Chapter 3 BASIC OPERATIONS

This chapter discusses fundamental operational components

To implement effective Public Sector ICT Security will require strong commitment from the various level of organisations within the government. ICT security as a programme encompasses a wide spectrum of topics such as technology, people, finance, training, policy, risk management, processes and measures taken in total to safeguard the government's information and communications systems. This chapter explains some fundamental operational components of ICT security that should be imparted to public sector employees. Major areas include information classification, roles and responsibilities, human factors, electronic facilities, document management, storage management, contingencies, incident handling and physical and environmental protection.

3.1 Information Classification

4 classifications of official matters–Rahsia Besar, Rahsia, Sulit and Terhad

Official matters are graded into four classifications i.e. *Rahsia Besar, Rahsia, Sulit* and *Terhad* as stipulated in the *Arahan Keselamatan.*

Information content created digitally follow similar classification. However the protection of digital information requires different handling needs when compared to paper-based information such as encryption, colour coding, labelling, precaution against piggybacking and electronic eavesdropping e.g. tempest (Refer to Table 3.1 and Figure 3.1).

Mode	Conventional	Digital
Media	Hard copy	Digital Information
Handling	As per *Arahan Keselamatan*	Handling protection (As per Figure 3.1)

Table 3.1: Conventional vs. Digital Information Handling

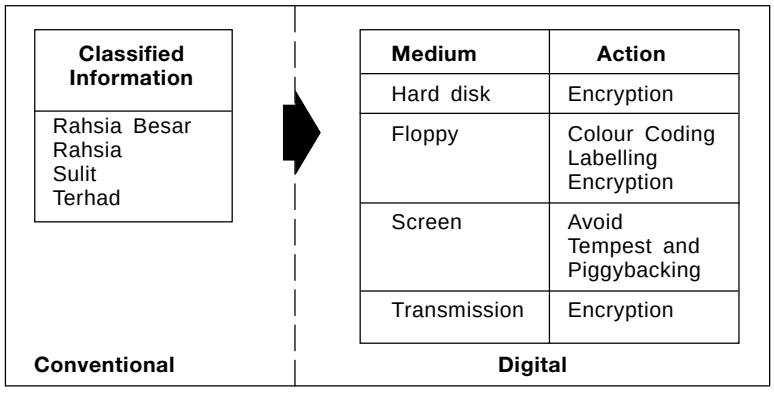


Figure 3.1: Handling Protection

3.2 Roles and Responsibilities

Management involvement is critical to ICT security. Capital expenditures alone cannot accomplish security. Management concern and effort are needed to plan, guide, motivate, and control an effective ICT security programme via the formation of ICT Security forum. A balanced programme, with proper concern for practicality and human values, will enhance the overall effectiveness of the information processing function.

3.2.1 Head of Department

Roles of Head of Department

Heads of Department are owners of Public Sector ICT assets and are accountable for their safe-keeping and protection. Essentially, the Head of Department should realise the importance of Public Sector ICT Security before it is implemented across the entire organisation. The Head of Department needs to be responsible for and supportive of ICT security programmes, promote compliance to standards, procedures and guidelines, and align Public Sector ICT Security requirements to the department's missions and objectives. In addition, the Head of Department should ensure adequate resources, both financial and personnel, are available for the programmes.

The roles and responsibilities of the Head of Department include:

(a) ensure all users including government employees, vendors and contractors understand the need for Public Sector ICT Security policy, standards and guidelines;

(b) ensure all users including government employees, vendors and contractors abide by the Public Sector ICT Security policy, standards and guidelines (necessary action must be taken upon non-compliance of any security measure);

(c) undertake evaluation of risk and security programmes based on the Public Sector ICT Security policy, standards and guidelines;

(d) develop an Adherence Compliance Plan for the purpose of managing risk arising from non-compliance of the Public Sector ICT Security policy, standards and guidelines; and

(e) report to MAMPU and other relevant authorities as required under *Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) - Pekeliling Am Bil. 1/ 2001* dated 4 April 2001 the following:

i. information loss or unauthorised information disclosure or suspected information loss or suspected unauthorised disclosure;

ii. unauthorised or suspected unauthorised usage of ICT system;

iii. loss, stolen or unauthorised disclosure of access control mechanisms or passwords or suspected loss, stolen or unauthorised disclosure of access control mechanisms or passwords;

iv. unusual systems behaviour such as missing files, frequent crashes and misrouted messages; and

v. attempted ICT break-ins and untoward security incidents.

3.2.2 Chief Information Officer

Roles of CIO–Strategic Planner of Public Sector ICT Security

The Chief Information Officer (CIO) is another important ICT resource person. The roles and responsibilities of the CIO include:

(a) support the Head of Department in discharging Public Sector ICT Security responsibility;

(b) transform the responsibilities above into an effective action plan;

(c) incorporate Public Sector ICT Security requirements into existing CIO functions i.e. preparing the IT Strategic Plan. A sample ICT Strategic Plan is as per Appendix G; and

(d) in some cases, the CIO is also the Departmental Security Officer.

3.2.3 Computer Manager

Roles of Computer Manager

The Computer Manager acts as the Operational Head of ICT and is responsible for managing Public Sector ICT Security at site.

The Computer Manager supervises and monitors personnel in the department and acts as the key player in ICT security programme.

The roles and responsibilities of the Computer Manager include:

(a) understand, support, and abide by the Public Sector ICT Security Policy, standards (MS ISO/IEC 13335 part 1-3, MS ISO 17799 part 1) and MyMIS;

(b) ensure that all users understand, support and comply with the Public Sector ICT Security policy, standards and guidelines;

(c) implement ICT security controls consistent with the requirements of the department;

(d) create a positive atmosphere that encourages all users to report on ICT security concerns;

(e) define realistic 'need-to-know' or 'need-to-restrict' criteria to implement and maintain appropriate access control;

(f) review physical security safeguards, in consultation with the Chief Government Security Officer, Public Sector ICT Security officer and others, as required. (Physical security should not only address the central ICT installations only but also back-up facilities and office environments);

(g) ensure that ICT security reviews are performed as and when required either by internal policy, regulations or ICT security concerns. Some examples of circumstances that trigger such a review include:

i. large loss from a security failure;

ii. purchase or upgrade of computer systems or software;

iii. acquisition of new communications services;

iv. introduction of new tools;

v. introduction of new out-sourced processing vendor; and

vi. discovery of a new threat or a change in a threat's direction, scope or intent.

(h) develop, review and align the contingency planning of the department;

(i) review the entry and exit procedures in terms of user accessibility to system resources when employees join or leave the department;

(j) apply security principles in preparing exception requests;

(k) ensure subordinates participate in the ICT security awareness programme;

(l) report any ICT security concerns to the CIO; and

(m) periodic review of access rights and privileges.

3.2.4 ICT Security Officer

The ICT Security Officer (ICTSO) is in charge of the development, implementation and maintenance of the Public Sector ICT Security programmes of the department.

Roles of ICTSO

The roles and responsibilities of the ICTSO include:

(a) manage the overall Public Sector ICT Security programme of the department;

(b) enforce the Public Sector ICT Security policy, standards and guidelines for use throughout the department (these documents should be kept up-to-date, reflect changes in technology, organisation's direction and potential threats);

(c) assist in the development of specific standards or guidelines that meet Public Sector ICT Security policy requirements for specific applications within the department;

(d) review ICT systems against stated security requirements to identify vulnerabilities and risks;

(e) perform Public Sector ICT Security audits based on accepted Public Sector ICT Security policy, standards and guidelines to identify non-compliance;

(f) ensure that when exceptions to policy are required, the risk acceptance process is adhered to and that the exception is reviewed and re-assessed periodically;

(g) suggest measures to bridge the gap in the case of non-compliance;

(h) review audit and examination reports dealing with ICT security issues and ensure that management understands the Public Sector ICT Security issues involved. The ICTSO should be involved in the formulation of management's response to the audit findings and follow-up periodically to ensure that controls and procedures required are implemented within the stipulated time frame;

(i) confirm that the key threats to information assets have been defined and understood by management;

(j) keep up-to-date on current threats, information processing technologies and the most current information protection methods and controls through periodic information up-dates, ICT security seminars and on-the-job training;

(k) prepare and disseminate appropriate warning of potentially serious and imminent threats to the organisation's information assets, e.g. computer virus outbreak;

(l) form a security handling team to handle security incidents;

(m) co-ordinate or assist in the investigation of threats or other attacks on information assets;

(n) assist in the recovery from attacks;

(o) assist in responding to department's client security issues, including letters of assurance and questions on security; and

(p) report any Public Sector ICT Security issues to Departmental Security Officer and CIO.

3.2.5 System Administrators

Roles of System Administrator

The roles and responsibilities of System Administrators include:

(a) maintain the accuracy and completeness of access control privileges based on instructions from the information resource owner and in accordance with applicable Public Sector ICT Security policy, standards and guidelines;

(b) take appropriate action when informed by the respective manager whenever employees terminate, transfer, take leave of absence, or when job responsibilities change;

(c) closely monitor users with high-level privileges and remove privileges immediately when no longer required;

(d) monitor daily access activity to determine unusual activity such as repeated invalid access attempts that may threaten the integrity, confidentiality or availability of the system (these unusual activities, whether intentional or accidental in origin must be brought to the attention of the ICTSO for investigation and resolution);

(e) ensure that every user be identified by a unique identification (user ID) associated only with that user (the process should require that the user identity be authenticated prior to gaining access to the information resource by utilising a properly chosen authentication method);

(f) make periodic reports on access activity to the appropriate information owner; and

(g) ensure that audit trail information is collected, analysed and protected.

The System Administrator's activities should be reviewed by the ICTSO or any authorised independent party on a routine basis.

3.2.6 Help Desk

Roles of Help Desk

The main function of the Help Desk is to provide quick assistance to users on problems and issues related to computer applications and set-up. The Help Desk is the first point of reporting on ICT incidents and to re-route callers to responsible personnel. A sample of Help Desk Reporting Form is attached as in Appendix I.

3.2.7 Users

Responsibilities of users

By definition, a user is anyone who accesses any government ICT asset. A user may be a government employee, members of the administration, contractors, vendors or anyone who accesses or uses government ICT assets.

All users are held responsible for their actions when accessing government ICT assets. This accountability should be made clear to all potential users. In order to ensure compliance, all ICT systems should support facilities that record and detect user actions.

The roles and responsibilities of users include:

(a) understand, support, acknowledge and abide by the Public Sector ICT Security policy, standards and guidelines;

(b) aware of the security implications of their actions;

(c) promptly report to relevant authorities any suspicious behaviour or circumstance that may threaten the integrity of information assets or processing resources; and

(d) keep each department's information confidential.

3.2.8 Vendors, Contractors and External Service Providers

Responsibilities of Vendors, Contractors and External Service Providers

The responsibilities of Vendors, Contractors and External Service Providers include:

(a) understand, support and abide by the Public Sector ICT Security policy, standards and guidelines;

(b) be aware of the security implications of their actions;

(c) promptly report to relevant authorities any suspicious behaviour or circumstance that may threaten the integrity of information assets or processing resources; and

(d) keep the government's information confidential.

3.3 Human Factors

Employees are important assets

For any department, the employees are its most important assets. Through proper planning of acculturation, employees can and do contribute successfully to achieving the mission and vision of the department.

Employees play crucial roles in supporting departmental security ICT programmes. Armed with proper training, most employees can be depended upon to identify anomalies and deviations from good security practices, which can then be the basis for remedial actions. It is also useful to note of cases where employees take advantage of vulnerabilities resulting in theft, information exposure or wrongful communication. Employees also commit mistakes whether intentional or otherwise that may later lead to security breaches.

Statistics also indicate that employees perpetrate computer crime in lieu of their intimate knowledge on internal systems.

Mobilising human resources

To mitigate the risks mentioned above, government department should consider developing suitable approaches in identifying vulnerabilities that could be taken advantaged off by employees. A good case in point is the ICT hierarchy where certain positions become sensitive due to its association with powerful privileges. In such case, all personnel earmarked to such positions should be thoroughly vetted. It is also good practice for management to "know their employees" so that such intangible factors such as attitudes and inclinations may be known. Some of the controls listed below represent safeguard in human factors.

3.3.1 Personnel Security

Reducing security risk from errors

Personnel security encompasses activities aimed at minimising security risk caused or originating from employees resulting from errors and or oversight.

Safeguards include:

3.3.1.1 Confidentiality Agreement

Confidentiality declarations and agreements

Employees that are privy to sensitive information will be required to sign a non-disclosure agreement. (A good example is as per *LAMPIRAN 'D' of Arahan Keselamatan*).

The original copy of the duly signed agreement should be retained for safekeeping and future reference.

3.3.1.2 Personnel Screening

Personnel screening should be addressed at the recruitment stage

Personnel screening calls for the vetting of government personnel and as practiced, implemented at the recruitment stage. There may also be instances where the employee is subjected to detail vetting due to scope enlargement or promotion.

All matters pertaining to personnel screening should be referred to the Office of the Chief Government Security Officer.

No automatic right of access

No automatic right of access will be granted to individuals regardless of their security vetting. In all instances of information exposure, the need-to-know principle must prevail.

3.3.2 Awareness

Head of Department should establish awareness programme

Employees should inculcate good ICT Security practices. This could be achieved by establishing an ICT communications and awareness programme to inform employees of the importance and seriousness of ICT security. In order to further minimise risk, a 'clear desk' policy should be implemented.

Clear desk can be defined as not leaving sensitive materials on desk when left unattended.

3.3.3 Problem Employees

Assist problem employees

Employees with personal problems that could result in possible ICT security exposures should be given assistance.

3.3.4 Former Employees

Surrender all properties

Employees who leave the organisation must surrender all organisational assets under the employee's supervision immediately.

3.4 Electronic Facilities

3.4.1 Telecommuting

Telecommuting and remote accesss

The current technology has enabled users to initiate work from anywhere and at the same time remain connected to the office. This facility or telecommuting allows mobility and users access into the office ICT system.

The following should be considered in addressing security issues for telecommuters:

(a) equipment borrowed must be with a prior approval from head of department. The employee is accountable for the safety of the borrowed equipment;

(b) allow an employee to telecommute only after consideration is given to the employee's interpersonal skills, communication skills, and ability to work in an unsupervised environment;

(c) establish and distribute a clear written procedure on telecommuting; and

(d) require any employee who wishes to telecommute to execute a written agreement which addresses the following issues:

i. equipment to be used;

ii. phone lines;

iii. maintenance;

iv. costs and reimbursements;

v. supervision;

vi. liability for personal injury, fire, etc.; and

vii. physical and logical security to include protection of equipment, information transmitted or stored, hardcopy, back-up of information, disposal of hardcopy and diskettes, and protection of networks.

3.4.2 Voice, Telephone and Related Equipment

Telephones, PBX, facsimile and Voice Mailboxes are the penetration points

Telephones, Private Branch Exchange (PBX), facsimile machines and Voice Mailbox systems are frequent penetration point and are also open to abuse. The most common security hole is the use of insecure maintenance modes/interfaces.

PBX attacks often result in attackers making long distance telephone calls, perhaps completely unnoticed until bills suddenly increase. Often maintenance modes are badly protected or special features are enabled for outside access when they should not be.

In general, they are subjected to the following:

(a) where possible, maintenance interfaces should not be accessible externally;

(b) maintenance passwords should never be left at their default settings; and

(c) all devices with external interfaces should be configured such that they are not easily open to abuse.

Voice mail systems are subject to threats and exposures

Organisations utilising voice mail systems are indeed subject to a variety of potential threats and exposures. This includes disclosures of messages, liability for long distance telephone charges and possible loss of service due to unauthorised access to voice mail systems. It is completely necessary to get the ICTSO involved in the implementation and review of appropriate security controls offered by vendors. This will eliminate or reduce possible security exposures.

The following subsections illustrate control mechanisms that should be used to secure voice and related information.

3.4.2.1 Access to Voice Mail System

Control access to voicemail service

The integrity of information residing in voicemail can be preserved and the expenses and liability of unauthorised use of voicemail services limited by controlling access to voicemail service with physical controls and with logical access controls.

3.4.2.2 Private Branch Exchange

Control access to PBX

A PBX is an internal switch for attached telephone units within an organisation. The switch usually supports connections to outside telephone lines and may support electronic switching of information to the attached computer devices.

PBX systems can be protected against unauthorised outside calls as well as unauthorised disclosure, modification or destruction of information via its electronic components by:

(a) maintaining close liaison with the PBX supplier and network service providers concerning emerging fraud and other problems;

(b) providing physical access controls that restrict access to the PBX by authorised individuals;

(c) protecting any maintenance or administrative ports that are accessible via remote dial-up, with passwords, and either require secure call-back or challenge/response procedures;

(d) producing an audit trail of all administrative and maintenance access;

(e) changing all default password settings immediately upon installation of a PBX;

(f) documenting all changes following approved change control procedures. It may be necessary to use call accounting software;

(g) preventing all access to local ‘hot numbers’ or other expensive services; and

(h) following least privilege on setting facilities for particular extensions, e.g. deny international access unless explicitly authorised.

3.4.2.3 Spoken Word

Control access to spoken word

It is completely necessary to educate employees to the sensitivity of information being discussed regardless of circumstances by advising employees periodically and to be aware of who is present during conversations involving official

secret information. Whenever official secret information is to be discussed, an announcement to that effect should be made, unless it is clear that persons who are party to the conversation or meeting are aware of the sensitivity of the information.

3.4.2.4 Intercept

Interception during transmission

Communication can be intercepted. The prevailing technology has made the process simpler and can be mounted within a short time span. Therefore, it is advisable that organisations protect against interception of official secret information during telephone transmission by:

Encrypt communications to prevent interception

(a) encrypting telephone calls in which official secret information will be discussed; and

(b) prohibiting use of unencrypted cellular or cordless telephones for transmission of official secret information, except in emergencies.

3.4.2.5 Casual Viewing

Minimise casual viewing

In order to minimise the disclosure of information on computer terminal screens through casual viewing:

(a) position computer displays away from public view;

(b) implement password screen saver; and

(c) apply the need-to-know principle.

3.4.2.6 Output Distribution Schemes

Destroy unused hard copy

There is a trend to replace paper documents such as reports and statements with on-line access to computer systems.

In order to protect against unauthorised modification of official secret information reports, destroy unused hard copies completely.

3.4.2.7 Destruction

Dispose unused official secret information

All unused official secret information should be disposed of securely and completely.

3.4.2.8 Clock Synchronization

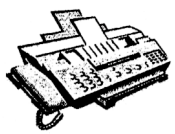
Set the computer clock correctly

It is important to ensure correct setting of computer clocks. This will become apparent when determining sequence of events and audit trail.

3.4.3 Facsimile

Control access to the facsimile

Facsimile is the transmission of paper-based text, graphs, drawings, plans and other written images electronically via telephone lines.



Since the fascimile allows for the transmission, receipt and hence the dissemination of information, suitable controls should be implemented to govern its use:

(a) all facsimile machines should be installed in rooms that are visible and be easily monitored;

(b) allow personnel with granted access privileges to pick up messages; and

(c) the transmission of official secret information when done through facsimile should only be done using secured facsimile machines approved by the government.

3.4.3.1 Modification

Employ separate verification

To preserve the authenticity of the source documents, employ separate verification means such as prearranged telephone calls to confirm transmission and receipt.

3.4.3.2 Transmission Acknowledgement

Use of transmission acknowledgement

In preventing false claims of message receipt or denial of message delivery, apply transmission acknowledgement controls such as transmission acknowledgement and telephone confirmation.

3.4.3.3 Misdirection of Messages

Check identity of the receiver

To avoid misdirection of official secret information and hence disclosure, re-check the receipient number and identifying prior to sending.

Attach appropriate warning coversheets to assist in the retrieval of facsimile documents at the receiving end and also to assist in detecting misdirected facsimile messages.

3.4.3.4 Disclosure

Encrypt facsimile for official secret transmission and prevent unauthorised viewing

All transmission of official secret information must be encrypted using approved encryption. Similarly, to prevent unauthorized disclosure such as unauthorised viewing of unattended facsimile equipment, employ the following measures:

(a) locate facsimile machines and image processing terminals within areas under physical access control;

(b) prohibit facsimile transmissions carrying official secret information, unless it is determined by independent means that a properly authorised person is present at the receiving terminal. One method of doing this is to send the cover sheet only, wait for telephonic acknowledgement of its receipt, then resend the entire package using the redial button on the facsimile device; and

(c) classify and label documents in image systems or those received via facsimile using the same criteria used for paper documents. Documents should bear markings appropriate to their classification.

Use secured cellular facsimile for transmission of official information

The use of secured cellular facsimile raises potential disclosure concerns. In protecting against disclosure of facsimile sent via secured cellular connections, prohibit transmission of official secret information through cellular facsimile unless encryption is in use.

3.4.3.5 Unsolicited Messages

Disclose facsimile number on a need-to know basis

Restrict the disclosure of encrypted facsimile machine numbers on a need-to-know basis. This will help reduce unsolicited messages and minimise service loss caused by junk facsimile.

3.4.3.6 Retention of Documents

Keep a copy of information on secured media

In order to prevent the loss and modification of necessary business records (including facsimile on thermal paper and stored image where source documents are not available), store image on secured media. It should then be stored, or a separate copy made, kept off-line and retained.

3.5 Electronic Mail

E-mail – an electronic communication over computer system

Electronic mail (e-mail) is the electronic communication over computer systems that enable two or more parties to send, receive, store and forward communications over public and private networks. Multiple message types may be transmitted such as text, digitised voice and images.

Within the public sector, there are two (2) categories of e-mail:

Categories of e-mail

(a) Official E-mail

Official e-mail is under the supervision and control of the Malaysian Government. Contents of the official e-mail can be categorised as:

i. non-classified official e-mail for handling unclassified official information by following the procedure issued from the respective ministry, department and agency; and

ii. classified official e-mail for handling classified official information that must be protected in the interest of the government.

(b) Personal E-mail

Personal e-mail is not under the supervision and control of the Malaysian Government. Personal e-mail cannot be used for official matters.

3.5.1 Authorised Users

Use logical and physical access control

Authorised access to e-mail facilities should be controlled. Employ both logical and physical access controls to ensure authorised access.

3.5.2 Physical Protection

E-mail physical protection

All ICT assets when taken together provide e-mail services should be protected from unauthorized users and to ensure service provision. Protective measures include:

(a) limit physical access to employees and or maintenance crew who are necessary for the operation of the system; and

(b) house ICT assets supplying e-mail services away from public areas.

3.5.3 Logical Protection

E-mail logical protection

In order to prevent unauthorised modification, disclosure or destruction of information residing in computer systems, logical access control for all computers must be applied.

3.5.4 Integrity of Content

E-mail integrity

E-mails can be the beginning of a series of actions to be taken. Before actions are initiated, it may be necessary to determine the integrity of its content. This is accomplished by:

(a) verifying the authenticity of source through telephone, facsimile or reply e-mail, or

(b) use of approved digital signature.

3.5.5 Disclosure

Protect against disclosure via e-mail systems

E-mails carrying official secret information must be protected against unauthorised disclosure via:

(a) label information that is classified as per *Arahan Keselamatan*;

(b) prohibit the transmission of official secret information over e-mail, unless encrypted using technique approved by government;

(c) all classified information must be kept encrypted; and

(d) forwarding of official secret information must be with prior permission from the document originator.

Minimising misdelivery

In order to minimise misdelivery:

(a) to avoid misdirection of official secret information and hence disclosure, re-check the receipient e-mail address and identify prior to encryption and sending. Attach appropriate warning messages to assist the receipient at the receiving end.

(b) receiver must acknowledge receipt of information;

(c) for bounced mail, prohibit retransmission until the cause is identified; and

(d) use trusted public network providers.

3.5.6 Message Retention

Messages should be stored and easily retrieved

Official e-mails are public records and should be treated as such. As with current paper based documents, e-mails should be stored into appropriate folders for easy retrieval and reference. There may also be cases where e-mails are stored for business and regulatory reasons. To assist in proper management of e-mails:

(a) create a record retention;

(b) purge unread and unsaved messages after a specified time; and

(c) handle all electronic records of archival value, in compliance with *Akta Arkib Negara Malaysia 44/1966*.

Public key certificates or authentication keys used during processing should be archived together with messages to ensure proper reconstruction and authentication.

3.5.7 Message Reception

Facility to confirm message status

Most e-mails of good repute offer function to allow users to manage their e-mail messages. Users may find it useful to use automated status checking facility to ensure all messages are received and read.

3.5.8 Protection against Malicious Code

Message should be free from malicous code

Messages sent and received via the mail system should be cleaned from malicious code by:

(a) scanning all files and attachment;

(b) not opening any attachment files from unknown or suspicious senders; and

(c) using the latest and up-dated anti-virus software.

3.5.9 Security Labelling

Message should be labelled as per *Arahan Keselamatan*

E-mails and its attachment containing official secret information must be given security labels as per *Arahan Keselamatan*.

3.6 Mass Storage Media

Storage media for vast quantity of information stored

Microfilm, microfiche, compact disk (CD), diskette, tape, cartridge and other mass storage media pose special concerns because of the vast quantity of information they can store, and the relative inability to readily ascertain their contents. Hence special precautionary measures have to be taken in order to ensure that the confidentiality, integrity and availability of the information contained within the storage media are intact and secured.

The following controls should be put in place:

3.6.1 Protection of Information in Storage Media

Information protection in storage media

In order to provide greater security of official secret information stored on magnetic media, the following steps have to be taken:

(a) encrypt all official secret information upon storage;

(b) physically protect the storage media from unauthorised access or removal;

(c) maintain a formal record of the authorised recipients of information;

(d) provide access restrictions and control to back-up files/copies activities; and

(e) index the media for identity with instructions on special handling, if required.

3.6.2 Environmental Considerations

Media are sensitive to environmental conditions. Storage site should be adequately provided with fire and environmental control

Mass storage media may have different sensitivities to environmental factors, and therefore require different measures of environmental protection. Magnetic media, such as diskettes or magnetic tapes are sensitive to temperature, liquids, magnetism, heat, smoke and dust.

In order to prevent destruction of information due to environmental problems, the storage sites should be provided with adequate fire protection and environmental control in accordance to the media's manufacturers' specifications.

3.6.3 Disposal of Storage Media

Disposal of unused storage media

Storage media should be disposed of securely and completely when it is no longer required, to prevent improper disclosure.

Formal procedures should be taken to minimise the risk of sensitive information leaking through careless disposal. The recommended procedures are as follows:

(a) media containing classified information should be disposed by shredding, grinding (granularising) or burning;

(b) use of the degaussing process as a recommended method to magnetically erase data from magnetic ICT media. Two types of degausser exist: strong permanent magnets and electric degausser; and

(c) disposal of sensitive items should be logged in order to maintain an audit trail.

When accumulating media for disposal, consideration should be given to the aggregation effect, which may cause a large quantity of unclassified information to become more sensitive.

3.6.4 Non-Current Storage Media

Non-current storage media should be transferred to the new media before disposal

In order to ensure availability of information stored on non-current storage media, the information should first be transferred to the new current storage media before deletion or disposal. However, should the organisation continue to utilise non-current storage media, care must be taken to retain all the necessary peripheral equipment such as its drivers, and ensure its working order.

3.6.5 Intellectual Property Rights

Compliance to Malaysian Copyright (Amendment) Act, 1997

Commercial software products are usually supplied under a license agreement that limits the use of the products to specified machines and may limit copying to the creation of back-up copies only. In preventing infringement of intellectual copyrights due to unauthorised copying of software on mass storage media, compliance to the Malaysian Copyright (Amendment)Act, 1997 must be ensured at all times.

3.6.6 Vendors, Contractors, External Service Providers, Third Party Access

Control access by Vendors, Contractors, External Service Providers and Third Party

Information is an asset and should be protected. Third party access to government documents for referral to perform a specific task should be controlled. For example, a new ICT system installation may require referral to blue prints, plans, migration forms, approvals etc.

Access to information including assets, facilities, and documents should be evaluated. This is to ensure acceptable risk by allowing third party access. The more sensitive the information is, the higher approval authority is required.

In the government environment, the authority level is specified clearly for the official secret information as described earlier. Government officers must strictly adhere to guidelines issued such as *Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Kerajaan Bil. 03 Tahun 2000* before allowing third party access.

3.7 Business Resumption

Business Resumption Plan for the Public Sector

Government ICT installations store huge amounts of information. This information is varied in nature, from information for daily functions to information for producing trends and analysis. The monetary value attached is of sizable amount. The content value of the information is immeasurable and in some instances may be difficult or if not impossible to reconstruct. Therefore all ICT installations should have some form of business resumption plan.

The plan should be geared towards achieving continued business operation. In instances where it becomes impossible to do so then the plan should target for continuous functioning of core operations. The activities involved in the business resumption are as follows:

(a) risk analysis;

(b) disaster recovery/contingency plan;

(c) regulatory compliance; and

(d) insurance.

3.7.1 Risk Analysis

Organisation Risk Analysis Model

The organisation's risk analysis involves analysis of background of risk, business impact, threat and vulnerability, protection, compliance, follow-up and feedback. These major components are essential for the analysis of risk. The organisation risk analysis model is illustrated in figure 3.2: Risk Analysis Model.

3.7.2 Disaster Recovery/Contingency Plan

Disaster Recovery/ Contingency Plan to ensure continuous functioning of critical business

The Disaster Recovery/Contingency Plan (DRP) forms an important part of the Public Sector ICT Security programme. As mentioned earlier, its objective should be to ensure continuous functioning of critical business in the event of disruption. The plan should outline roles and responsibilities in the event of a disaster or conditions that prevent continuous business functions. In addition, the disaster recovery plan should ensure that information and information processing facilities are restored as soon as possible after an interruption. Please refer to Appendix L of a Sample of Disaster Recovery and Contingency Planning.

The disaster recovery/contingency plan should include at least the following:

(a) a list of core activities considered critical preferably with priority rankings;

(b) a list of personnel available both internal and from the vendor together with their contact numbers (facsimile, phone and e-mail). Apart from that there should also be a second list to replace personnel who may be unable to attend to the incident;

(c) a detailed list of information that requires back-up and the exact location of storage as well as instructions on how to restore such information and related facilities;

(d) identification of alternative processing resources and locations available to replace crippled resources; and

(e) agreements with service providers for priority resumption of services where possible.

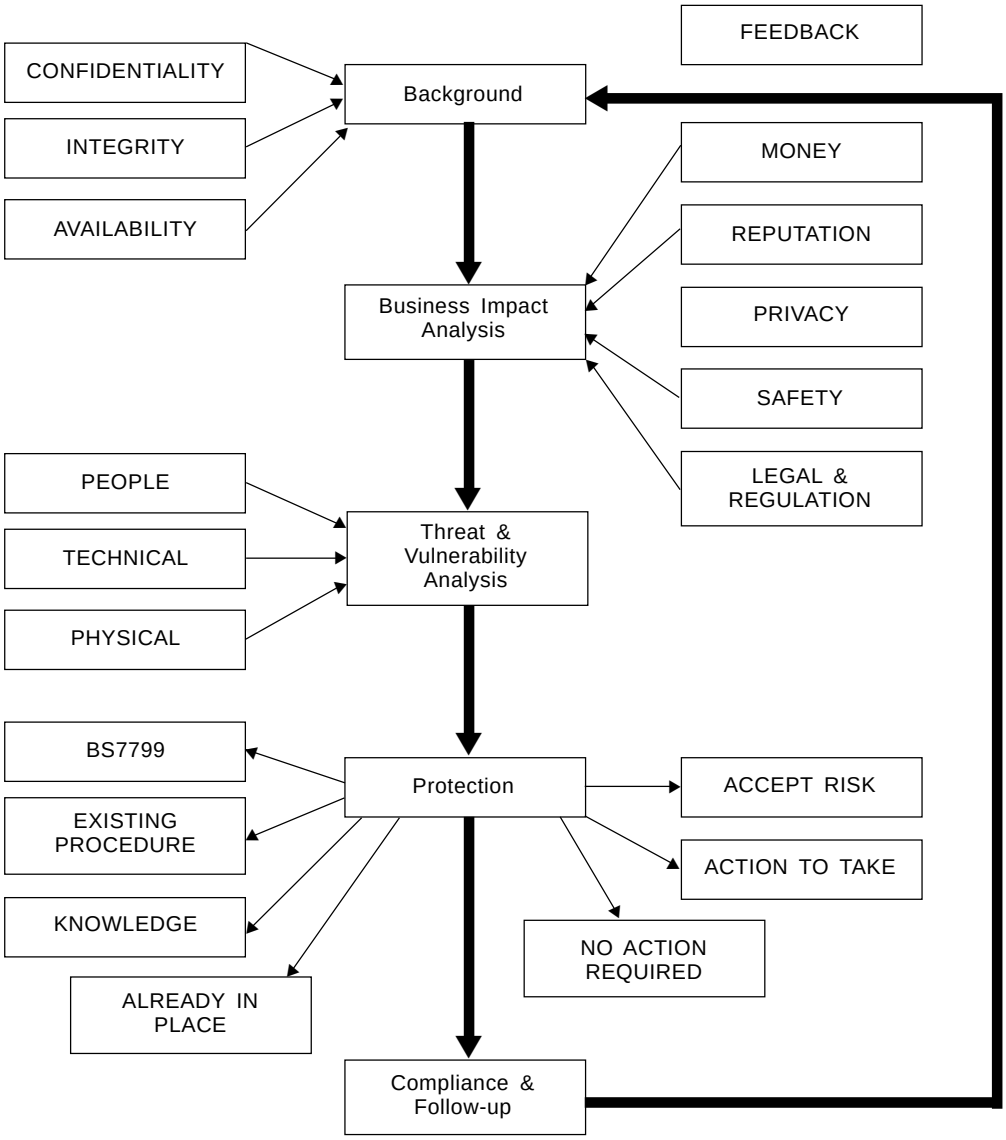


Figure 3.2: Risk Analysis Model

Source : NISER

Test the Disaster Recovery/Contingency Plan at least once a year

In order to ensure smooth transition, the disaster recovery/contingency plan should be tested yearly if not more. The testing of the plan has the added advantage of keeping the personnel trained and skills fine-tuned as well as identifying likely operational problems. The plan should also be evaluated periodically to ascertain that it is still appropriate and meeting the purpose it was intended for.

In ensuring against business interruption, recommended actions under the disaster recovery/contingency plan are:

(a) include telephone and voice mail service continuation to ensure the continued availability of voice mail and telephone services;

(b) include image systems and facsimile capability to ensure against business interruption due to loss of image systems;

(c) include e-mail service continuation to ensure business continuation in case of loss of e-mail services;

(d) continued availability of information stored on microfilm, microfiche, or other mass storage media should be ensured through the following procedures:

i. include mass storage media, as part of the contingency and disaster recovery plan;

ii. provide for back-up of all important files, critical business data, important programmes and documentation to enable business resumption of core processes;

iii. the frequency of back-up should be in-line with the importance of the information and the business resumption plan;

iv. back-up should be securely stored, and the recovery procedure checked and tested regularly for reliability; and

v. access to back-up should be strictly controlled.

(e) include paper documents and media storage to ensure that vital business records are not lost through destruction or loss of paper documents;

(f) protect government operations from disastrous effects of fire and/or water:

i. a business continuity or resumption plan should be in place and fully tested; and

ii. back-ups of all important information, services and resources should be available.

(g) protect buildings containing key equipment and the key equipment against the effects of lightning; and

(h) protect against natural disasters by avoiding disaster prone areas.

3.8 Public Sector ICT Security Incident Handling

A security incident affects confidentiality, integrity, availability and accountability

A security incident is an incident that affects either directly or indirectly, the confidentiality, integrity and availability of the ICT system.

Incident handling is similar to first-aid. Once an organisation suffers a disruption and is given an ‘incident handling’, where its ICT infrastructure needs to undergo a proper overall security diagnosis.

3.8.1 Causes of Security Incidents

Many causes of security handling

There are many causes of security incidents either:-

(a) intentional such as virus, deliberate attacks, sabotage etc; and

(b) unintentional such as programme errors, technical deficiencies, lapses in responsibility etc.

More common these days are events caused by deliberate technical activities internally or externally launched by hackers.

3.8.2 Handling Security Incidents

Security incident handling procedure

Following a security incident, the computer manager or ICTSO will be required to take necessary measures to minimise the resulting damage or those which may be required by law:

(a) order the security incident handling team of the organisation (if it has been set up) to look into the matter immediately;

(b) report the incident to Government Computer Emergency Response Team (GCERT), MAMPU and seek further advice as per requirements of the *Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) - Pekeliling Am Bil 1 Tahun 2001*; and/or

(c) report to respective agencies such as the police within 24 hours. [Refer to Appendix H for further advice]

3.8.3 Developing Security Incident Handling Capability

Characteristics of security incident handling

Characteristics of successful incident handling capability:

(a) Good Understanding of the Domain.

'Domain' means all relevant programmes and users affected by the anticipated incident. In a networked environment, an incident handling capability may define that its constituency to cover only a particular single Local Area Network (LAN) environment which is considered to be critical and cost justifiable. Certainly, if the domain coverage is as wide as the entire organisation, then the 'understanding' to be developed needs to cover the entire organisation;

(b) High-level Awareness

Users need to be aware of the importance of incidents handling, and to trust its capability. High-level awareness can be achieved through good and effective security training programmes. Users can play a significant role in recognising threats, reporting and providing preliminary emergency response;

(c) Centralised Reporting and Communications

All suspected security incidences must be reported to the ICTSO immediately. The ICTSO should then report to the CIO. Based on the gravity of the incident, the ICTSO may proceed to seek technical advice from MAMPU; and

(d) Competent Technical Support

In selecting members of the incident handling team, the following should be considered:

i. expertise in Public Sector ICT Security;

ii. ability to work as a team;

iii. effective communication between all parties from unskilled users to managers to law enforcement officers (police);

iv. reachable on call 24 hours X 7 days;

v. available on short notice; and

vi. ability to liaise with other organisations effectively.

Benefits of security incident handling capability

Benefits of an internal ICT Security incident handling capability;

(a) Limit Damage from an Incident

Such a capability enables users to report incidents promptly and the organisation to quickly provide appropriate response and assistance. This includes establishing contacts with supportive sources (technical, managerial, legal and security) to help in containing and recovering from the incident;

(b) Prevent Future Recurrence

When an incident occurs, the problem can be studied so that more effective safeguards can be implemented. Additionally, through outside contacts, early warnings can be provided and this tends to stop the problem from spreading;

(c) Identify Other Threats and Vulnerabilities

An incident handling can greatly facilitate analysis of future threats by exploiting information logged due to the incident. This helps to identify potential recurring problems;

(d) Enhancing Internal Communications and Organisation Preparedness

A crisis will encourage communication between members of the organisation to respond to any type of future incidents (not just security-related incident). It will also serve to maintain good relation between the organisation and other relevant agencies; and

(e) Enhancing Security Training and Awareness Programme

Based on incidents reported, training personnel will have a better understanding of user's knowledge and awareness of security issues. Citing actual events in training, results in better response.

Liaison with other organisations

Since computers are networked, incident occurring in one organisation may affect other organisations. Thus, there is a need to liaise with other teams in other organisations, perhaps even pooling knowledge via an e-mail group.

Support from technical team

A good technical team needs to be identified and trained to handle security incidents successfully. Otherwise the task has to be outsourced.

Immediate team action is facilitated by the establishment of a centralised reporting mechanism

Rapid team action is facilitated by the establishment of a centralised reporting mechanism. When the incident involves an organisation that handles national security, the means of communication must also be secure, for example using approved encryption for voice, facsimile or e-mail.

3.8.4 Issues to Consider When Setting an Incident Handling Capability

There are several issues that should be considered in setting an incident handling capability. These are:

Start up issues

(a) Set-up Cost;

(b) User's Perception;

(c) Personnel;

A minimum set of personnel listed in the plan includes a computer manager and at least one technical staff.

(d) Demography of the Organisation; and

Should the incident handling require travel to distributed sites, there should be funds allocated for this. Some organisations may also have branches overseas.

(e) Security Awareness and Training.

There will be requirements for initial training and continuous education on latest developments in Public Sector ICT Security. An associated issue will be the budget for seminars, workshops, conferences and continuous education programmes. It cannot be emphasised further how a good incident handling capability is closely related to an organisation's training and awareness programme. Users will be educated about such incidents and what to do when they actually occur. This can increase the likelihood that incidents will be reported early, thus minimising the damage.

3.9 Public Sector ICT Security Awareness, Training, Acculturation and Education

Allocate sufficient resources for planning and implementing Public Sector ICT Security awareness, training, acculturation and education programmes

ICT systems are as good as the people that operate them. Though application and sensitivity may differ amongst government departments the people is usually regarded as one of the weakest links in attempting to secure ICT systems. Therefore it is of the utmost importance to allocate sufficient resources for the planning and implementation of programmes on Public Sector ICT Security awareness, training, acculturation and education.

Security conscious and trained employees are able to improve ICT security systems

Security conscious and properly trained employees are still one of the best means to improve any Public Sector ICT Security system. Programmes that are conducted properly will make employees realise the importance of their role in ensuring the safety of their ICT environment. Therefore the Public Sector ICT Security awareness, training, acculturation and education programmes should be designed such that it enhances security from both the assets and human counterpart point of view.

This is performed by:

(a) Improving Awareness

Often the biggest challenge towards making a start in Public Sector ICT Security. Users should be exposed to Public Sector ICT Security issues to bond a common interest in the need to protect ICT systems. By making users aware of their responsibilities, they then become accountable for all their actions or inactions in lapses of security. Teaching users the correct ICT security practices (for example to avoid short cuts) helps mould user behaviour. It also supports individual accountability, which is one of the most important means of improving Public Sector ICT Security;

(b) Developing Skills and Knowledge

To enable users to perform or to take remedial actions in a more informed manner. Users tend to behave predictably once they become aware of the consequences of their actions. Skills development and knowledge upgrade has always been looked upon as a requirement for users to perform their jobs in an explained and secure manner. This requires a conscious and concerted effort from management; and

(c) Building In-depth Knowledge

Since threats are becoming more sophisticated, varied and sometimes identifiable only at the end of an attack, there is always the need to keep abreast with technology, defence mechanisms, methodologies, case studies etc as needed for the design and implementation of Public Sector ICT Security programmes.

3.9.1 Benefits of Public Sector ICT Security Awareness, Training, Acculturation and Education

Benefits of ICT security awareness, training, acculturation and education

The benefits of the Public Sector ICT Security awareness, training, acculturation and education programmes are as follows:

(a) the formalisation of the Public Sector ICT Security programmes should indicate the seriousness of the government in protecting its ICT assets. By understanding Public Sector ICT Security issues, employees are able to improve on their behaviour as they become more equipped and able to exercise best practices; and

(b) Heads of Department on the other hand are able to hold their staff accountable for all their actions or inactions and they would now not be able to plead ignorance.

Awareness stage which is followed by training, programme, enforcement and follow-up

The awareness stage can be followed by a training programme, such as identifying vulnerabilities and implementing safeguards. Once the training has been conducted, the enforcement and follow-up can follow suit. At this stage, it would be difficult for employees to provide convincing argument when caught doing something wrong.

Accordingly, the government adopts the principle of accountability as a basis of the Public Sector ICT Security Policy where all users are made accountable for all their actions or inactions. It is recommended that user accountability be stated clearly and prominently in accordance to the sensitivity of information accessed. To ensure that the responsibility is discharged, the government requires that ICT systems possess capabilities that can track user activities.

3.9.2 Public Sector ICT Security Awareness

Importance of ICT Security practices

Due to the huge repositories kept and the ingenuity to translate system weakness into gains, it has become necessary to remind those being trained about Public Sector ICT Security the importance of sound Public Sector ICT Security practices.

Explaining the consequences of Public Sector ICT Security failure in terms of effects to the organisation (embarrassment, monetary value, recovery efforts and time loss) and the preventive measures that should have been taken, should provide enough motivation to protect ICT assets.

Users are trained based on the level and job function

There are many types of users of government ICT assets. The awareness programme to be developed should consider the various roles to be extracted and expectations of these different user groups. For example, for those in management, the awareness programme could be designed towards managing the roles of establishing Public Sector ICT Security.

As for other groups such as those in the technical environment, the awareness programme should be geared towards Public Sector ICT Security relating to their actual jobs in processing, dissemination or report generation. In today's environment where almost everyone in the public sector has access to ICT resources, the awareness should consider the different educational backgrounds, job specifications and security clearance in deriving the maximum benefits for all target groups.

	AWARENESS	**TRAINING & ACCULTURATION**	**EDUCATION**
Attribute :	'What'	'How'	'Why'
Level :	Information	Knowledge	Insight
Objective :	Recognition	Skill & Experience	Understanding
Teaching Method :	Media : - Video - Newsletter - Posters - Lecture - Class room - Seminar	Practical Instruction - Lecture - Case study & workshop - Hands-on practice - Counselling	Theoretical Instruction - Discussion - Seminar - Background reading - Class room
Test Measures :	- Understanding - Interview - Case study	- Problem Solving (applied learning) - accreditation	Essay (interpret learning)
Impact Time Frame :	Short-term	Intermediate	Long-term

Table 3.2: Public Sector ICT Security Awareness, Training and Education Programme

Every employee has a role in ensuring and protecting ICT resources

The awareness programme should be designed to reinforce the importance of Public Sector ICT Security and the fact that every one in the civil service especially those who have access to ICT assets, have a role in ensuring and protecting ICT resources. Should employees fail to realise this or should they view Public Sector ICT Security as just another set of rules and procedures, they may end up becoming passive passengers. It is also advantageous that when awareness programmes are conducted, active participation is always encouraged so that views on security threats and vulnerabilities could then be used as input to improve Public Sector ICT Security.

Topics to be covered in the awareness programme

The awareness programme is also used to remind everyone of basic security practices such as the clear desk policy, need-to-know principle, proper log-outs and accountability. Thus it is recommended that governments department conduct regular Public Sector ICT Security awareness programme to cover suggested topics as follows:

(a) threats and vulnerabilities;

(b) impact of disclosure;

(c) roles and responsibilities;

(d) punitive actions; and

(e) abnormal events.

The list presented above may be expanded by the ICTSO when conducting such programmes.

Examples of media to be used to conduct the awareness programme

In conducting the ICT awareness programme it is also recommended that relevant information be used and conveyed through the use of multiple media such as:

(a) presentation papers;

(b) pamphlets, flyers and posters;

(c) films, videos, slides;

(d) CDs; and

(e) video conferencing.

3.9.2.1 Techniques

Awareness techniques

Established fora such as presentations, seminars, workshops, meetings, talks, lectures, demonstrations, and bulletin boards whether formal or informal should be used. It is also best to incorporate Public Sector ICT Security awareness into basic ICT training either at the point of recruitment or through scheduled training programmes. It is to be noted that no matter how well the awareness programme is designed, it may be neglected over time. For this reason the design of such a programme in terms of techniques and reach should be creative and flexible.

Awareness sessions are conducted via classes

In cases where the awareness programme is conducted through a classroom approach, it could be arranged either on a stand-alone basis or as part of another programme. The medium could be lecture-based, computer-assisted, multimedia-based or a combination of all three. It is also best to include case studies and a hands-on approach in designing such programmes.

3.9.3 Public Sector ICT Security Training & Acculturation

ICT training & acculturation should be designed with the purpose of imparting skills

Different from Public Sector ICT Security awareness, the Public Sector ICT Security training & acculturation should be designed with the sole purpose of imparting the necessary skills to users. Armed with the new skill sets, they should be able to perform their jobs more effectively. This includes a list of what they should or should not do and how they can go about doing it. There are however many levels of Public Sector ICT Security to be addressed depending on the sensitivity of the installation to be protected. It ranges from basic Public Sector ICT Security skills to the intermediate level or advanced and specialized skills. It can also be specific to particular ICT systems or generic to address common ICT issues.

In order to be effective, the training and acculturation programme should focus on the specific audience or be related to particular job skills. This is to ensure that the right people receive the correct skills to enable them to perform effectively. Under this topic there are two types of users that can be targeted:

(a) general users; and

(b) specialised or advanced skills users.

3.9.3.1 General Users

General users

This constitutes the majority of users who need to understand good Public Sector ICT Security practices such as:

(a) physical security e.g. protecting the perimeter, power supply, access control, environmental control, fire hazards, flood, etc;

(b) access security e.g. keeping access codes confidential, authorised versus unauthorised access, etc; and

(c) reporting responsibilities such as having knowledge of Public Sector ICT Security violations, virus incidents and any other form of untoward or unexplained incidents.

All users shall be formally advised by the respective departments regarding:

(a) individual access control, stating privileges based on current job functions; and

(b) the fact that ICT resources that they are privy to, belong to the government including the resources itself, data, stated information or information that is derived. The government reserves the right to monitor activities of all users accessing government ICT resources for misuse or use of ICT resources other than the purposes for which they were intended.

In designing training programmes, care should be exercised not to overload general users with unnecessary details. This is because the very same people are already the target for other training and acculturation programmes. It is best to focus on Public Sector ICT Security issues that affect the general users directly so that they remain alert to activities that affect them. For this group of users, the intention is to improve basic Public Sector ICT Security practices and not to make them experts on Public Sector ICT Security philosophy.

3.9.3.2 Specialised or Advanced Skills Users

Specialised or advanced skills

Apart from the general users, there is a small group within the public service that will require specialised or advanced ICT training on the technical and financial aspects of the ICT technology, specialised security products and specific mitigation efforts on security breaches. This group will include ICTSO, ICT officers and some senior members of management.

The identification of officers requiring specialised training can be done through various means often with the overriding objective to support and complement organisational goals.

One method is to identify new skill sets that would be required as a result of changes in requirements. For example, when organisations switch from mainframes to client server systems, it will cause a radical change to the system architecture hence affecting Public Sector ICT Security. Another method is to look at the job categories and job functions to identify skills needing upgrades. The management of skills upgrade, training and new skill opportunities is important to ensure the continuous supply of trained and competent human resource in ICT security. However, this function is often conducted haphazardly.

3.9.4 Public Sector ICT Security Education

Education training towards re-skilling and upgrading the skills

The ICT education programme offers a more structured approach towards re-skilling and skills upgrade in Public Sector ICT Security. It is normally targeted for ICTSOs or those whose job requires specific Public Sector ICT Security expertise.

3.9.5 Implementation

Implementation approaches

In order to ensure an effective Public Sector ICT Security awareness, training and acculturation, it is necessary from the very onset to have proper planning, execution and feedback. There are many approaches that could be used, one of which is outlined below consisting of seven major steps:

(a) understand the core business of the organisation;

(b) identify gaps in Public Sector ICT Security knowledge;

(c) align skill gaps so as to support the organisation's core business;

(d) identify suitable staff;

(e) secure financial resources and identify training locations; and

(f) execute, maintain and evaluate programme effectiveness.

3.9.5.1 Understand the Core Business of the Organisation

Identification of core business will assist in the design of the educational programme

The identification of the core business of an organisation will indicate the nature of the training programme that should be designed and implemented. The underlying factor is that the training programme to be embarked upon should support the goals and objectives of the organisation. From here onwards it would be easier to determine the scope of the training programme, which may include training for the entire hierarchy or limited to groups. Since training requirements differ, the training programme may need to be tailored accordingly or supplemented by more specific programmes.

The aim is to ensure ICT assets are protected at an acceptable level

The overall aim of the ICT education programme is to ensure that ICT assets are accorded the appropriate level of protection by increasing awareness towards Public Sector ICT Security.

3.9.5.2 Identify Gaps in Public Sector ICT Security Knowledge

The aim is to bridge existing gaps

The purpose of this exercise is primarily to bridge existing gaps in Public Sector ICT Security knowledge pertinent to the organisation. It also helps to reinforce and build upon basic knowledge already available amongst members. Should this not be done, the organisation runs the risk of sending people to the same course resulting in waste.

3.9.5.3 Align Skill Gaps to Support the Organisation's Core Business

The aim is to determine the education programme support organisational needs

This is also an important aspect in determining that the education programme support organisational needs. One method of achieving this task is to list all skills currently available and comparing it with the list of skills necessary to support the mission of the organisation. In doing so the skill gaps become apparent and should be prioritised accordingly.

3.9.5.4 Identify Suitable Staffs

The aim is to identify the level of skill

There are many levels of ICT training, each level being suitable to the different categories of staff within the organisation. At the beginning it may not be possible to meet all the training needs, thus it is suggested that the identification of staff eligible for training be segmented according to:

(a) Level of Public Sector ICT Security Knowledge

The target audience may be grouped according to its current level of Public Sector ICT Security knowledge. This may require some research to determine the individual skill level. For the ICT expert, a highly technical training programme is more suited than one that touches on management issues or Public Sector ICT Security fundamentals. The same can be said for a new recruit who will find difficulty in understanding highly technical issues;

(b) Job Task or Function

Target audiences may be grouped according to their job task or function such as data entry, operations, maintenance, general users, management or network specialists;

(c) Job Category

Different job categories generally carry different responsibilities whereby the Public Sector ICT Security training requirement will also be different. Some examples are application development, systems design, and systems testing; and

(d) Types of ICT Systems Used

Public Sector ICT Security measures vary according to platforms and applications. It may be necessary to design security training programmes that meet specific requirements of the installation.

3.9.5.5 Allocate Financial Resources and Identify Training Location

Training programme should be identified during budget

Training programmes can be a drain on financial resources especially for courses that are only available overseas. There may also be a time lag between the availability of funds and training dates. Currently in the public sector, for budgetary purposes, the planning to secure financial resources takes place once in two (2) years before the training programme starts.

In identifying training locations, departments are required to give preference to courses provided by recognized or reputable ICT training organisations. In doing so the course topics, content, methodology, approach, materials, courseware, etc can be assured to be of use and beneficial to the participants.

3.9.5.6 Execute, Maintain and Evaluate Programme Effectiveness

Training programme should be executed, maintained and evaluated for effectiveness

A training programme no matter how comprehensive will remain a training programme unless it is executed, maintained and evaluated for effectiveness. In terms of Public Sector ICT Security, the training programme should be visible so there is constant awareness of its existence. The visibility creates awareness signalling a high sense of anticipation. Users on the other hand realise that improper conduct could soon come to an end. In many instances, ICT training programme announcements create a receptive learning mode.

The methods used should include instructor-led sessions with consistent materials presented and tailored to the needs of the target audience. It could exist as a stand-alone, one time training or a series of training with gradual increase in subject matter. Apart from this, it could be useful to have a mix of classroom with hands-on training and exam.

ICT technology changes so rapidly that it is possible to expect new technologies in the market every two months. There should be planned effort to keep abreast of changes in the ICT technology especially those that affect security requirements.

It is possible that approved training programme needs may become irrelevant when an organisation uses new applications or effects changes to its environment. A good example is when an organisation switches to Internet technology thus renders existing security guidelines useless. Similarly a training programme can become outdated when there are changes in policies and laws. Before the advent of e-mail, the government's official communications was through letters, telephones and later facsimiles. With e-mail, new guidelines need to be established to regulate its use and to ascertain integrity and point of origin. Therefore in light of the inevitable changes brought about by either technology or changes in policies/laws, training programmes too should reflect such changes.

Measure training programme

Similar to other training programmes, the effectiveness of security training is not easy to measure. Nevertheless, some form of measurement must be made in order to justify resources spent. Indicators such as retention of information and adherence to security procedures do indicate a certain degree of effectiveness.

Organisation could also employ proven programme measurement indicators such as:

(a) Participant's evaluation of courses/programmes;

(b) monitor Public Sector ICT Security incidents before and after training; and

(c) use of 'cascade effect' by requiring returning participants to demonstrate skills and understanding.

More often, the training on Public Sector ICT Security occurs as an after thought. As threats and vulnerabilities become more sophisticated, liberalisation of the Internet added further exposure to practically all ICT resources. It is common knowledge that ICT attacks could be mounted from anywhere within a short time frame and all evidence removed in an equally short time. There is therefore an urgent need to match disruptive capabilities with superior on-going counter measures.

3.10 Physical and Environmental ICT-Security

Approval from the Chief Government Security Officer for all physical and environmental-related issues

In order to prevent unauthorised access, damage and interference to premises and information, all proposals related to buildings, acquisition, lease, renovation, purchase of government and private buildings housing information processing facilities have to be referred to the Chief Government Security Officer. The physical protection provided should commensurate with the identified risk and be based on the principle of defence-in-depth.

3.10.1 Physical Security Perimeter

Physical security perimeter should be considered to provide physical barriers around the premises

The physical strengthening of information processing facility is necessary to deter potential intruders. Multiple physical barriers that surround premises housing information facilities help to deter, detect and delay intruders. Where appropriate:

(a) clearly identify the perimeter to be secured;

(b) identify physical vulnerabilities and weaknesses by conducting risk analysis;

(c) ensure that the perimeter walls are physically sound and entrance into the perimeter area is only through doors equipped with suitable access mechanisms;

(d) use of real floor and real ceiling such that physical threats is seen and not hidden;

(e) control access by means such as registration counter, smart cards, camera etc; and

(f) alarms to detect excessive smoke, heat, moisture and unauthorized entry

3.10.2 Physical Entry Controls

Secure areas should be protected

Once areas are gazetted as Secure Areas, these areas are accorded suitable protection so as to allow legitimate access. The following controls should be considered.

(a) visitors should be escorted until “handed over” to their change and details of their entry and exit duly recorded. For some installations, visitors are accepted by appointment only with predetermined routes and access privileges;

(b) for unmanned counters, use identification tags that doubles as door access control;

(c) allow access to ICT assets and passageway to authorised employees only;

(d) authorised employees and visitors to use clearly identifiable tags so as to differentiate and to quickly identify trespassers;

(e) review access rights to secure areas regularly to reflect changes in function, job description etc; and

(f) Chief Government Security Officer advice on secure door locks and related access control services.

3.10.3 Secure Area

Secured area – area where access is restricted and limited to authorised employees only

A secure area may be defined as an area where access is restricted and limited to authorized employees only. This is done to protect the contents that are housed in the area. Department heads in consultation with the ICTSO is required to review the security requirements of their installation and plan for the provision of suitable protection within the secure area and its immediate surroundings. Consideration should also encompass relevant health and safety regulations. Reference should also be made to the Chief Government Security Officer to determine whether to gazette the secure area.

Preventive steps required to be taken to prevent unauthorized access include all or part of the controls below:

(a) limit the entrance and exit points;

(b) erect gates/grills and install security lighting;

(c) employ security guards equipped with suitable security tools;

(d) locate secure areas away from public passageway;

(e) secure areas to be bereft of markings, signs or any indication to betray its importance;

(f) secure areas should use doors that slam shut after opening or leave an audible warning when left open for an unreasonable duration;

(g) secure areas should be manned where possible with random patrols. When left unattended, all exits, entrances and windows should be locked;

(h) install intruder detection systems such as cctv and silent alarms linked to a command control center; and

(i) treat information, no matter how trivial emanating from secure areas as confidential and employ need to know principle.

3.10.4 Working in a Secure Area

Working protocols in secure areas

Employees and third party personnel may work in a secure area. As such, control mechanisms should be emplaced to prevent any untoward incident.

The following should be considered:

(a) escort third party personnel at all times;

(b) provide separate working areas for employees and third party personnel;

(c) halt all production work within secure areas when in the presence of authorized guest(s);

(d) all work within secure areas should be supervised;

(e) information about work within secure areas is on a need to know basis; and

(f) control movement, transfer, introduction or removal of equipment.

3.10.5 Site Protection for Data Centre and Computer Room

Data Centre and Computer Room should be secured

The following site design guidelines and controls should be considered and implemented where appropriate:

(a) the site shall not be in a location that is vulnerable to natural or man-made disaster e.g. flood, fire, explosion etc. Relevant health and safety regulations, standards and also any security threats presented by neighbouring premises should be taken into account;

(b) the site should be made as inconspicuous as possible to give minimum indication of its purpose;

(c) locations of computer facilities should not be identified;

(d) hazardous and combustible materials should be stored securely at a safe distance from the site;

(e) main fallback equipment and back-up media should be at a safe distance to avoid simultaneous damage;

(f) safety equipment should be checked regularly;

(g) emergency procedures should be documented and tested regularly;

(h) doors and windows should be locked at all times and external protection should be considered for windows; and

(i) external wall of site should be of solid construction.

3.10.6 Equipment Protection

In order to ensure all equipment are secured accordingly and are fully functional, the following equipment protection guidelines and controls should be considered:

3.10.6.1 Hardware Protection

It is important to ensure that all hardware are secured, operating and functioning well.

3.10.6.2 Storage Media Protection

Physical and environmental protection for storage media

In order to ensure the safety of official information stored on mass storage media, the following procedures need to be applied:

(a) designate a special restricted area for storage of mass storage media containing official information. As such, the restricted area would be accorded suitable physical protection;

(b) provide special storage facilities approved by Chief Government Security Officer such as protective cabinets or other securable storage facilities for media containing official information. This facility should protect its contents against unauthorised access and/or the effects of natural disasters such as fire or floods and harmful substances (e.g. dust).

(c) restrict access to the secure storage location; and

(d) document all procedures and access authorisation levels.

In preventing unauthorised removal, destruction or disclosure of information, the following management procedures are recommended:

(a) provide access restriction and control to all areas containing a concentration of information storage media. In addition, consideration should be given to the use of electronic article surveillance security systems;

(b) all media should be stored in a safe, secure environment, in accordance with the manufacturers' specifications;

(c) logging of all accesses made to the media should be established to support accountability;

(d) provide automated media tracking systems for maintaining inventories of storage media libraries; and

(e) authorisation for the removal of information should be required from the organisation and a record of all such removals should be kept.

3.10.6.3 Documentation Protection

In ensuring that documentation is not open to unauthorised access, consider the following steps:

(a) store/lock safely and securely;

(b) use physical or electronic security label;

(c) use encryption software for classified document;

(d) handle properly movement of classified document; and

(e) for secure handling of paper documents, refer to *Arahan Keselamatan*.

3.10.6.4 Cabling Protection

Cables need to be protected

In protecting cables from interception, damage and overloading, consider the following:

(a) cabling should be physically protected against accidental or deliberate damage;

(b) select cable type appropriate to its purpose;

(c) plan carefully by taking into account future developments; and

(d) cables should be protected against wiretapping.

3.10.7 Environmental Security

In order to ensure environmental security, proper functioning of critical and sensitive information processing facilities must be given due consideration.

3.10.7.1 Environmental Control

Power supply should be suitable and air conditioning should be controlled

The following guidelines should be considered:

(a) plan carefully the layout of the data centre (console room, printing room, partitioning of computer equipment, etc);

(b) control room temperature and humidity accordingly;

(c) provide adequate ventilation for work areas;

(d) provide suitable eye and nose protection appliances;

(e) printing rooms should be separate from computer equipments; and

(f) use raised flooring in the data centre.

3.10.7.2 Power Supply

All ICT equipment should be protected from power failure. A suitable power supply should be provided including uninterruptible power supply, if necessary. The use of a stand-by generator is required for critical data centres.

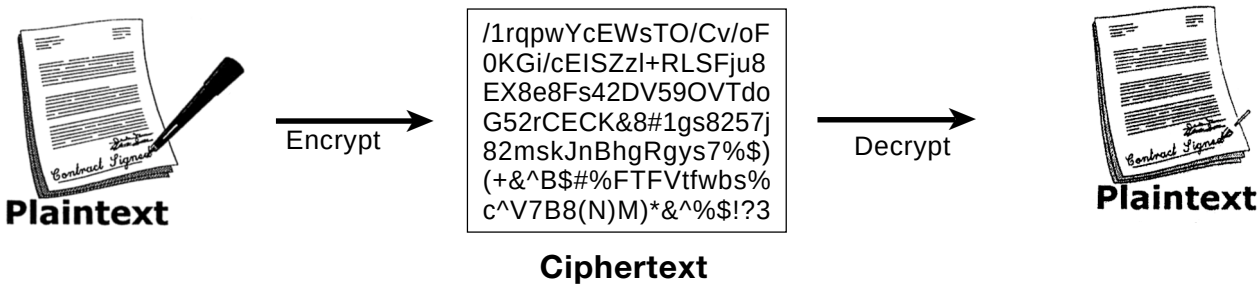
3.10.7.3 Emergency Procedures

Emergency procedures should be established, documented and posted at key locations. It should be tested at least once a year.

3.11 Cryptography

What is cryptography

Cryptography which is traditionally known, as the art of 'secret writing' is a branch of mathematics based on the transformation of data. The transformation process is called encryption. When encrypted, a plaintext becomes unintelligible and the unintelligible version is called a cipher text. In order to recover the initial plaintext, the cipher text must be subjected to a reverse process called decryption. Both encryption and decryption are done using a key.



Ciphertext

Importance of cryptography to ICT security

Today, cryptography is the most important and fundamental tool to manage ICT security. Its usage is found in almost all aspects where security is of concern. This is more than just for keeping secrets (confidentiality), but also data integrity, digital signature and advanced user authentication.

Encryption is only part of the total solution

Although modern cryptography relies upon advanced mathematics, a typical user can still reap its benefits without understanding the heavy mathematics. Nevertheless, there are important issues to be considered when incorporating cryptography into computer systems. This is because any security solution should be seen in totality. Employing strong encryption may still not solve a problem because break-ins are made through other weaknesses and vulnerabilities.

Cryptography consists of algorithm and key

Basically, cryptography relies upon two components namely an algorithm and a key. In modern cryptographic systems, algorithms are complex mathematical formulae and keys are strings of bits. For two parties to communicate, they must use the same algorithm (or algorithms which are designed to work together). In some cases they must also use the same key. Such keys are normally kept secret. There are also situations in which even the algorithms need to be kept secret.

Two types of cryptography systems: symmetric and asymmetric

There are two types of cryptographic systems: symmetric and asymmetric. A symmetric cryptosystem (also known as secret-key cryptosystem) uses the same key to encrypt and decrypt a message, while an asymmetric cryptosystem (also known as public-key cryptosystem) uses one key to encrypt a message and a different key (the private key) to decrypt it.

Comparison between symmetric and asymmetric systems

Both types of systems have different features and offer advantages and disadvantages. Although they can be differentiated, comparing them is like comparing an apple with an orange. For example, symmetric systems are generally faster and require only a single key, whereas asymmetric systems are slower and need two keys. However, key distribution is a major problem for symmetric systems, yet it is not so in the asymmetric systems. Often, they are combined to form a hybrid system to exploit the strength of each type. In determining which system to use, an organisation needs to identify its security requirements and operating environment. An appropriate policy should be developed.

3.11.1 Symmetric (or Secret) Key Systems

In symmetric system, key privacy is most important

In symmetric key systems, two or more parties share the same key, which is used to encrypt and decrypt data. Here, the security hinges on maintaining the key secret. If the key is compromised, the security offered is severely reduced or eliminated. In this type of system, it is assumed that all members who share the same key do not disclose it and are responsible to protect it against disclosure.

The best known symmetric key system is the now unused Data Encryption Standard (DES). It was recommended as a standard by NIST, United States until it was shown in the early 90's to be breakable.

Main problem with symmetric system is secure key distribution

Symmetric cryptosystems have a problem: how to transport the secret key from the sender to the recipient securely and in a tamper-proof fashion? Frequently, trusted couriers are used as a solution to this problem. Examples of symmetric key systems include 3DES (which reuses the DES 3 times), IDEA, RC5, Twofish and Rijndael. Another, more efficient and reliable solution is to rely on an asymmetric key system.

3.11.2 Asymmetric (or Public) Key Systems

Asymmetric system is designed to address key management problem

Since a secure cryptographic system requires the periodic changing of an encryption key, key management becomes a significant problem. Asymmetric or public-key encryption which was developed in 1976 addresses this problem. A public key encryption algorithm uses different keys for encrypting and decrypting information. Information encoded with either of the keys can only be decoded with the other key. It cannot be decoded with the same key. These two keys are created together and form a key pair. One of these keys is kept secret by the owner and is known as the private key. The other key, known as the public key, can be published widely. The relationship between the keys is such that it is extremely difficult (impossible for all practical purposes) to derive one key from the other.

In a public key system, there is no need for the sender and receiver to share the private key. It is only the public key that is distributed. In other words, the private key is never shared. Confidential messages can be sent using only the public key, and the decryption process requires the private key that is held just by the intended recipient. A further, very significant benefit is that public-key encryption can be used not only to ensure confidentiality, but also for authentication and digital signature.

Examples of asymmetric key systems include RSA (due to the designers Rivest-Shamir-Adleman), Digital Signature Standard (DSS), and ElGamal.

Minimum key length is 1024 bits

The minimum key length for encryption to be used in the public sector is 1024 bits and the cryptographic algorithm approved by the government.

3.11.3 Key Management Issues

Keys need to the managed properly to maintain integrity

The importance of looking after the cryptographic keys has raised many issues. The way they are created, distributed and used is critical to the confidence placed upon the cryptographic system. It is vital that there are well understood processes for:

(a) generation of new keys : users to be able to obtain suitable pairs of public and private keys;

(b) publication of the public keys;

(c) verification of the owner of a public key;

(d) determining the validity period of a pair of keys; and

(e) dealing with private keys that are lost or that may have been compromised.

Today the commonly accepted way to deal with the verification of public keys is through the use of certificates. A certificate is an electronic document that verifies the claim that a particular public key does in fact belong to a given individual (or organisation).

3.11.4 Disaster Cryptography and Cryptographic Disasters

When a disaster strikes, (see also Section 3.7.2 - Disaster Recovery/Contigency Plan), ICT components that use cryptography will require special handling. The situations are generally called disaster cryptography and cryptographic disaster.

3.11.4.1 Disaster Cryptography

Disaster cryptography is when disaster affects a cryptography

A ‘disaster cryptography’ means a situation when disaster affects cryptosystems and its uses. For a typical ICT component, recovery from disaster may entail a simple recovery using back-up and the person who is directed to perform the recovery may be allowed to read and access the components. However, for components which use cryptography, the procedure is not as straightforward as that. The person may not be allowed to freely access such assets, or may not have the key to perform the recovery process.

From the DRP perspective, cryptographic facilities, such as key management centres and Certification Authorities (CA), must also be brought back on-line following a disruption. Ensuring that keys remains secure while they are made available from back-up sites is just one of the complicating factors. Split knowledge in the form of a secret sharing scheme or dual control can be utilised. However, the back-up site for a certificate authority should use a separate certificate root since the integrity of the signature system is derived from the non-disclosure of the root key which is outside of the certificate authority’s key generation device.

If, for example, an organisation uses cryptographic facilities to secure its communication, it must be ensured that those facilities (e.g. CAs, key management server) operate with the same security after a disaster.

Need for crypto DRP

Therefore every organisation must have a DRP for its crypto facilities. The crypto DRP can be complicated because one simply cannot run a back-up for a CA key service as in the case of a 'normal' database. Due to the confidential character of the data, there must be a secured back-up that has to be restored in a secure way by trusted staff.

3.11.4.2 Cryptographic Disasters

Dealing with cryptographic disasters

The second relationship between a DRP and cryptography is planning how to deal with events caused or made complicated by cryptographic services, especially unforeseen failures. As an example, an institution may have an up-until-now-secure logical access control system, yet has noticed clear signs of an intruder into the system. One possibility is that the cryptographic system has failed. In such a situation, there should be clear instructions on how to proceed. Without such instructions, well-intentioned acts may exacerbate the problem. For example, attempting to unravel cipher text by modifying it may cause permanent damage.

Clear instruction to recover from cryptographic failure

Key escrow may help in emergency situations

Another example of a cryptographic disaster is the encryption of vital information by an employee who is now demanding a ransom for the decryption key in exchange for a gain. Such a problem may be solved through technical means (escrow), law enforcement, or negotiation. Unless the organisation plans for a technical solution, other solutions may be expensive, embarrassing, or both.

No complete list of threats exists and a complete list of counter-measures is impossible to produce. As a general guideline on this issue of cryptographic disaster, an information and communications security and disaster recovery programmes of an organisation must address cryptographic threats, at least in a generic form.

A written policy should cover the following:

(a) regular monitoring of the information processing system for abnormal behaviour;

(b) procedures to be followed in determining the cause of abnormal behaviour and guidelines on how to respond to a threat, intruder, compromise, etc;

(c) procedures for dealing with the failure of any cryptographic control; and

(d) provision for the availability of cryptographic services, keying material, and other related services following business interruption.

3.11.4.3 What to do in the Event of a Cryptographic Disaster

Take steps according to the incident reporting mechanism when crypto disaster occurs

Following a disaster, the officer responsible for ICT security in a department is required to act based on the *Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)* as per Appendix H.

3.12 Public Key Infrastructure (PKI)

What is a PKI?

An 'infrastructure' is a set of facilities which enable and promote certain types of activities. A set of public infrastructure such as roads, bridges, and airports facilitates transportation for economic activities. A Public Key Infrastructure (PKI) is the combination of software, encryption technologies, and services that enables organisations to protect the security of their communications and business transactions on the Internet.

More secure method is digital signature

Nowadays, apart from password-based logons, a more secure method is to use digital certificates. Each certificate contains specific identifying information about a user, including his name, public key and a unique digital signature, which binds the user to the certificate. Certainly, certificates should not last forever. Each certificate is issued with an expiry date and sometimes will need to be revoked early, such as when an employee quits. As with key pairs, there is a need to co-ordinate the issuance and revocation of certificates. That is another function of a PKI, acting as a comprehensive architecture encompassing key management, the registration authority, certificate authority and various administrative tool sets.

A PKI integrates digital certificates, public-key cryptography, and certificate authorities into a total, enterprise-wide secure network architecture. A typical enterprise's PKI includes issuance of digital certificates to individual users and servers; end-user enrolment software; integration with organisational certificate directories; tools for managing, renewing, and revoking certificates; and related services and support.

PKI protects information assets in several ways:

(a) Authenticate Identity
Digital certificates issued as part of a PKI allow individual users, organisations, and web site operators to validate the identity of each other.

(b) Verify Integrity
A digital certificate ensures that the message or document the certificate 'signs' has not been changed or corrupted.

(c) Ensure Privacy
Digital certificates protect information from interception during transmission.

(d) Support for non-repudiation
A digital certificate validates user identity, making it nearly impossible to later repudiate a digitally 'signed' transaction, such as a purchase made on a web site.

Some services need PKI immediately e.g. e-mail, fail transfer, remote access

In the public sector, some services stand out as immediate candidates for the need of a PKI: e-mail, secure file transfer, document management services, remote access, e-commerce and Web-based transaction services. Support for non-repudiation, which ensures that transactions cannot be disowned, is also required and supplied through the use of digital signatures. Then there are wireless networks and virtual private networks, in which encryption is essential as a guarantee of confidentiality. For the corporate network and e-commerce, a single point sign-on is a common requirement.

PKI software comes in different flavours depending on whether an organisation self-develops it or procures it commercially. In each case, the certificates issued need to conform to the international standard (CCITT X.509v3 is currently the referred standard) so that interoperability to other certification authorities even overseas is ensured. It is also worth noting that until today, there still exist some doubts among industry experts on the full-fledged implementation of an internationally standardised PKI.

3.13 Trusted Third Parties (TTP)

TTP provides the vehicle for safe transactions

The market has recognised the need for enhanced security services provided by an entity mutually trusted by other entities. These services range from increasing trust or business confidence in specific transactions to provision of recovery of information for which encryption keys are not otherwise available to authorised entities. Trusted Third Parties (TTP) is the vehicle for the delivery of such services.

A TTP delivers assurances between its sub-divisions as well as between itself and external parties. An institution may choose to set up an internal TTP or subscribe to an external provider for TTP services.

3.13.1 Assurance

Criteria to be met to provide quality service

A TTP, whether internal or external to an organisation can only add value when users of the services are assured of its quality. In achieving this, a TTP must satisfy itself that the following issues are addressed:

(a) Trust
The TTP must be organised, controlled and regulated in such a way that its operation can be relied upon, checked and verified.

(b) Accredited
The TTP must be at least accredited by a recognised national or international party.

(c) Compliance
The TTP must be operated in compliance with accepted industry standards and relevant regulations.

(d) Contract
There must be a legally binding contract in place covering the provision of service and addressing all the issues in this list. There must be contracts with co-operating TTPs which also address these concerns.

(e) Liable
There must be a clear understanding as to issues of liability. Areas of concern include circumstances under which TTP may be liable for damages and whether the TTP have sufficient resources or insurance to meet its potential liabilities.

(f) Policy Statement
The TTP must have a security policy covering technical, administrative, and organisational requirements.

(g) Audit
TTP auditors must be appointed by the TTP controller.

3.13.2 Services of a TTP

The services, which a TTP provides, may include:

(a) key management for symmetric cryptosystems;

(b) key management for asymmetric cryptosystems;

(c) key recovery;

(d) authentication and identification;

(e) access control;

(f) non-repudiation; and

(g) revocation.

What is a key recovery?

Key recovery is the ability of a TTP to recover, either mathematically, through secure storage, or other procedures, the proper cryptographic key used for the encryption of information. This function would assure an institution that it can always have access to information within its information processing resources. Such a recovery service may be essential in disaster recovery. It may also satisfy law enforcement regulations for an institution to be able to produce such a key or encrypted information in answer to a lawful court order.

3.13.3 Legal Issues

Government's contract with a TTP needs to address legal issues

Government departments have higher-level requirements for record retrieval. The contract with a TTP should address specific issues relating to maintenance of keys used for encryption, authentication, and digital signature as these may need to be reproduced many years later.

Liability for the poor services of a TTP may include direct and consequential damages and must also be fully understood by the management. In the first place, the TTP must have adequate financial reserves or insurance to meet any liability.