Protective Security Management

Security Risk Management

Risk Management
in the Public Sector

Objectives

- Explain the purpose of risk management in the public sector as stipulated in *Arahan Keselamatan* and MyMIS .
- Describe the government's direction to risk management in the public sector
- Understand SIRIM's risk assessment method

Risk Management in the Public Sector

"'Be careful'! All you can tell me is 'be careful'?"

Arahan Keselamatan

- Stipulates that
  - Heads of Government Department are responsible to create and maintain sufficient protective security environment to protect official documents and classified information
  - Protective security covers
    - Personnel security
    - Physical security
    - Document security
    - ICT security

Arahan Keselamatan

- Protective Security
  - Should be carried out throughout the organization
  - Based on
    - real facts
    - financial matters
    - related laws
    - Best practices
    - Risk management

Arahan Keselamatan

- Protective Security Management Plan
  - Public organizations to:
    - Identify risks
    - Undergo risk management based on systematic approach
    - Adopt risk management as the organizational culture
    - Integrate daily routines and management in the security plan

Arahan Keselamatan

- Protective Security Management Plan
  - Public organizations to:
    - Include higher management input in the risk management plan
    - Be committed in the implementation and enforcement of protective security policies, principles and standards
    - Specify levels of protection for official information based on risk assessment results, related laws, Government's directives and existing regulations

Arahan Keselamatan

- Protective Security Management Plan
  - Public organizations to:
    - Safeguard official documents and information at all times
    - Classified documents upon receiving and handling them
    - Ensure the information are not exposed and disclosed to unauthorized users

Arahan Keselamatan

- Security Risk Management in the Public Sector.. Objectives
  - To protect the assets
  - To ensure agencies measure and analyze risk level of all assets
  - To control the identified assets' risks

Arahan Keselamatan

- Security Risk Management in the Public Sector
  - Role of the Heads of Department:
    - To ensure risk assessment is done at least once a year
    - To report the result of the assessment
    - To ensure originators of each classified document are aware about the risks that the documents might possess

MyMIS

Malaysian Public Sector ICT Management Security Handbook (MyMIS)

The Government of Malaysia is committed towards modernising its administrative machinery and enhancing its service delivery mechanisms. The process of ensuring an efficient and effective public sector is being driven by the enabling capabilities of information and communications technology (ICT). The resultant widespread adoption of ICT systems by the public sector has meant that more and more Government agencies are moving towards the paperless work environment where ICT systems have become indispensable for the provision of Government services to citizens. The expansion of ICT systems within the public sector has in turn led to a significant increase in the number of public sector information repositories and other ICT-based installations and assets. The security of these ICT installations and assets are exposed to the vulnerability of open and networked electronic systems. As such agencies now face the additional responsibility of securing ICT-based Government information and systems as well as ensuring that they are available to authorized users.

The Malaysian Public Sector ICT Management Security Handbook (MyMIS) is intended as a reference and guide for public sector personnel in managing security in all public sector ICT installations. MyMIS serves to complement the ICT security measures taken earlier by the Government by way of Pekeliling Am Bil. 3 Tahun 2000 entitled 'Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan' (Government Information and Communications Technology Security Policy Framework) and Surat Pekeliling Am Bil.1 Tahun 2001 entitled 'Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)' (Information and Communications Technology (ICT) Security Incident Reporting Mechanism). While every effort has been made to address all possible ICT security situations in the handbook, there will of course be instances during normal ICT operations where the incidents encountered may not be sufficiently covered in this handbook. In the event of such cases, the best practice available for the relevant situation should be followed.

Needless to say, the MyMIS handbook is the product of close collaboration between MAMPU and various other Government agencies. Their contributions have certainly helped sustain the momentum during periods of waning energy in the course of completing this handbook. MAMPU would therefore like to place on record its appreciation to the following agencies:

- National Security Division, Prime Minister's Department (Bahagian Keselamatan Negara, Jabatan Perdana Menteri)
- Office of the Chief Government Security Officer, Prime Minister's Department (Pejabat Ketua Pegawai Keselamatan Kerajaan, Jabatan Perdana Menteri)
- Ministry of Energy, Communications and Multimedia (Kementerian Tenaga, Komunikasi dan Multimedia)
- Ministry of Defence (Kementerian Pertahanan)
- National Institute of Public Administration (INTAN)

MyMIS Public Sector
ICT Security Risk Management

- Security can be defined as a condition that is free from threats and unacceptable risks and it is 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.

MyMIS Public Sector ICT Security Risk Management

- The objectives of securing ICT assets are:
  - To ensure government operations continuity
  - To minimize disruptions or damage by preventing and minimizing the impact of security incidents
  - To facilitate information sharing
  - To ensure the protection of the information and ICT assets.

MyMIS Public Sector
ICT Security Risk Management

- **Steps in Risk Management**:
  i. formation of a risk management committee
  ii. identifying the risks and threats
  iii. evaluating the risks and threats
  iv. identifying the necessary safeguards and counter measures
  v. managing residual risk
  vi. implementing safeguard and monitoring effectiveness
  vii. undertaking uncertainty analysis

Steps in Risk Management

i. Formation of a risk management committee

- Coordinated by the ICTSO - ICT SECURITY OFFICER
- Best performed by a team of individuals representing the following disciplines:
  - data processing operations management
  - software programming (operating systems & applications)
  - systems analysis
  - data base administration
  - physical security
  - communication networks
  - legal issues

Steps in Risk Management

ii. Identifying the risks and threats

- 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 channeling of resources, which consists of funding, training efforts and future planning.

Steps in Risk Management

ii. Identifying the risks and threats (cont)

- Hence, the proper planning of this activity cannot be overemphasized and should focus on avoiding core business shutdown or, at the least, minimizing disruptions.
- In the public sector, unauthorized disclosure may result in embarrassment where the risk may not be quantifiable in terms of monetary loss.

Steps in Risk Management

ii. identifying the risks and threats (cont)

- ICTSO, Chief Information Officer (CIO) and administrators need to:
  - review the value of the information contained in their systems or information that could be derived from their information systems.
  - determine events or combinations of events that could disrupt business operations
  - establish the priority to the risk elements identified

Steps in Risk Management

iii. Evaluation of risks and threats

- Once identification of risks and threats is completed, the process evolves towards risk evaluation, which involves the collection and analysis of data
- This can be performed by focusing on areas that have the greatest impact on the organization

Steps in Risk Management

iii. **Evaluation of risks and threats** (cont)

- Steps in risk evaluation:
  - quantify the monetary value of a loss
  - determine the potential economic impact of those risks or events
  - estimate the probability of the undesirable events occurring within a specified period of time

Steps in Risk Management

iii. Evaluation of risks and threats (cont)

- Steps in risk evaluation:
  - evaluate the suitable risk treatment options
  - determine whether security safeguards are needed and if so, allocate the cost
  - identify alternative security safeguards and provide recommendations for cost-effective security solutions

Steps in Risk Management

iv. Identification of necessary 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
- Example: it may be effective from an economic and safety viewpoint to impose a new locking mechanism rather than to employ a security guard.

Steps in Risk Management

v. Managing residual risks

- 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.

Steps in Risk Management

vi. Implementing Safeguards and Monitoring Effectiveness

- Once a decision has been made to implement the appropriate safeguards or control, the decision must be followed through.
- Therefore it is required to:
  - Maintain the controls and this process must be seen as ongoing to avoid ineffective safeguards.
  - Periodically assess the controls to improve the controls with possible requirement for re-analysis of risk.

Steps in Risk Management

vii. Uncertainty Analysis

- 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.

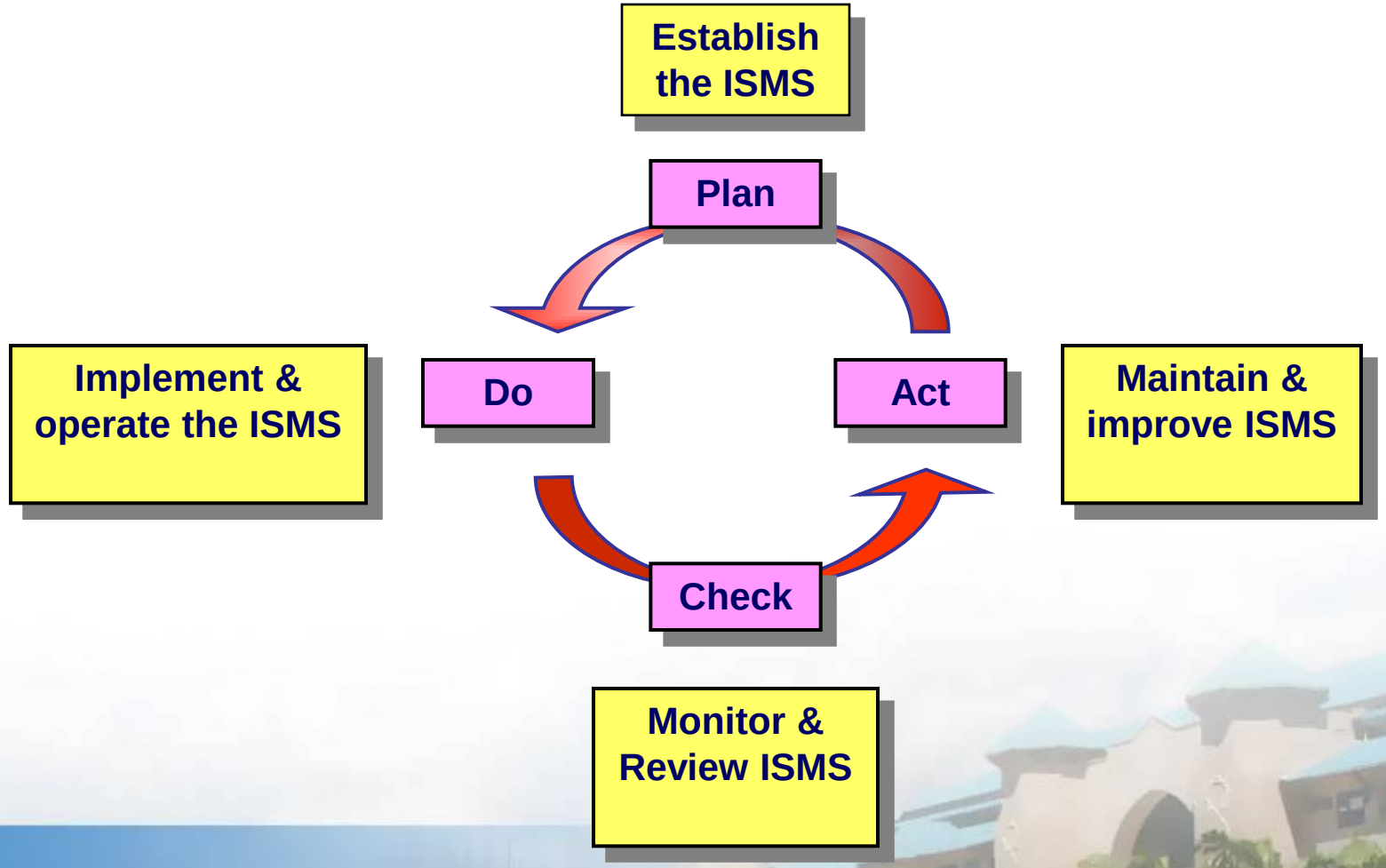
SIRIM's Risk Assessment

- About SIRIM
  - The Standard and Industrial Research Institute of Malaysia (SIRIM) is a government-owned company under the Ministry of Finance.
  - SIRIM QAS International is the first Certification Body in South East Asia to be accredited by United Kingdom Accreditation Service (UKAS) for the Information Security Management System Certification Scheme.

SIRIM's Risk Assessment

- As the Malaysian certification body of ISO 27001 ISMS, SIRIM QAS developed Automated Information Security (AISec) system in 2004, to assist public and private organizations to implement Risk Assessment in their organizations.
- In 2005, an upgrade version of AISec called Information Security Management System Assimilator Application Tool (aISMilator) was deployed.

ISMS PDCA Process



ISMS PDCA Process

- **Plan Phase**
  - **Define the ISMS scope.**
  - **Define an ISMS policy.**
  - **Identify the risks.**
  - **Assess the risks.**
  - **Select control objectives and controls.**
  - **Prepare a Statement of Applicability.**

ISMS PDCA Process

- **Do Phase**
  - **Formulate a Risk Treatment Plan**
  - **Implement the Risk Treatment Plan**
  - **Implement controls selected to meet the control objectives**

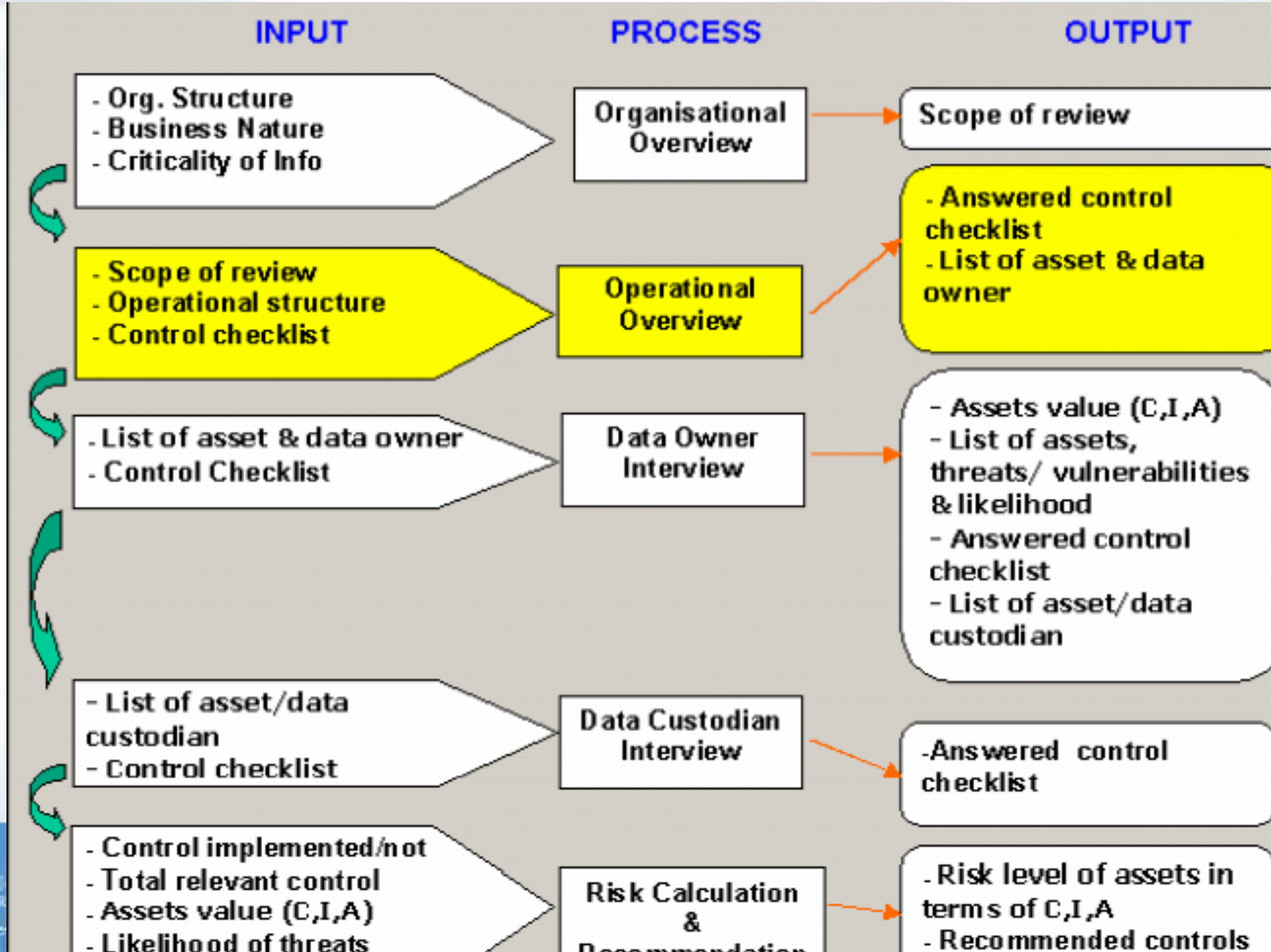
ISMS PDCA Process

- **Check Phase**
  - **Execute monitoring processes**
  - **Conduct internal audits of the ISMS at planned intervals**
  - **Undertake regular reviews of the effectiveness of the ISMS**
  - **Review levels of residual risk and acceptable risk**

ISMS PDCA Process

- **Act Phase**
  - **–Implement improvements identified**
  - **–Take appropriate preventive and corrective actions**
  - **–Communicate the results and actions**
  - **–Ensure improvements meet their intended objectives**

SIRIM's: Risk Assessment methodology



SIRIM's Risk Assessment methodology

- Firstly, the management will be interviewed to outline the scope of their assets
- Secondly, the important assets will be identified and listed
- The possible threats to each asset are also identified
- Based on the identified assets, the management has to identify the owners of the assets, the custodians and also the users or the operators
- The assets' owner, custodian and operator will be interviewed to know whether controls to safeguard the assets are implemented or not (to get the PW value)
- The asset owners will have to rate or value their assets according to CIA (V)
- The owners will also specify the likelihood of threats to happen to each of their assets (frequency of threat to happen) (T)

SIRIM's Risk Assessment methodology

The risk calculation formula:

RISK CALCULATION in AiSec / aISMilator

Risk = V x T x (1-PW)

V = asset value according to CIA

T = frequency of threat to happen

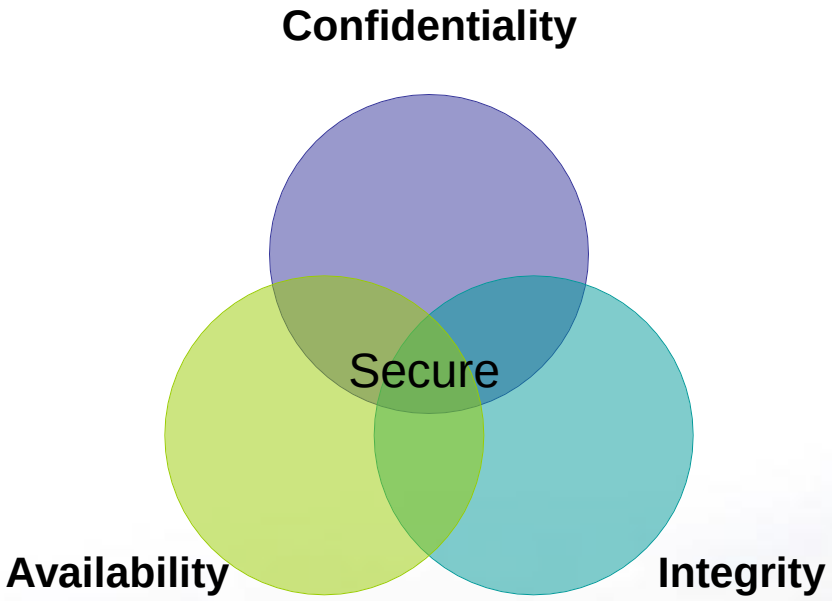
PW = controls implementation/Total Relevant Controls

- Asset Value, V, is the value from 1 – 10 based on confidentiality, integrity and availability
- Threat Value, T, is also the value from 1 – 10 based on the frequency of threats to happen
- The controls (PW) is based on Annex A of ISO27001:2005
- This method is a combination of qualitative and quantitative approach to risk assessment

SIRIM's Risk Assessment methodology

ASSET VALUE

- Based on **CIA**
- **Confidentiality** means Information is not made available or disclosed to unauthorized individuals
- **Integrity** means Safeguarding the accuracy and completeness of information
- **Availability** means Information is accessible and usable upon demand by an authorized entity



END OF SESSION

Topics that have been covered:

- ***Arahan Keselamatan*'s Risk Management**
- **MyMIS' Public Sector ICT Security Risk Management**
- **SIRIM's Risk Assessment**