# Chapter 1 INTRODUCTION

## 1.1 General

Definition

"Public Sector ICT Security can be defined as the process of ensuring business continuity and services provision free from unacceptable risk. It also seek to minimize disruptions or damage by preventing and minimizing security incidents" – Public Sector ICT Security Policy (Appendix A).

Security of information within the government's ICT system is a major concern

The security of information within the Government of Malaysia's Information and Communications Technology (ICT) system is a subject of major concern. Threats such as impersonation, malicious code, misuse of data, easily available penetration tools, powerful analytical techniques contribute in whole or in part to the necessity of providing adequate protection to public sector ICT assets. These threats if left unchecked, will result in painful explaination at the very minimum or untold damage to the country. Apart from incurring financial losses, both in terms of resources and unavailable services, these threats severely jeopardises the confidentiality, integrity and availability of official government information and in the end may be of detriment to the country. The hardest thing to comprehend is that an attack can be easily mounted by anyone from anywhere courtesy of the information superhighway and the misused concept of global instantaneous information sharing. Some examples of common threats are listed in Appendix B.

Need for effective Public Sector ICT Security management

Over the years, government agencies have been religiously collecting vast amount of information. It is in the early 70's that these information have been deposited into digital format and since then, these repositories have unknowingly become exposed because of the invaluable information they keep and now in a format easily manipulated without stringent audit trail. The government realises this and that the government is also aware that there is an urgent need to secure the vast information resource through effective management of the security of ICT systems. In this regard, efforts are being made to ensure Public Sector ICT Security management achieve and maintain a high level of confidentiality, integrity and availability.

A comprehensive approach to ICT Security processes is required

A comprehensive approach is required in planning, developing, operating and maintaining the government's ICT security processes. The ICT security measures need to be incorporated early, in the requirement specification and design of the ICT system, before the implementation stage to ensure a cost-effective and comprehensive system. The main steps include:

*(a)* assessing the current security strengths and vulnerabilities;

*(b)* developing ICT security policies, standards and processes;

*(c)* designing and developing a customised security architecture; and

*(d)* evaluating and selecting the best security system for the organisation.

The ICT security process must cover various aspects in achieving a secure enviroment

The ICT security process must cover all aspects of operation, including mechanisms used by hardware and software systems, networks, databases and other related systems and facilities. The goal is to achieve a secure working environment for employees and other persons working at or visiting the government's facilities as well as to help establish processes to ensure the protection of information.

ICT security processes should mirror management's direction

The ICT security process should mirror the management's direction in relation to:

*(a)* overall organisational policy;

*(b)* organisational roles and responsibilities;

*(c)* personnel;

*(d)* government's asset classification and control;

*(e)* physical security;

*(f)* system access controls;

*(g)* network and computer management;

*(h)* application development and maintenance;

*(i)* business continuity;

*(j)* compliance to standards as well as legal and statutory requirements;

*(k)* classification and protection of information media;

*(l)* employee awareness programmes; and

*(m)* incident reporting and response.

## 1.2 Standards Framework

This handbook provides guidelines on ICT security based on international standards

This handbook provides essential guidelines to government employees on the ICT security process in the public sector. It is based mainly on two standards i.e. the MS ISO/IEC 13335 (Part 1 - 3) and the BS 7799 (Part 1 and 2). It also makes references to the Canadian Handbook on Information Technology Security, German IT Baseline Protection Manual and other related ISO standards.

Various levels of details of standards can be viewed in the model depicted in Figure 1.1. In comparison to other standards and documents of ICT security management particularly to their level of detail, this handbook can be positioned along with the BS 7799, the Canadian MG-9 and the American National Institute of Science and Technology (NIST). This is warranted by the fact that this handbook is jurisdictional and specific to the Malaysian public sector.

Description of model (Figure 1.1)

In the model, the areas and level of details of these standards varies between each standard. Level 1, 2, 3 and 4 represent the Guidelines for the Management of IT Security (GMITS) or ISO/IEC 13335. It indicates the depth of knowledge required to understand the respective level. As an example, a Level 1 document needs no prior knowledge on ICT security management while a Level 2 document needs at least some understanding of the previous level.

Level 1 to level 4 of the model

The model progresses from Level 1 'Concepts and Models' to Level 2 'Managing and Planning IT', Level 3 'Techniques for the Management of IT' before detailing 'Selection of Safeguards, Management Guidance on Network and Guidelines for the Management of Trusted Third Parties' in Level 4.

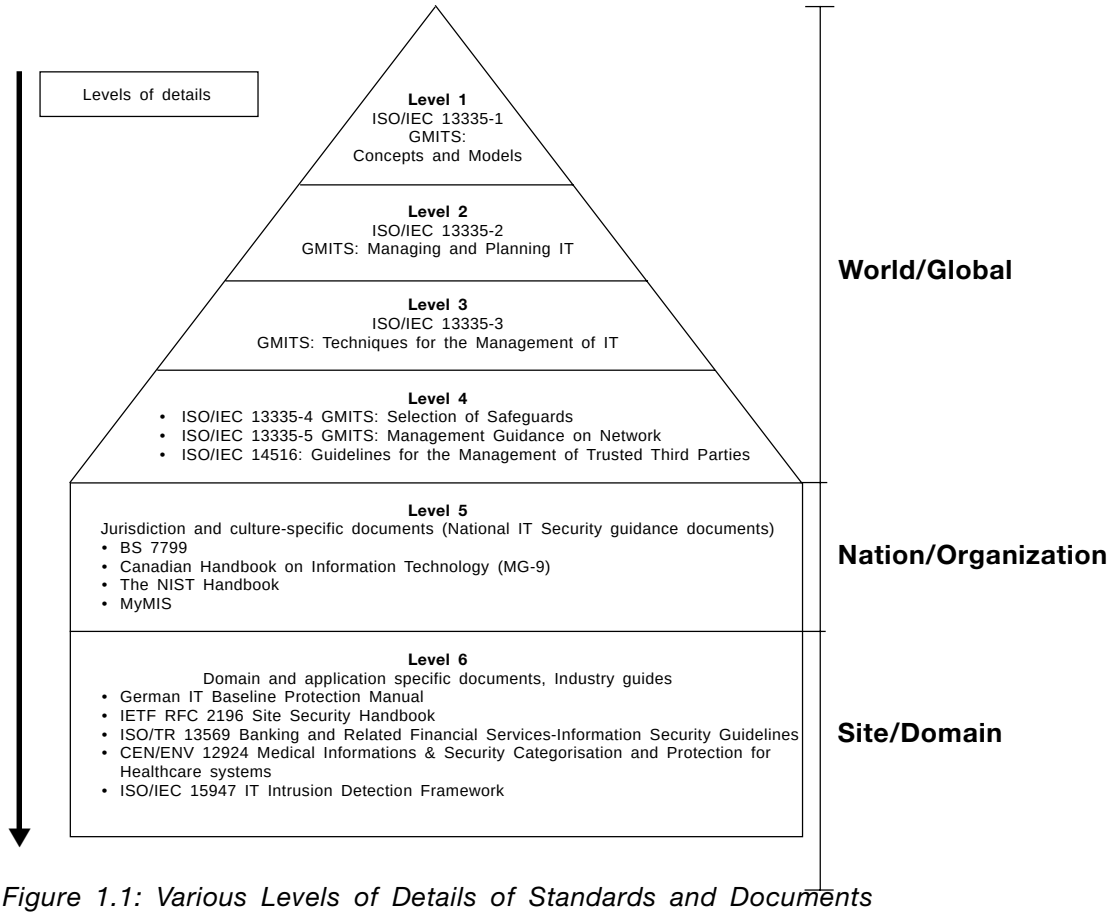


*Figure 1.1: Various Levels of Details of Standards and Documents*

Level 5 of the model

Level 5 represents the three standards referred, i.e. BS 7799, the Canadian Handbook of Information Technology and the NIST. Documents under this group are categorised as jurisdictional and culture-specific. The MyMIS handbook is represented at this level.

Level 6 of the model

The standards within Level 6 are domain and application specific. Examples of such standards are the German IT Baseline Protection document, the IETF RFC 2196 Site Security Handbook, the ISO/TR 13569 on Banking and Related Financial Services, the CEN ENV 12924 on Medical Informatics: Security Categorisation and Protection Healthcare Systems and the ISO/IEC 15947 on IT Intrusion Detection Framework.

## 1.3 Handbook Coverage

This handbook describes safeguards, operational and technical issues and legal implications

This handbook provides the necessary guidelines on ICT security management safeguards to enable implementation of minimal security measures. It discusses elements of management safeguard, common operational and technical issues, and legal implications. The appendices at the end of the handbook may be of use to users with templates on security policies, adherence compliance plan, strategic plan, incident reporting mechanism, checklists and procedures. Its capacity is advisory and where the information contained is superceded (changes in technology, processes, legal requirements, public expectation) the reader is advised to refer to current adopted best practices.

ICT security management safeguards

The ICT security management safeguard identify five (5) major elements that should be considered by all public sector ministries, departments and agencies to protect their ICT systems. These elements are the ICT security policy, ICT security management programme, ICT security risk management, planning and incorporation of ICT security into the ICT systems life cycle and establishing ICT security assurance.

The handbook further explains some fundamental operational components of ICT security that is best recognised by public sector employees.

Technical details of ICT security

Technical security involves the use of safeguards incorporated into computer and communications hardware and software, operations systems or applications software and other related devices. This chapter explains the technical level of ICT security in greater detail.

Legal implications

The last chapter of this handbook briefly explains legal matters with respect to Malaysian law. It highlights Malaysian cyber laws and the various aspects of criminal investigations.

The appendices of this handbook provide some samples of framework, plan, checklist and forms useful in the ICT security management process.

## 1.4 Audience

Main objective is to provide guidance to all government employees

The main objective of this handbook is to provide guidance to employees within government agencies on the essential components of ICT security. It is intended to be the primary reference book used by all government employees in safeguarding the government's ICT assets.

The handbook is for ALL government employees

Various categories of government employees will benefit from the handbook as it covers a wide range of topics. Nevertheless this handbook is also useful to anyone wishing to learn about the application of ICT security.

Organisation of the content of the handbook

The handbook is presented in five (5) chapters that can be divided into three (3) different levels; Essential, Intermediate and Advanced (Figure 1.2). The Essential level, which comprises of Chapter 1, Chapter 2 and Chapter 5, provides fundamental knowledge on ICT security and is suitable for chief executives and managers in the public sector.

The Intermediate i.e. Chapter 3 is intended for general ICT users of the public sector. The description and explanation will provide guidance to users on the basic operational security safeguard to be implemented and maintained by them.

The Advanced stage i.e. Chapter 4 is proposed for the more experienced ICT administrators and managers. The descriptions on technical details of ICT security should provide guidance and direction on steps that need to be taken to ensure the confidentiality, integrity and availability of public sector ICT systems.

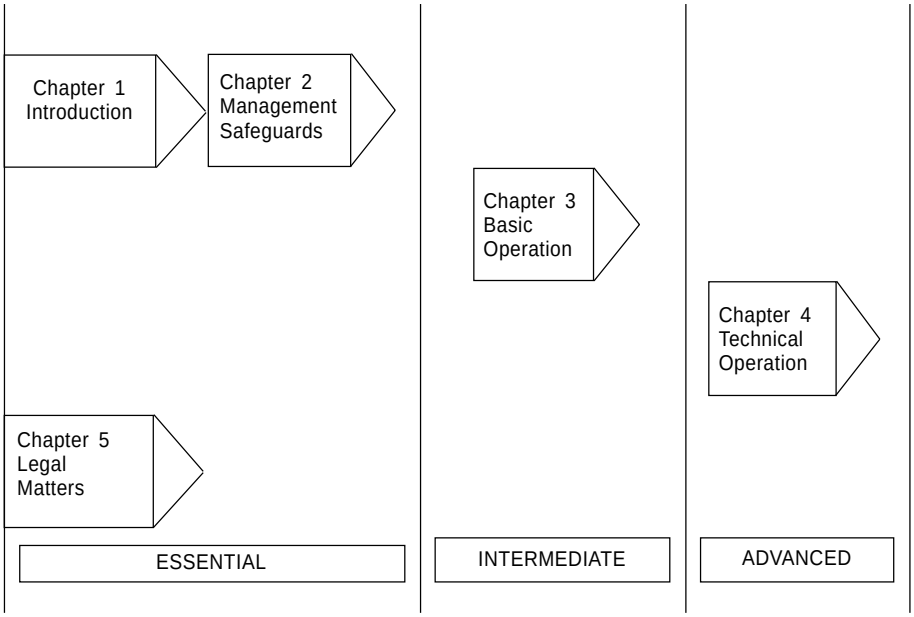


*Figure 1.2: Malaysian Public Sector Management of ICT Security Handbook (MyMIS) Roadmap*