TCSEC and Common Criteria presented more technical point of view. These criteria are used as a basis for implementing different software systems. ISO 17799 is a more flexible standard. It proposes setting up different safeguards, but the real attention is put to organizational changes.

Both organizational approach and increasing popularity were arguments, which convinced me to choose this standard. ISO 17799 as a continuation of BS7799 regulation, at the time of this study (2003 - 2004) has actually become a leading information security standard and been widely implemented throughout the world: Canada, US, UK, South Korea, Japan, Hong Kong, India, China, Germany, Australia, New Zealand, Greece and so forth (ISMS Journal 1[17]). Thailand's ICT Ministry Dr.Surapong, in his keynote speech at the World Summit on the Information Society (WSOIS) in Geneva late last year, has revealed the determination of Thai government to study the ISO 17799 implementation in enterprises meanwhile confirming that such a good standard sooner or later will be forced to adopt in state-run organizations as well as academic institutions (Karnjana[5]). Another feature goes from the structure according to which this regulation is prepared. It is very similar to other ISO standards, which potentially allows to perform the same implementation process together with setting up a few standards like production quality ISO 9001, environmental friendly ISO 14001 and ergonomic ISO 18000 series, together with information security process managed according to ISO 17799. Last but not least, it's the selected risk assessment method's compatibility to the BS 7799, whose good information security practices are somewhat adapted in the catalog of practice of the OCTAVE$^{SM}$ approach.

### 4.4 An insight into BS 7799-2:2002 – The structure of ISMS

For the purposes of BS 7799-2:2002, the process used is based on the PDCA model shown in figure below:

| PDCA | Description |
|---|---|
| **Plan** (develop the ISMS) | *Establish a security policy, along with objectives, goals, processes and procedures for managing risk and improving information security, in order to deliver results in keeping with the organization's overall objectives and policies.* |
| **Do** (implement & operate the ISMS) | *Implement and operate the security policy, controls, processes and procedures.* |
| **Check** (monitor & review the ISMS) | *Assess, and where applicable measure, process performance against security policies, objectives and practical experience. Report the results to management for review.* |
| **Act** (maintain and improve the ISMS) | *In order to continually improve the ISMS, carry out corrective and preventative action based on the results of the management review.* |

***TABLE 3-1:*** *PDCA adopted for ISMS.*
***Source:*** *Adapted from BS 7799-2: 2002.*

For this study, in accordance with the scope stated in Chapter 1, I'll thus focus on the *Plan phase – Developing an ISMS.*

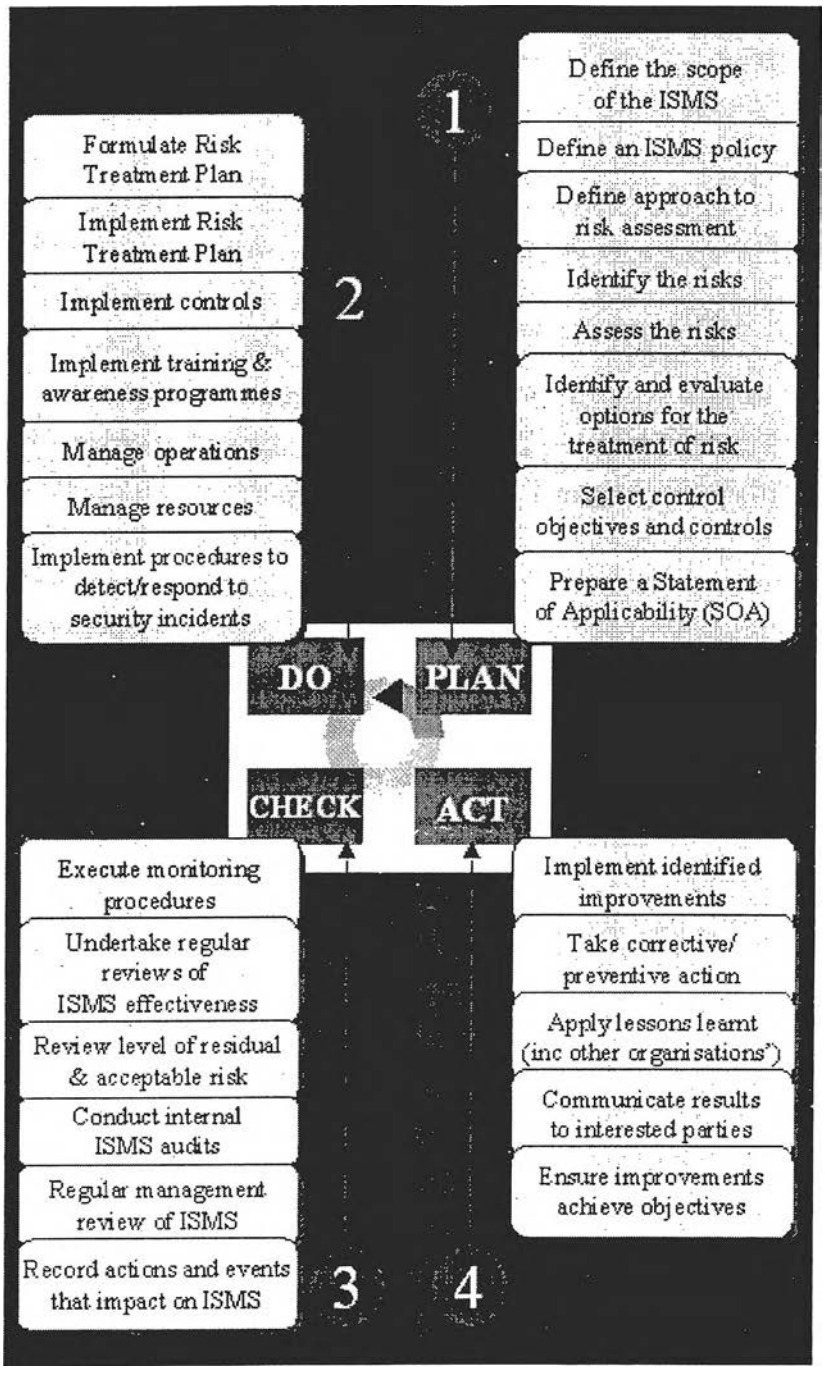


***FIGURE 3-9:*** *PCDA Model suggested by BS 7799-2: 2002.*

***Source:*** *British Standard Institute – URL:http://www.bsi-global.com*[51]

BS 7799-2: 2002 instructs organizations how to establish an efficient ISMS using control objectives described in ISO 17799: 2000. Developing an ISMS requires a six-step process as followed (see Figure 3-10):

***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. An ISMS policy:

- includes a framework for setting its objectives and establish an overall sense of direction and principles for action with regard to information security;
- takes into account business and legal or regulatory requirements and contractual security obligations;
- establishes the strategic organisational and risk management context in which the establishment and maintenance of the ISMS will take place;
- is approved by management.

***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 characteristics of business, 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.

Lim, Kwan and Alvin[19] at Sun Professional Services, Thailand suggested that an organisation may define different ISMSs 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.

### *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.

First, organisation should:

- identify a method of risk assessment that is suited to the ISMS and the identified business information security, legal and regulatory requirements;
- determine criteria for accepting the risks and identify the acceptable levels of risk.

Second, when conducting risk assessment, organisation should:

- identify the assets within the scope of the ISMS and the owners of these assets;
- identify the threats to those assets;
- identify the vulnerabilities that might be exploited by the treats;
- identify the impacts that loses of confidentiality, integrity and availability may have on the assets.

### *4. Risk Management*

After identifying risk, the organisation should assess the business harm resulting from security failure and the likelihood of occurrence. Furthermore, organisation should estimate the levels of risks and determine whether the risk is acceptable or requires treatment using the criteria established.

Different organisations have different risk tolerance levels. 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 should 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 (Details will be intimately presented regarding the processes 7 of the OCTAVE[SM] method in Chapter 4).

***5. Selection of Controls***

Once the risk areas have been identified, analysed and evaluated (in step 3 and 4), *controls should be selected* and implemented to ensure risks are reduced to an acceptable level. Sun Professional Services, Thailand, when consulting for its customers in this step, believed that the key consideration in the selection process is the cost of implementation in relation to the perceived impacts and losses if a security breach or incident occurs. Intangible factors such as loss of reputation should also be taken into account. Simply put, when the risk analysis produces a high impact value of an identified risk, there might be a combination of preventive, corrective and detective control.

When the controls are selected, given the experiences of Sun Professional Services, Thailand, Lim[19] et al. suggested to set up a management forum to ensure that there is a clear direction and visible management support for security initiatives. 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 tasks:

- 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.

The BS 7799 standard describes a number of general controls - whose details can be found in ISO 17799 - which can be considered as good guiding principles for implementing information security:

- 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.

### *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*. Some special cases of risk mitigation plans should also be mentioned.

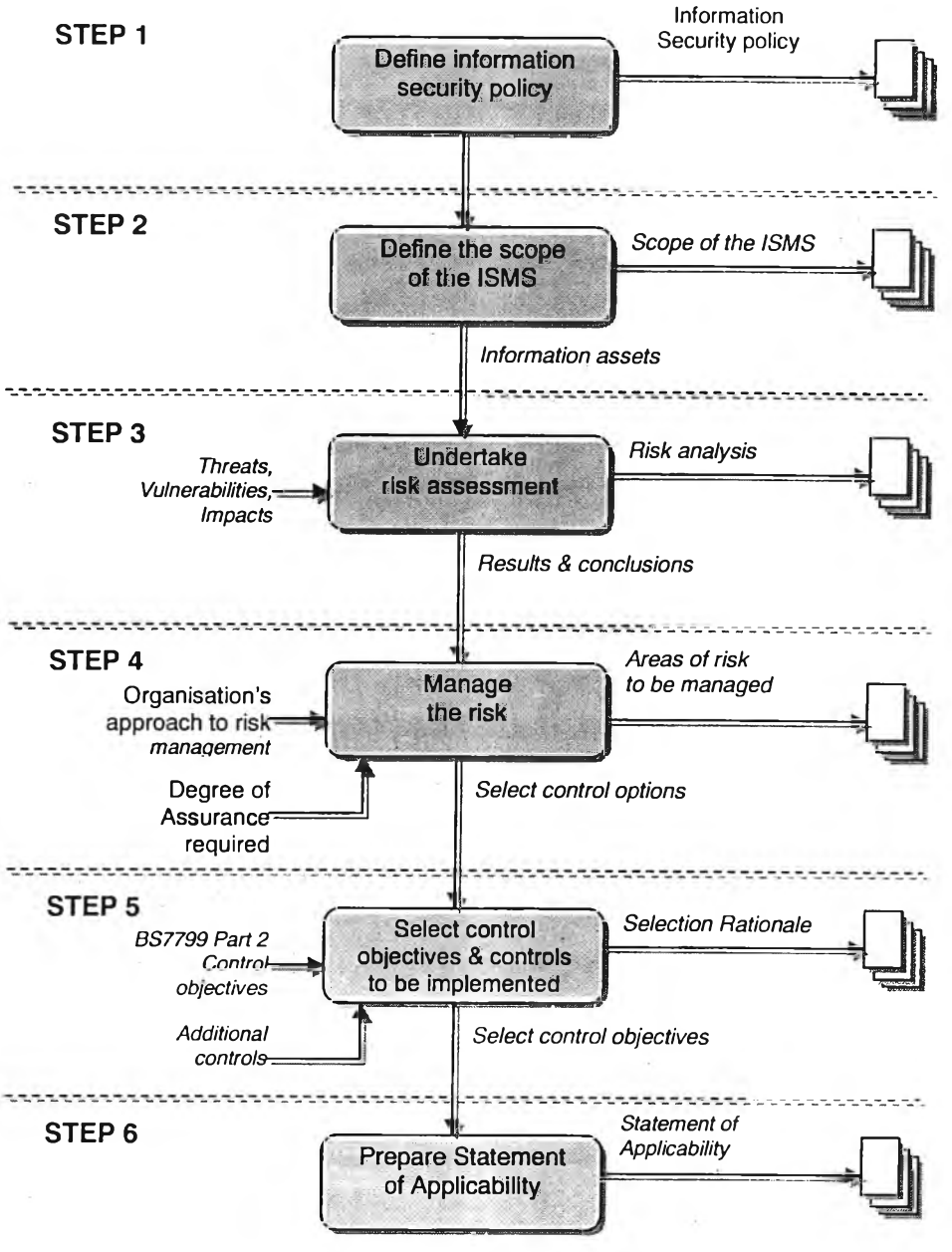


***FIGURE 3-10:*** *Steps in developing ISMS suggested by BS 7799-2: 2002.*

***Source:*** *British Standard Institute – URL:http://www.bsi-global.com*[49]

## 4.5 BENEFITS OF ISMS BASED ON BS 7799/ISO 17799

A major characteristic of BS 7799 / ISO 17799 that is most impressive to me is its *flexibility*. It presents a set of "best security practices" that can be applied to any organization, regardless of size or business sector. In addition, according to CALLIO – a consulting firm in the area of information security and quality system (URL:http://www.callio.com/page.asp?id=85[52]) – BS 7799 / ISO 17799 is *technologically neutral* and does not require the adoption of a specific technical solution. The standard can thus evolve in a constantly changing technological environment.

What's more, BS 7799 / ISO 17799 concerns *public confidence*. Just as ISO 9000 represents a guarantee of quality, this standard constitutes a mark of confidence in an organization's overall security posture. At least, in my opinion, when someone knows that the organization has developed an ISMS, he or she somehow knows that the organization has undertaken a risk assessment and has identified and implemented controls appropriate to the information security needs of the business. Moreover, when organizations can achieve certification, the high profile of ISO standards means that BS 7799 / ISO 17799 is often used to serve managers on the need for information security. Along with advantages described above, various authors have identified other benefits generated by the BS 7799 / ISO 17799 standard:

- Increased mutual confidence between partners. This, in my opinion, is particularly important when organizations wish to interconnect electronically in the global market.
- Potentially lower premiums for computer risk insurance
- Improved privacy practices and compliance with privacy laws
- Better protection of the organization's confidential or sensitive information
- Reduced risk of hacker attacks
- Faster and easier recovery from attack and improved ability to survive disaster
- Compliance with legal and contractual specifications
- A structured and internationally recognized methodology
- Better management of information security on a continuing basis.
- Reduces the need for multiple assessments.
- Reduced need for assessment and inspection of the information security management by the customer or business partner.
- Simplified purchase procedures and decisions.

## 5. CONCLUSION

This chapter was begun with a motto *"Without a deep change...bring little safety"* that serves as an illumination throughout my presentation. Indeed, understanding how to develop an ISMS is an important initial step in a road of establishing, operating and maintaining ISMS. Thanks to doing that way, senior management, with the ISMS in their hands, may confidently transform their information security ideas and intentions into action, whereby enabling policies drive technology, procedures and system. Reality has testified that such a solution is most appropriate.

I would once again lay stress on the issue that many organizations often lose their bearings – Security is about much more than software. As Timothy Dyck, co-author of *'5 STEPS TO ENTERPRISE SECURITY'*, concluded "The tightest software configuration can't protect a server if a determined attacker can wear a maintenance uniform, walk into the server room and sit down at a logged-in console". It stands to this ironical fact that the "awareness and behavior" is a key to success of the whole ISMS mechanism.

Should organizations did not manage their system with prudence and vigilance, the trade-off would be costly.