Chapter 2 MANAGEMENT SAFEGUARDS

Senior management commitment

The main objective of this chapter is to highlight the major elements that should be considered by all government ministries, federal departments, statutory bodies, state secretaries and local authorities in their efforts to safeguard their respective ICT systems. Of utmost importance is senior management commitment towards acknowledging and addressing security issues.

5 major elements

The five (5) major elements of management safeguards are:

(a) Public Sector ICT Security Policy;

(b) Public Sector ICT Security Programme Management;

(c) Public Sector ICT Security Risk Management;

(d) Incorporating Public Sector ICT Security into ICT System's Life Cycle; and

(e) Public Sector ICT Security Assurance.

2.1 Public Sector ICT Security Policy

ICT Security Policy must ensure the government's information is secured

The government acknowledges its obligation to ensure appropriate security for all ICT assets under its ownership. This is best implemented by having a written ICT Security Policy that serve to assist in identifying at the very outset what needs to be protected. The document will also inform department members what activities are allowed or what activities are disallowed. The policy should define common rules to be abided by everyone within the organisation. The policy so formulated should address the need for a total enforcement of controls and measures to safeguard government ICT assets.

Policy needs to be balanced between rigid and loose information control

The tremendous increase in ICT dependency and usage especially with the advent of the Internet, exposes government information to a much larger audience and with that a potential threat that government information being compromised. This is especially worrying on classified government information and if left unchecked, can cause serious integrity issues to the government. At the same time, there need to be a balance between rigid information control that limits service delivery on one hand against a loose information control that would compromise security or severely affect the interest of the public service or the nation.

It is in realising the absolute importance of the provision of ICT security, the ICT Security Policy be drafted based on concrete ICT principles, best practices, responsibilities towards securing information, threats and incremental steps towards upgrading information security.

Important factors to consider in formulating the ICT Security Policy

Essentially the ICT Security Policy document should state:

(a) the ICT Security Policy statement;

(b) the rationale behind ICT security in protection against unauthorised access, ensuring availability and minimising security breaches;

(c) the ICT security definition inclusive of coverage of assets to be protected;

(d) the objectives of ensuring government operations continuity and to minimise disruptions by minimising impact of security incidents;

(e) the security principles adopted;

(f) the establishment of a clear management framework defining general and specific responsibilities for ICT security management, including reporting security incidents;

(g) the need for ICT security awareness training for all staff and specific security training for those with greater responsibilities; and

(h) the understanding of the requirement for shared responsibility in protecting government information.

There are three (3) different levels of Public Sector ICT Security Policy formulation. The higher level is the **Central Level** that provides the general policy direction. The next level is the **Ministry/State Level** that addresses specific issues and the **Departmental Level** handle operational issues.

2.1.1 Central Level

MAMPU is at the Central Level of formulating ICT policies for the public sector

This is the top most management level that initiates ICT Security within the public service. This role has been entrusted to Malaysian Administrative Modernisation and Management Planning Unit (MAMPU), Prime Minister's Department. MAMPU initiates and maintains the Public Sector ICT Security Policy Framework and is the referral centre on Public Sector ICT Security issues.

The high level policy issued as a General Circular 3/2000 dated 1 October 2000 *(Pekeliling Am Bil. 3 Tahun 2000 bertarikh 1 Oktober 2000)* provide the direction towards securing government ICT assets (Appendix A). The policy:

(a) defines the purpose and scope;

(b) assigns the responsibilities for programme implementation; and

(c) principles adopted.

2.1.2 Ministry/State Level

Specific issues affecting particular organisation

Issues addressed at this level are normally specific issues of concern affecting particular organisation or across the public service such as the disposal of unwanted computing equipment or backup of sensitive data.

Issue-specific level focuses on local areas or current issues

While the Central Level policy is intended to address the broad Public Sector ICT Security programme, the ministry/state level ICT management statements are developed to focus on specific areas currently relevant and of concern to the ministry/state.

Issue a plan of action

The management may find it appropriate, for example, to issue a plan of action on how the ministry/state should approach contingency planning (example centralised vs. decentralised) or the use of a particular methodology for mitigating a particular risk to ICT systems. Ministry/State wide plans may be appropriate when new issues arise, such as integration to legacy systems that may possibly require additional protection of some particular information.

While the Central Level broad-based policy may not require much modification over time, ministry/state policy formulation will likely require more frequent revision as changes in technology, demands, requirements, legislation and business rules take place.

2.1.3 Departmental Level

Operating at the action level

Operating or System-specific level focuses on actions taken to protect a particular system. This is operating at the action level where detail knowledge on procedures, standard, and guidelines are the daily norm.

The operating level or system specific provides detail information to address issues

While the Central and Ministry/State Specific Levels address issues from a broad perspective encompassing the entire organisation, they do not provide detailed information for example, on establishing application priorities, access controls and other specific requirements. This is where the departmental level or specific programme is needed.

The operating level security policy has important impact on system and its security

Departmental Level security policy is applied at the computer system operations level and may vary from system to system even within the same organisation. The departmental security policy has an important impact on system usage and safeguarding Public Sector ICT Security. The decision to adopt a departmental ICT Security Policy for the organisation can be made at the managerial level. Refer to Appendix D: Example of Contents List for an Agency/Department ICT Security Policy for guidelines on formulating policy.

2.2 Public Sector ICT Security Programme Management

Programme management is important

This sub-section discusses the importance of programme management and presents an organisation-wide approach in managing Public Sector ICT Security. Programme management among others encompasses nominating ICT Security Officers, developing security policies, carrying out security audits and providing ICT security incident response and handling services. In this respect, it is noted that the various ministries, departments and agencies in the public sector differ vastly in function, size, complexity, management style and culture.

2 different levels of programme management

In comparison to Public Sector ICT Security Policy formulation, there are only two (2) different levels of programme management. The higher level is the Central Level, which is responsible for overall strategy, co-ordination, planning and implementation as well as advice and direction on ICT security issues. Next is the Operating Level, which encompasses both ministry/state and department. ICT security programme management at this level details the procedures for implementing cost-effective ICT security.

2.2.1 Central Public Sector ICT Security Programme Management

Central Level ICT Security programme components

At the Central Level, ICT security programme management consists of the following:

(a) formulating Public Sector ICT Security Policy Framework;

(b) ICT Security Awareness and Training;

(c) ICT Security Incident Response and Handling;

(d) ICT Security Posture Assessment;

(e) ICT Security Business Resumption Plan Framework; and

(f) enforcement, audit and supervision.

Benefits of ICT Security programme

A central Public Sector ICT Security programme should provide three distinct types of benefits:

(a) Increased Efficiency and Economies of Scale of Public Sector ICT Security;

(b) Efficient, Economic Co-ordination of Information

A co-ordinated centralised programme can assist in the collection and dissemination of ICT Security related information efficiently throughout the Public Sector. Since it is centrally controlled, various information can be channelled directly to the respective Public Sector ICT Security Officer at the various agencies; and

(c) Central Enforcement and Supervision

One of the functions of the Central Level is the evaluation of enforcement activities and compliance. In this regard, the organisation needs to understand the business requirements, issues, vulnerabilities and Public Sector ICT Security discrepancies internally. This could be done through an internal supervisory function that allows a first-hand look at ICT issues without the potential embarrassment of an external audit or investigation.

2.2.2 Operating Level Public Sector ICT Security Programme Management

Scope of Operating Level Public Sector ICT Security Programme

Unlike the central programme that addresses the entire spectrum of Public Sector ICT Security, the operating level addresses the procedures for implementation of appropriate and cost-effective ICT security. Some of the salient items in considering the operating programme are:

(a) implementing safety measures;

(b) selection and installing of safety measures;

(c) day-to-day Public Sector ICT Security administration;

(d) evaluation of ICT system vulnerabilities; and

(e) responding to Public Sector ICT Security problems.

Local advocate

The local advocate for the security programme at this level is the ICT Security Officer (ICTSO). This officer is nominated by the ministry or department as suggested in the Public Sector ICT Security Policy Framework.

Action by ministry and department

At the operating level, the ministry or department should embark on:

(a) formulating departmental ICT security policy;

(b) undertaking ICT system life cycle management with respect to security;

(c) providing ICT security awareness and training;

(d) testing Business Resumption Plan; and

(e) conducting scheduled ICT security review.

2.3 Public Sector ICT Security Risk Management

Public Sector ICT Security is a continuous process

Need to ensure security is within an acceptable risk level

Security can be defined as a condition that is free from threats and unacceptable risks. Public Sector ICT Security should be looked upon as a continuous process. It involves periodic activities that must be implemented to ensure that security is within an acceptable risk level, taking into consideration technology change that brings with it rapidly changing threats and vulnerabilities.

Principal objective is to ensure business continuity

The principal objectives of securing ICT assets are to ensure government operations continuity and minimise disruptions or damage by preventing and minimising the impact of security incidents. ICT security aims at facilitating information sharing and simultaneously ensuring the protection of the information and ICT assets. In order to achieve the desired Public Sector ICT Security acceptance level, the vehicle used in assessing risk is aptly termed Public Sector ICT Security Risk Management. By definition, risk management is the process of assessing risks, taking steps to mitigate the risks to an acceptable level, accepting and monitoring the residual level of risks. A sample of ICT Security Risk Management process is as in Appendix E.

Steps for better risk management include identifying risks, evaluating risks and implementing safeguards

Steps required for better risk management includes:

(a) formation of a risk management committee;

(b) identifying the risks and threats;

(c) evaluating the risks and threats;

(d) identifying the necessary safeguards and counter measures;

(e) managing residual risk;

(f) implementing safeguard and monitoring effectiveness; and

(g) undertaking uncertainty analysis.

2.3.1 Formation of Risk Management Committee

Representation on Risk Management Committee

Risk analysis should be co-ordinated by the ICTSO and are best performed by a team of individuals representing the following disciplines:

(a) data processing operations management;

(b) systems programming (operating systems);

(c) systems analysis;

(d) applications programming;

(e) data base administration;

(f) auditing;

(g) physical security;

(h) communication networks;

(i) legal issues;

(j) functional owners; and

(k) system users.

2.3.2 Identification of Risks and Threats

Identifying risks and taking action

The identification of risks and threats is a critical step towards securing ICT assets. The result of the identification will dictate further activities and the channelling of resources, which consists of funding, training efforts and future planning. Hence, the proper planning of this activity cannot be overemphasised and should focus on avoiding core business shutdown or, at the least, minimising disruptions.

Unauthorised disclosure will cause embarrassment

In the public sector, unauthorised disclosure may result in embarrassment where the risk may not be quantifiable in terms of monetary loss.

In identifying the risks and threats, the ICTSO in consultation with the Chief Information Officer (CIO) and administrators will need to:

CIOs and the ICTSO need to discuss the risks and threats

(a) review the value of the information contained in their systems or information that could be derived from their information systems. Once this is done, the value attached to the ICT assets can help determine the level and types of risks that can or should be tolerated;

(b) determine events or combinations of events that could disrupt business operations. Admittedly, this is rather difficult to implement since the list could be endless. However most risks are visible and can be easily listed. Examples are physical sites, access controls, power supplies, environmental controls, etc.; and

(c) establish the priority to the risk elements identified. Some risks can have low priority whilst others are categorised as high priority risks. There is no rule to establish this, as risks are interpreted differently by agencies according to differing perceptions about the level of disruption or damage. In this light, the management may want to attach an association between risks, its potential disruptive ability and the cost of reconstruction.

The methods employed for identification of risks and threats may be formal (user observation reports), informal (corridor talk), quantitative or qualitative or a combination of these methods.

2.3.3 Evaluation of Risks and Threats

Evaluating risk through analysis of data and information

Once identification of risks and threats is completed, the process evolves towards risk evaluation, which involves the collection and analysis of data. There are many sources of information that can be used to conduct this exercise. Since information sources can be numerous, steps should be taken to screen and analyse the data. This can be performed by focusing on areas

that have the greatest impact on the organisation. The following steps can be adopted in evaluating the risk:

(a) quantify the monetary value of a loss by considering these key elements in risk analysis:

i. an estimate of the impact or cost of a specific difficulty if it happens; and

ii. an estimation of the probability of encountering that difficulty within a period of time;

(b) determine the potential economic impact of those risks or events associated with each threat by using the list of vulnerabilities associated with the department's information assets identified in the previous step;

(c) estimate the probability of the undesirable events occurring within a specified period of time (usually one year). Identifying risks and their economic impact does not directly lead to identifying which security exposures are worth corrective action and which are not. Estimating and considering the likelihood or probability of the undesirable events is vital. For example, events such as floods or earthquakes have catastrophic consequences. However, if they appear to have a low probability of occurrence they might not justify protective measures and the decision may be to tolerate the risks;

(d) evaluate the suitability of the following options once the monetary value exposure or its annual loss is estimated:

i. tolerate the risk;

ii. insure against the risk;

iii. lower the monetary impact by implementing those measures costing less than the exposure; or

iv. lower the probability of the loss occurring by implementing protective measures costing less than the exposure;

(e) determine whether security safeguards are needed and if so, allocate the cost. The information gained from this can be used to estimate the annual monetary value of a loss, which subsequently can be used to provide a common denominator for determining the magnitude of each risk. A department may then develop safeguards against the high monetary loss risks; and

(f) identify alternative security safeguards and provide recommendations for cost-effective security solutions.

2.3.4 Identification of Necessary Safeguards

Identify the safeguards– could be additional or removal of ineffective safety measures

Amongst the key elements of Public Sector ICT Security is to identify suitable safeguards. The process of identification could result in acquiring additional safeguards or the removal of ineffective safety measures because both monetary

and non-monetary factors are involved. For example, it may be effective from an economic and safety viewpoint to impose a new locking mechanism rather than to employ a security guard.

In the assessment of risks other than monetary issues, there will be areas where it is not obvious as to what kind of safeguard is appropriate.

ICTSOs and ICT managers need to consider many factors in identifying the safeguards

The other factors that should be considered by ICTSOs and ICT Managers are:

(a) legislation, regulation and organisation policy;

(b) user and business requirements;

(c) ICT system performance requirements;

(d) timeliness, accuracy, and completeness requirements;

(e) the life cycle costs of Public Sector ICT Security measures;

(f) the relative strength of the proposed safeguard;

(g) the reliance of other safeguards being considered;

(h) technical requirements; and

(i) cultural constraints.

2.3.5 Managing Residual Risks

Not possible to mitigate all risks and threats

Need to make decision on which ones

It is not possible to mitigate all risks and threats identified because, in reality, all ICT installations operate on limited resources. The management needs to decide what risks should and can be mitigated. The remainder of the risks not mitigated is generally known as residual risks. Once this type of risk has been identified based on priority ranking, a decision has to be made as to whether these risks are acceptable or otherwise. Managing residual risk should not severely affect the delivery of services and should be properly documented and monitored over time. Such residual risks should be quantified as far as possible and additional safeguards should be implemented if they are considered too high. The decision to balance between acceptable and unacceptable risk is a management decision.

2.3.6 Implementing Safeguards and Monitoring Effectiveness

Once decision is made-need for follow-through

Need to maintain, ensure it is ongoing

Need for periodic assessments

Once a decision has been made to implement the appropriate safeguards, the decision must be followed through. There is also the requirement that the safeguards be maintained and this process must be seen as ongoing, for inappropriate maintenance can render the safeguards ineffective. Also, it calls for periodic assessments to improve the safeguards with possible requirement for re-analysis of risk.

2.3.7 Uncertainty Analysis

Uncertainty analysis attempts to document grey areas

There will be instances when the management of risk relies on hearsay, speculation, best guess, assumption and incomplete data. Uncertainty analysis attempts to document this grey area so as to keep management informed and aware.

Two primary sources of uncertainty in the risk management process are:

(a) unknown precision of the methodology used; and

(b) difficulty to determine the exact value of the various elements in the risk model such as threats frequency, potential damage etc.

Projections and assumptions can be indeterminate.

It is possible that a data source is uncertain. Normally, data is collected from two sources; statistical data and expert analysis. However, there are potential problems from both sources. For example: samples taken may not be reflective of the true situation; missing or not properly counted parameters; misleading results and insufficient data. When expert analysis is done, it should be recognised that projections are subjective and the assumptions are always questionable.

2.4 Incorporating Public Sector ICT Security into the System Life Cycle

The purpose of incorporating the Public Sector ICT Security Plan into the ICT System Life Cycle is to ensure that the Public Sector ICT Security component is not overlooked. Since ICT has played an irreversible role in service delivery in the public sector, the planning of ICT systems should always include Public Sector ICT Security at the very onset. The Public Sector ICT Security Plan should be viewed as a documentation of the structured process to plan for adequate, cost-effective Public Sector ICT Security protection for the overall system.

2.4.1 Benefits of Integrating Public Sector ICT Security in the System Life Cycle

Might be too expensive to incorporate later.

Also can cause delay, disruption, etc.

It is recommended that the Public Sector ICT Security Plan be developed at the beginning and incorporated into the system life cycle. It would be difficult and expensive to redesign the applications to cater for security features at a later stage. Moreover, it can cause project delays, disruptions, diminish expectations and overall low morale.

Furthermore, it is virtually impossible to anticipate the whole array of security problems that would deter the incorporation of the Public Sector ICT Security Plan at the later stages of the system life cycle. Updating the security plan, at least, at the end of each phase in the system life cycle can minimise issues.

The documentation of decisions related to Public Sector ICT Security into the system life cycle should help assure management that Public Sector ICT Security is fully addressed in all phases including applicable legislation and other requirements.

2.4.2 The ICT System Life Cycle Phases

5 stages of ICT system life cycle.

It is recommended that planning for Public Sector ICT Security follow the stages described in most models of ICT System Life Cycle consisting of the following five (5) basic stages, incorporating ICT security issues in each stage and as depicted in Figure 2.1:

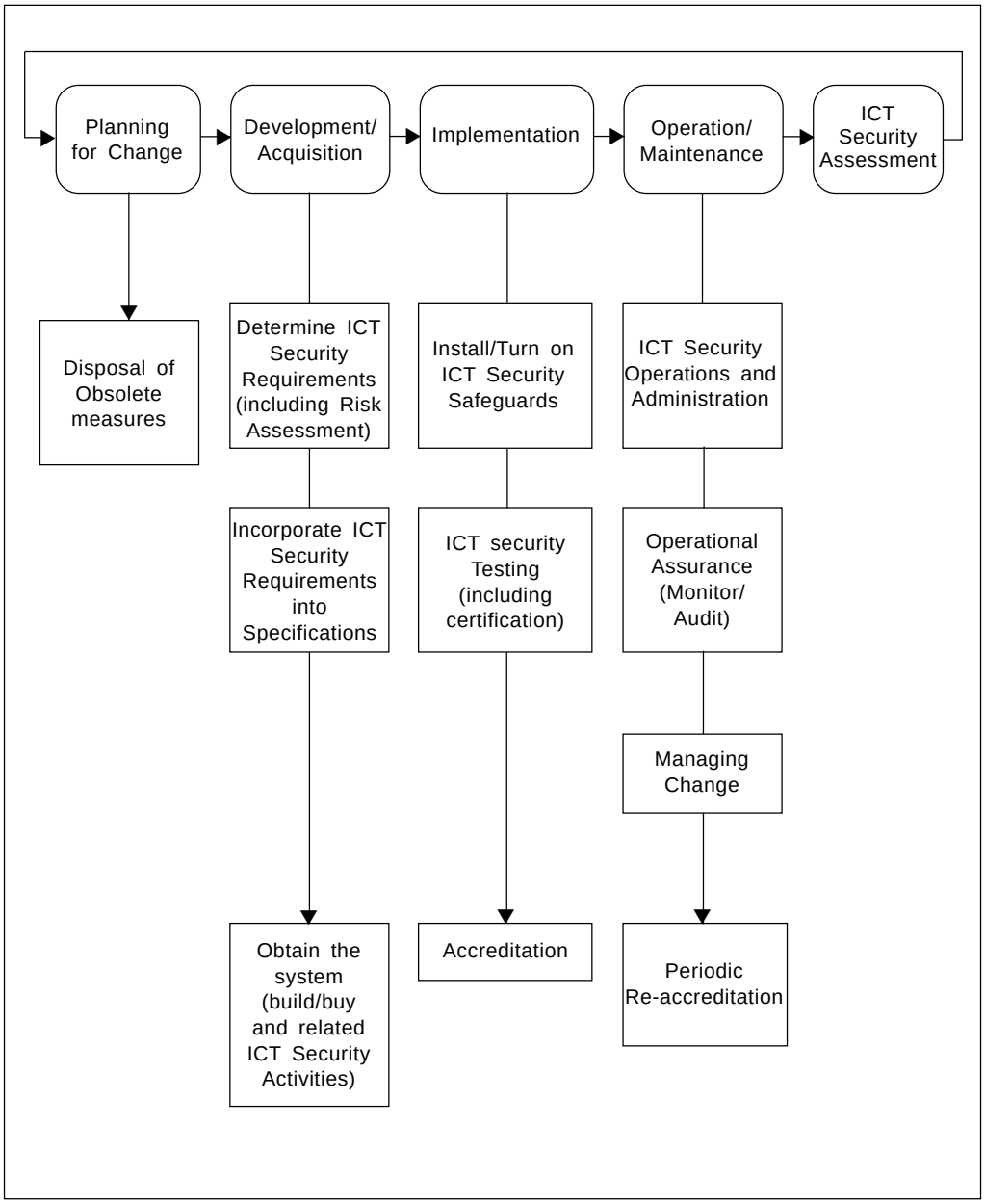

Figure 2.1: ICT Security in the System Life Cycle Phases

1st stage: Planning For Change - This is to plan for the changes that will occur with the implementation of the new ICT system to meet operational and Public Sector ICT security requirements. This exercise can be very daunting, as it will involve practically everyone in the organisation especially in areas such as re-training, adaptation and the inception of completely new procedures.

2nd stage: Development/Acquisition - This is the stage where the ICT system is being constructed, programmed, developed or purchased. The Public Sector ICT security requirements based on core business functions, ICT asset value and risk assessment should be included in this stage.

3rd stage: Implementation - This is the stage where, upon final acceptance by the government, the ICT security safeguards are initiated.

4th stage: Operation/Maintenance - This is the stage where the developed system runs alongside the daily operations of the department. As the system matures, expansion through additional equipment and application systems is inevitable. New requirements may become apparent and obsolete functions may need to be removed.

5th stage: ICT Security Assessment - This is the stage where an assessment is made to determine whether ICT Security requirements are met.

At each of the five (5) stages, additions or deletions to the existing system may take place. Therefore the security aspects must be considered for each activity in every stage.

2.5 Public Sector ICT Security Assurance

2 rule of thumb questions.

The Public Sector ICT Security assurance means the confidence level in the Public Sector ICT Security safeguards to operate correctly as planned. The effectiveness of ICT security is not easy to assure because of the difficulty in quantifying assurance. As a rule of thumb, two (2) questions should be asked:

(a) who needs to be assured; and

(b) what type of assurance is required.

There are many methods and tools available. Two (2) of these are described below: Design and Implementation Assurance; and Operational Assurance.

2.5.1 Design and Implementation Assurance

The design and implementation assurance means that the design features of the ICT system, its operations or ICT assets must meet requirements and specifications. Assurances of this nature require the examination of the ICT system design, the correct functioning of each application and the manual processes that support it. Design and implementation assurance is associated with the development, testing, as well as pre- and post-implementation stages of the ICT system life cycle. The design and implementation assurance seeks to address whether the end product complies with the agreed Public Sector ICT Security specifications. It is also used to provide evidence of deviation and remedial action.

The following sub-sections suggest some of the major methods that can be adhered to in achieving design and implementation assurance.

2.5.1.1 Testing and Certification

Testing to ensure compliance to requirement and quality.

Testing is an activity to quantify compliance to stated requirements. In addition, it can be used to address the quality of the ICT system as it is being built, implemented and operated. Therefore, the testing should be performed throughout the development cycle or wherever proof of compliance is required.

Some examples of testing are;

(a) unit test;

(b) components test;

(c) system test;

(d) integration test;

(e) stress test; and

(f) penetration test (to see whether the safeguards can be bypassed).

Certification is formal testing conducted by an independent party. The appointment of such experts must conform to the current government procedures pertaining to the appointment of consultants. *(Refer to Surat Pekeliling Perbendaharaan Bil. 3 Tahun 1995 – Peraturan Perolehan Perkhidmatan Perunding).*

2.5.1.2 Conformance Testing

The organisation may conduct conformance tests on products such as software, hardware and firmware. Conformance to ICT standards is important to ensure the inter-operability or strength of ICT security.

2.5.1.3 Use of Reliable Architectures

Need to use reliable architecture.

The use of reliable architecture such as fault-tolerance, redundancy and mirroring enhances the degree of assurance of ICT systems. However the use of costly reliable architecture is normally reserved for very critical systems that demand practically zero fault.

2.5.1.4 Ease of Safe Use

Ease of safe use of Public Sector ICT Security products and mechanisms is another important aspect of the successful implementation of Public Sector ICT Security systems. When the interface with safeguards is easy and straight forward, the tendency is that the user is more likely to use the system correctly and commit fewer mistakes. Thus, acceptance by the users enhances the overall security assurance.

2.5.1.5 Evaluation and Reviews

Product evaluation and review will help achieve assurance.

Evaluation and reviews are another option for achieving assurance. Product literature in reviews provides useful information and is normally geared to product superiority above other similar products. However, product reviews are less formal and do not offer detailed and extensive examination as is available through an evaluation.

Important factors to consider when attempting to seek comfort level via this means are as follows:

(a) independence of the review group;

(b) evaluation criteria;

(c) testing parameters;

(d) competence;

(e) integrity of the evaluating body; and

(f) assumptions made.

2.5.1.6 Assurance Documentation

Describing how ICT security requirements are met.

Assurance documentation is one that describes Public Sector ICT Security requirements and how they are met when compared against these requirements. The significance of assurance documentation is the indication of the degree of understanding as portrayed by the designers, and their presumed ability to construct solutions to meet the necessary Public Sector ICT Security requirements. Please refer to Appendix F: A Sample ICT Security Adherence Compliance Plan for guidance on compliance programmes.

2.5.1.7 Certification of Product to Operate in Similar Situation

Assurance to operate products in different environments.

There will be instances when a department seeks clarification that the ICT Security product it is about to procure operates seamlessly in its current environment. This may be the case for departments that operate on proprietary systems wishing to employ products outside their operating environment.

Most producers of ICT Security products, with very good reputation produce documentation, brochures and advertisement statements of certification of their ICT Security products that operate in similar situations. However, it should be realised that certification to operate in a similar situation is environment specific, since it may be certified to operate in one environment but may not work in another, even though the certification is performed by the same body.

The risks are high if the products to be procured and used at the required department are non-certified products. It might be a better decision to opt for other certified products. Certification should be nationally accepted.

2.5.1.8 Self-Certification

Test conducted by vendors or suppliers can be indicators.

In many instances the software vendor or the system integrator of the ICT Security system conducts self-certification of their own products. This is done to determine or at least provide some indication the quality and performance of their products. This technical evaluation may not be partial but does provide a minimum degree of assurance. In cases where a high degree of assurance is required, a third party independent evaluation is recommended.

2.5.1.9 Warranties and Liabilities

Undertaking to correct errors and provide upgrades.

This is another form of assurance where the manufacturer or integrator provides an undertaking to correct errors or provide upgrades via version releases. It can be in the form of a formal declaration or certification of the product or published assertion. The manufacturer's commitment is seen through its endorsement to correct errors and indemnify loss or damage should the product be non-conforming.

Assurance by digital signature, anti-virus software.

2.5.1.10 Distribution Assurance

The assurance of ICT products obtained via electronic distribution is important. In such a situation, the distribution of unmodified copies and its integrity can be ascertained through the use of digital signature or check-bits. Sources downloaded from unknown origin such as bulletin board should be verified by anti-virus software at the very least.

2.5.2 Operational Assurance

Operational assurance addresses technical issues.

Whilst design and implementation assurance addresses the quality issues, operational assurance seeks to address technical features such as vulnerabilities, conformance to procedures and changes to Public Sector ICT Security requirements. The ICT system being a 'living' system changes over time. Some causes of change include changes to the ICT system due to expansion of scope, operating systems or threat environment.

The operational performance of ICT systems tends to degrade over time. Creative users and operators resort to new ways to bypass Public Sector ICT Security measures with the sometimes incorrect perception that it may improve performance. It is very rare where adherence to procedures is strictly followed. In some instances this can produce disastrous results for the administration of the ICT system.

There are two basic methods to observe operational assurance:

(a) ICT System Audit

This can be either a scheduled or an unscheduled event to evaluate Public Sector ICT Security. It is important to define the scope of work since the auditing process can easily be side-tracked towards less important issues. The auditing process can both be investigative in nature (to resolve specific issues) or developmental.

(b) Monitoring

This is one of the most effective mechanisms to ensure operational assurance. However this activity is time consuming and requires more resources. It involves periodic checks on the overall ICT system including user activities, standard operating procedures, the environment etc.

2.5.2.1 Audit Methods and Tools

Auditing needs to be developmental rather than fault-finding.

All audits conducted on public sector ICT installations, environments or premises should follow stated or implied Public Sector ICT Security Policy and Public Sector ICT Security Auditing Guidelines or other documents published later. In conducting the ICT audits, the audited department plays a crucial role in extending assistance. The audits have to be treated as developmental and not as a fault-finding exercise. It is best for the government if the audited department and the audit team identify the appropriate Public Sector ICT Security requirements (which may be additional) based on the existing ICT environment. The audit conducted should not interrupt the business operation of the audited department. Three (3) different types of auditing methods with respect to depth and objectives are described in the following paragraphs.

(a) Audit Methods

i. Public Sector ICT Security Review

Public Sector ICT Security Review can be conducted by internal staff. This review is comparative in nature and is regarded only as informative. Reviews are normally conducted for a short duration but its preliminary initial results may lead to more advanced and detailed types of audits.

ii. Internal Audit

The internal audit measures the compliance of the ICT systems. The results of this exercise could be used as a guide even though there may be a conflict of interest.

In every environment, the internal staff is more knowledgeable in the ICT system installation, system security, etc than a third party. Hence the internal audit review is a required step to be performed.

Inadequacy of an internal review is that a poorly designed or poorly operated security system could still be acceptable. On the other hand, there could be a strong desire to improve the Public Sector ICT Security system.

iii. External Audit

In comparison, external auditing involves a third party that has no stake in the ICT systems. The independent party should review the ICT system installation, system security, etc.

In all three cases it is important to ensure that auditing personnel possess sufficient knowledge of Public Sector ICT Security.

Suitable generic auditing tools for the various types of audit described above are briefly explained below:

(b) Audit Tools

i. Automated tools (active and passive tools)

Tools for auditing the Public Sector ICT Security system.

The use of automated tools reduces the amount of work that has to be completed. It is used to identify a variety of threats and vulnerabilities such as improper access control, weak password or failure in using current up-dates and patches.

Active automated tools are designed to locate vulnerabilities by trying to exploit them. Passive automated tools examine only the ICT system and infer the existence of problems.

The government's Public Sector ICT Security could be in a difficult situation if automated tools are not used. This is primarily due to the fact that hackers use similar tools to identify weaknesses of the ICT system.

Some of the current automated tools are easier to use while others require specific skills and pre-requisites.

ii. Internal control audit

These tools are used to determine the effectiveness of control or safety measures. It includes analysis on both ICT and non-ICT based controls or safety measures. Techniques used include inquiry, observation and testing to detect illegal acts, misuse, errors, irregular incidents or a general lack of compliance

iii. Security checklist

This is a tool normally developed by system owners to ensure that changes to the ICT system configuration has been reviewed. The checklists should be formulated to reflect local operation of an ICT installation.

iv. Penetration testing

The penetration test could be used as a tool to emulate the real life situation of potential attackers attempting to break into ICT systems. Findings from the tests are used to overcome vulnerabilities and weaknesses. On conducting such tests the 'attackers' should be using tools as would be used by the genuine attacker such as:

* automated tools as described previously;
* manual penetration;
* internet tools; and
* social engineering.

2.5.2.2 Monitoring Methods and Tools

Public Sector ICT Security need to be monitored continuously.

The ICTSOs and senior management in the public sector need to be sensitive to the vulnerabilities of the Public Sector ICT Security and react to ICT incidents. Thus it is important that the monitoring of the entire Public Sector ICT Security should be treated as an on-going process.

Many tools are available today and there are more being developed to handle new and complex attacks on ICT establishments. Below are some of the tools used for monitoring which also complements tools used in auditing. These tools enable monitoring to review ICT systems regularly and in real time. Access to audit tools, tabulation analysis and recommendations should be restricted and authorised.

(a) ICT System Logs — A documented evidence and a chronological event of all ICT system activities. This log should consist of information such as identification of unauthorised access, unexplained or abnormal activities. The logs should be viewed regularly in order to verify the usual and/or unusual activities in the ICT system.

Best practice : View and check the log daily on critical or sensitive systems.

(b) Automated tools

i. Virus Scanners

Readily available on the market both for stand-alone or networked systems. All users should use anti-virus software to verify the integrity of their systems. However, it should be noted that the threat from virus requires periodic up-dates of the anti-virus software

Best practice: Up-date anti-virus software regularly.

ii. Check Summing Algorithm

Work by generating mathematical value based on the contents of the file. Verification of the file is done by comparing the value of the sum generated by the current file with the previously generated value. The integrity of the file is verified when the two values are identical. Another common tool is the digital signature, which is also used to verify the integrity of the files.

Best practice: Ensure the check summing tools are run on the new installation, clean version and check sum value are stored securely.

iii. Password Crackers

These are specialised software to check against proper user passwords as compared to easily guessed passwords.

Best practice: Run monthly.

iv. Integrity Verification Programmes

Some of the techniques applied in integrity verification include consistency check, sensible checks and validation during data entry and processing. The objective is to ensure that the data is not tampered, omitted or unintentionally entered by way of examining data elements and expected relationships.

Best practice: Incorporate during planning, design and programming stage.

v. Intrusion Detectors

These are online applications used to analyse log-in activities, connections, operating system calls and other various command parameters to detect intruders.

Best practice: Use for critical system.

vi. ICT System Performance Monitoring Analysis.

This programme analyses system performance in real time to look for items such as abnormal system response time or abnormal request for resources.

Best practice: Run constantly at the background. Consider adequate lead-time for remedial action.

Improving operational assurance addresses technical issues.

2.6 Operational Assurance Issues

Several issues are addressed and recommended to improve the operational assurance.

(a) Encouragement in the Usage of Locally Developed Security Products

Locally developed security products are preferred over foreign makes to help spur local ICT security development.

(b) Network Auditing

Network auditing methods and tools should be use to ensure the security of the network and to simplify the management of network auditing. Examples of automated auditing methods are the checking and verifying of the data packet from one terminal to the other.

(c) Analysis of the ICT System Activity Log

The ICT system produces the ICT system log. This could be a daily, weekly, monthly or other time-based activity log. It is a detailed log that indicates the user's activity. The log should be checked and reviewed by the ICTSO or by internal or external auditors.

(d) Maintenance Contract

Maintenance clauses should be incorporated into Sales and Purchase Agreement to include provisions for hardware maintenance by the supplier during the warranty period. In some cases it may be necessary to stipulate the service level required.

(e) Standard Operating Procedures

Standard Operating Procedures should be documented and formalised.