



**UNIT PEMODENAN TADBIRAN DAN  
PERANCANGAN PENGURUSAN MALAYSIA  
(MAMPU)  
JABATAN PERDANA MENTERI**

**RISK ASSESSMENT GUIDELINE**

**MS ISO/IEC 27001:2007**

**Disediakan/Disemak Oleh:**

.....  
**Nama : Nur Hidayah binti Abdullah  
Jawatan : Ketua Penolong Pengarah  
Kanan,  
Seksyen Pengukuhan ICT  
Tarikh : 21 Jun 2010**

**Diluluskan Oleh:**

.....  
**Nama : Osman bin Abdul Aziz  
Jawatan : Pengarah  
Bahagian Pematuhan ICT  
Tarikh : 21 Jun 2010**

Versi:  
(Tarikh)

Muka Surat:



MAMPU-BPICT-ISMS-P1-008



**RISK ASSESSMENT GUIDELINE**

**HISTORY RECORD**

DATE	VERSION NO. / UPDATE	SECTION / PAGE	DESCRIPTION
10 Jun 2010	1.1	Cover page	Replacement of term MS ISO/IEC 27001:2006 to MS ISO/IEC 27001:2007
		List Of Distribution	Withdrawal of List of Distribution
21 Jun 2010	1.2	Para 6	Adding para 6 d) confirm the risk that remains after the controls for the treatment of risk have been implemented.
		Para 17 Page 33	Adding word "Sulit" in each of report listed in Appendix.

Version:  
(Date)

Page:



**RISK ASSESSMENT GUIDELINE**

**Contents**

1. OBJECTIVE..... 1

2. DEFINITIONS..... 1

3. RELATED DOCUMENTS ..... 3

4. ABBREVIATION ..... 3

5. RISK ASSESSMENT METHODOLOGY ..... 3

6. REQUIREMENT FOR RISK ASSESSMENT ..... 4

7. RISK ASSESSMENT PROCESS ..... 4

8. DESCRIPTION OF THE RISK ASSESSMENT STEPS..... 5

9. RISK ASSESSMENT REVIEW BOUNDARY STATEMENT ..... 8

10. RISK ASSESSMENT TEAM..... 10

11. RISK ASSESSMENT TEAM ROLES AND RESPONSIBILITIES ..... 11

12. ASSETS VALUE RATING ..... 12

13. GUIDELINES ON DECISION WITH RISK IDENTIFIED..... 13

14. MANAGEMENT APPROVAL..... 16

15. WORK FLOW DIAGRAM ..... 17

    a. Establishment of Team..... 17

    b. Risk Assessment Boundary ..... 18

    c. Identification of Assets within RA scope..... 19

    d. Valuation of Assets and Establishment of Dependencies Between Assets  
        ..... 20

    e. Assessment of Threat ..... 21

    f. Assessment of Vulnerability ..... 22

    g. Identification of Existing & Planned Safeguards ..... 23

    h. Analysis of Impact ..... 24

    i. Analysis of Likelihood..... 25

    j. Calculation of Risk ..... 26

    k. Recommendation on Option Handling Risks..... 27

    l. Protection Strategy..... 28

    m. Criteria for risk assessment: (i)..... 29



**RISK ASSESSMENT GUIDELINE**

n. Risk assessment based on criteria (ii):..... 30

o. Risk assessment based on criteria (iii):..... 31

16. RECORDS..... 32

17. APPENDIX ..... 33

    Appendix 1(a) ..... 34

    Appendix 1(b) ..... 36

    Appendix 1(c) ..... 38

    Appendix 1(d) ..... 40

    Appendix 1(e) ..... 51

    Appendix 1(f) ..... 51

    Appendix 1(g) ..... 52

    Appendix 1(h) ..... 53

    Appendix 1(i) ..... 54

    Appendix 1(l) ..... 58

    Appendix 1(k) ..... 61

    Appendix 1(l) ..... 62

    Appendix 1(m) ..... 63

    Appendix 1(n) ..... i

**RISK ASSESSMENT GUIDELINE****1. OBJECTIVE**

The purpose of this document is to provide an understanding for a security risk assessment in information security management systems.

**2. DEFINITIONS**

For the purposes of this risk assessment process, the glossary listed in General Circular Letter No. 5/2006: Public Sector Information Security Risk Assessment Guidelines apply.

No.	Terms	Description
1.	Asset	Anything of value for that may cause losses should it be lost or altered. In MyRAM assets are grouped into data/information, services, software, hardware and people. Refer to section 8, Description Of The Risk Assessment Steps: Identification of Asset (Step S3) for more details.
2.	Asset Depended On	A subject state at the occasion of an event. It means other assets are needed to perform its functions. Refer to section 8, Description Of The Risk Assessment Steps: Valuation Of Assets And Establishment Of Dependencies Between Assets (Step S4) for more details.
3.	Custodian	Immediate personnel who performs the act of keeping safe, maintaining or guarding an asset. Refer to section 8, Description Of The Risk Assessment Steps: Identification of Asset (Step S3) for more details.
4.	Dependent Assets	A subject state at the effect of an event. It means the asset output is needed to support other asset(s) to function. Refer to section 8, Description Of The Risk Assessment Steps: Valuation Of Assets And Establishment Of Dependencies

**RISK ASSESSMENT GUIDELINE**

		Between Assets (Step S4) for more details.
5.	Owner	Immediate legal possessor in-charge of an asset. Refer to section 8, Description Of The Risk Assessment Steps: Identification of Asset (Step S3) for more details.
6.	Risk	In general is a possibility of meeting danger or suffering harm or loss, especially from lack of proper care. Refer to section 8, Description Of The Risk Assessment Steps: Calculation of Risk (Step S6) for more details.
7.	Risk Assessment	Evaluation to the possibilities of meeting danger or suffering harm or loss of ICT assets.
8.	Threat	Identification for any potential event or act that could cause one or more of the following to occur: unauthorized disclosure, destruction, removal, modification or interruption of sensitive or critical information, assets or services. A threat can be natural, deliberate or accidental. Refer to section 8, Description Of The Risk Assessment Steps: Assessment of Threat (Step S5) for more details.
9.	Vulnerability	Characteristic of any asset which increases the probability of a threat event occurring and causing harm in terms of confidentiality, availability or integrity that may increases the severity of the effects of a threat event if it occurs. Refer to section 8, Description Of The Risk Assessment Steps: Assessment of Vulnerability (Step S6) for more details.



### 3. RELATED DOCUMENTS

This risk assessment exercise makes reference to the following general circular and guidelines:

- a) General Circular No. 3/2000: Government ICT Security Framework;
- b) General Circular Letter No. 5/2006: Public Sector Information Security Risk Assessment Guidelines;
- c) The Malaysian Public Sector Information Security Risk Assessment Methodology;
- d) The Malaysian Public Sector Information Security Risk Assessment Methodology Handbook; and
- e) Malaysian Administrative Modernisation and Management Planning Unit ICT Security Policy

### 4. ABBREVIATION

SPSS	Seksyen Pengurusan Serangan Siber
SPS	Seksyen Pemantauan Siber
MyRAM	Malaysian Public Sector Information Security Risk Assessment Methodology
MAMPU	Malaysian Administrative Modernisation and Management Planning Unit

### 5. RISK ASSESSMENT METHODOLOGY

Risk assessment is a method for determining what threats exists to a specific asset and the associated risk level of that threat. Establishing risk level provides organisation with the information required to select appropriate safeguards and control measures for lowering the risk to an acceptable level.



**RISK ASSESSMENT GUIDELINE**

MAMPU has developed the Malaysian Public Sector Information Security Risk Assessment Methodology or MyRAM to assist public sector organisations in identifying and managing ICT security risks. MAMPU will utilise MyRAM to ensure the integrity of Government information and assets in providing efficient and effective services to all customers.

Refer the Risk Assessment Report that implements the methodology described in section 7. Risk Assessment Process.

**6. REQUIREMENT FOR RISK ASSESSMENT**

The risk assessment shall be carried out to:

- a) take account of changes to organization structure and new assets;
- b) consider new threats and vulnerabilities; and
- c) confirm that controls remain effective and appropriate;
- d) confirm the risk that remains after the controls for the treatment of risk have been implemented.

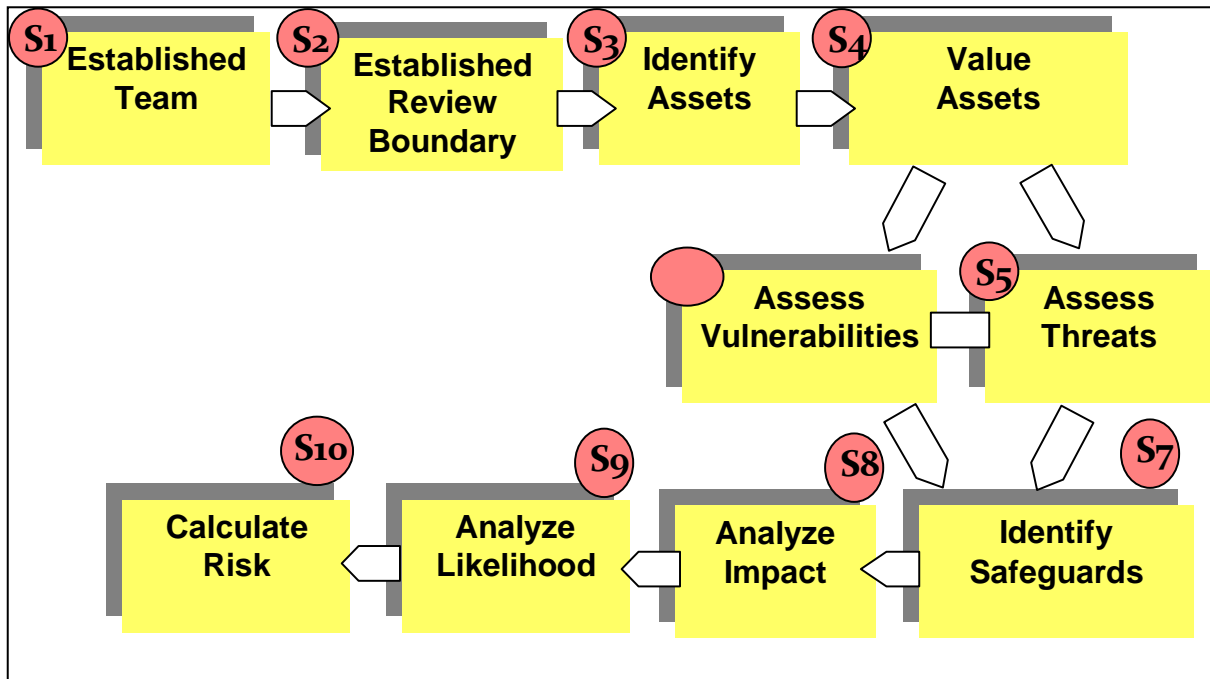
**7. RISK ASSESSMENT PROCESS**

The approach adopted strictly the risk assessment process outlined in MyRAM document, starting from Establishment of Team step until Step 10, which is Calculation of Risk. These steps are related to each other because input for one step of the risk assessment activity may be taken from the output of one of its previous steps. Figure 1 below shows the ten (10) steps in a risk assessment exercise.





**RISK ASSESSMENT GUIDELINE**



**Figure 1: Risk Assessment (RA) Process**

**8. DESCRIPTION OF THE RISK ASSESSMENT STEPS**

Below is the overview of the steps in the risk assessment process, its description and the subtasks involved in each step.

**Table 1: Description of RA Steps**

Steps	Description	Task(s) Involved
Establishment of Team (S1)	Creates a basic component of a risk assessment exercise. The team members that possess vast knowledge of the organization are identified. The schedule and logistics are established to ensure the smoothness of the whole	a) Identify the assessment team members b) Draw up Tasking Schedule List Output template: Refer to Appendix 1(a).



**RISK ASSESSMENT GUIDELINE**

	exercise.	
Establishment of Review Boundary (S2)	Determines the scope of the risk assessment process. The final scope will be submitted to the senior management. Once it has received approval, the assessment team will collect all the relevant materials and information.	<ul style="list-style-type: none"> <li>a) Identify the scope of the risk assessment</li> <li>b) Obtain approval from management</li> <li>c) Gather information related to the review boundary</li> <li>d) Revisit Step 1 as necessary</li> </ul> <p>Output template: Refer to Appendix 1(b).</p>
Identification of Assets (S3)	Identifies all the assets which are within the scope of the risk assessment boundary.	<ul style="list-style-type: none"> <li>a) Identify related assets</li> <li>b) Group and classify assets</li> <li>c) Identify assets' owners and custodians</li> <li>d) Verify and Validate the Findings of the Questionnaires</li> </ul> <p>Output template: Refer to Appendix 1(c).</p>
Valuation of Assets and Establishment of Dependencies Between Assets (S4)	Assigns semi-quantitative values to the assets and determines those assets' dependencies.	<ul style="list-style-type: none"> <li>a) Identify dependencies associated with the assets</li> <li>b) Assign a quantified value to each asset</li> </ul>



**RISK ASSESSMENT GUIDELINE**

		<p>c) Verify and Validate the Findings of the Questionnaires</p> <p>Output template: Refer to Appendix 1(d).</p>
Assessment of Threat (S5)	Determines types of threats associated with the assets, and their relative levels.	<p>a) Create a generic threat profile</p> <p>b) Identify all relevant threats to assets</p> <p>c) Verify and Validate the Findings of the Questionnaires</p> <p>Output template: Refer to Appendix 1(f).</p>
Assessment of Vulnerability (S6)	Identifies all potential vulnerabilities which may be exploited by threats. In addition, it will rate the relative vulnerability exposure levels.	<p>a) Identify potential vulnerabilities exploited by threats</p> <p>b) Verify and Validate the Findings of the Questionnaires</p> <p>Output template: Refer to Appendix 1(g).</p>
Identification of Existing & Planned Safeguards (S7)	Identifies all types of existing & planned safeguards which have been or will be deployed to protect the assets.	<p>a) Review existing and planned safeguards for protecting the assets</p> <p>b) Verify and Validate the Findings of the Questionnaires</p>
Version: (Date)		Page:

**RISK ASSESSMENT GUIDELINE**

		Output template: Refer to Appendix 1(h).
Analysis of Impact (S8)	Quantifies the business impacts of the assets accordingly. The calculation will be based on the assets' values & business loss.	<ul style="list-style-type: none"> <li>a) Determine the business loss</li> <li>b) Determine the impact levels</li> <li>c) Verify and Validate the Findings of the Questionnaires</li> </ul> Output template: Refer to Appendix 1(i).
Analysis of Likelihood (S9)	Ascertains the likelihood of threats & vulnerabilities that may happen, with or without safeguard(s) in place.	<ul style="list-style-type: none"> <li>a) Determine the likelihood of threats &amp; vulnerabilities that may happen</li> <li>b) Verify and Validate the Findings of the Questionnaires</li> </ul> Output template: Refer to Appendix 1(j).
Calculation of Risk (S10)	Calculates the risk level for each asset, based on the impact value & likelihood results.	<ul style="list-style-type: none"> <li>a) Calculate the risk level for each asset</li> </ul> Output template: Refer to Appendix 1(k).

**9. RISK ASSESSMENT REVIEW BOUNDARY STATEMENT**

**RISK ASSESSMENT GUIDELINE**

The review boundary is agreed as:

MAMPU Senior Management has agreed in the Senior Management Meeting MAMPU No. 26/2008 dated 17 September 2008 that the scope of ISMS implementation is as follows:

Information Security Management System (ISMS) to provide information security services include the following:

- a) monitoring network security government agencies under the control of PRISMA; and
- b) handling incidents Government agencies (GCERT).

Based on the ISMS scope above, the business functions confined by the scope are:

- a) To detect proactively and reactively cyber threats via ICT infrastructure monitoring system remotely 24 x 7 and to provide early warning to agencies under the purview of PRISMA to reduce ICT security incidents and their impact;
- b) To implement scanning on Public Sector ICT infrastructure and ICT assets remotely to assist in identifying vulnerabilities and to provide remedial counter measures;
- c) To conduct penetration testing on 15 PRISMA agencies and to conduct Security Posture Assessment upon request;
- d) To analyse cyber threats, forecast trends and provide early warning of expected cyber attacks;
- e) To analyse threats / vulnerabilities; and
- f) To manage Public Sector ICT security incident response handling.
- g) To analyse threats / vulnerabilities;
- h) To manage Public Sector ICT security incident response handling;



## 10. RISK ASSESSMENT TEAM

The Risk Assessment (RA) team comprised of personnel from ICT Compliance Division. The members will gather and analyze information as well as produce the risk assessment's final report. Some other roles and responsibilities include:

- a) Stating roles and responsibilities in general for all team members to set the participation expectation for all members;
- b) Gathering, analyzing and reporting the findings of the risk assessment exercise;
- c) Making sure that all tasks are performed properly; and
- d) Coordinating logistics and schedules for the exercise.

Below is an RA team structure:

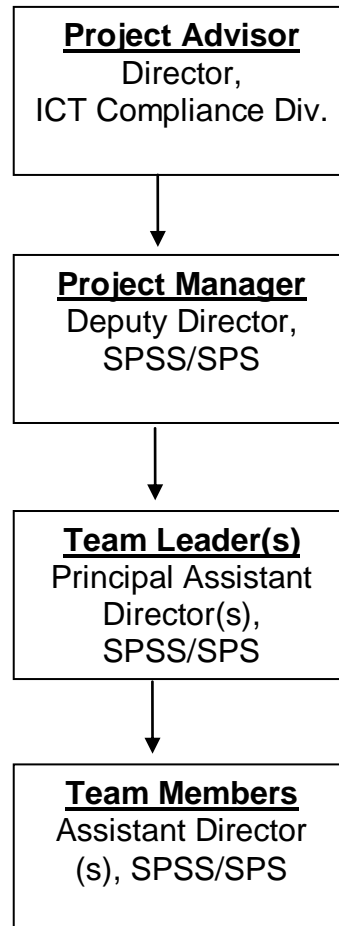


Fig 1: Risk Assessment Team Structure

## 11. RISK ASSESSMENT TEAM ROLES AND RESPONSIBILITIES

The roles and responsibilities for the RA team are as follows:

Project Advisor:

- Provide expert advice for the risk assessment activity.

b) Project Manager:

- Manage the risk assessment activities;
- Ensure timely completion; and



**RISK ASSESSMENT GUIDELINE**

- Conduct reviews of all output and documents before they presented to Project Advisor.
- c) Team Leader:
- Regularly ascertain the scope of work;
  - Evaluate results, assess gaps and provide feedback; and
  - Performs all tasks defined under each risk assessment step.
- d) Team Members:
- Perform all tasks defined under each risk assessment step.

Refer Appendix 1 (a): Project Team list report format.

**12. ASSETS VALUE RATING**

The RA team has to establish value rating for the requirements of ICT security, namely Confidentiality (C), Integrity (I) and Availability (A) base on the subjective levels of Low, Medium and High. In rating the sensitivity of each asset, RA team shall use the following guidelines:

- a) **Confidentiality.** The impact of unauthorized disclosure of confidential information can result in loss of stakeholder confidence and embarrassment.
- b) **Integrity.** This is the impact on the system that would result from deliberate, unauthorized or inadvertent modification of the asset.
- c) **Availability.** This is the impact as a result from deliberate or accidental denial of the asset's use.

Each asset must be evaluated according to their respective confidentiality, integrity and availability levels. Refer Appendix 1 (d): Summary of Asset Value and Dependencies Report Format.

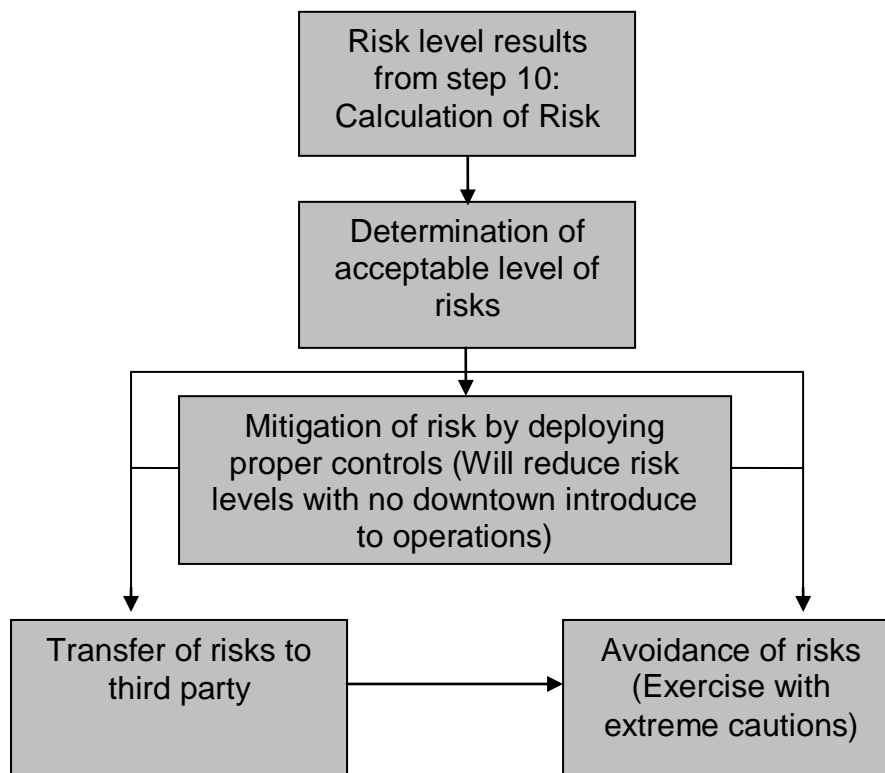




### 13. GUIDELINES ON DECISION WITH RISK IDENTIFIED

The output of the risk assessment process is input to a decision-making process which determines whether to accept, reduce, transfer or avoid risks identified.

The RA team shall establish the High-Level Recommendation to obtain written approval or acknowledgement from the ISMS Committee in handling risks. At this point the RA team will define what is to be done after obtaining the risk level for all identified assets. During this stage, decisions of whether to accept, reduce, transfer, or avoid risks that have identified must be made only after the risk assessment exercise has been completed.

Basically decision making of whether to accept, reduce, transfer, or avoid risks level are based on the factors of time, money, manpower and equipment. Determination of option on handling the risk can be done by following the steps in figure 2 below.



	MAMPU-BPICT-ISMS-P1-008	
<b>RISK ASSESSMENT GUIDELINE</b>		

### Figure 2: Decision on Options in Handling Risk

As shown in figure 2 above, the first step to make high-level recommendations is by getting the result of the risks levels from Step 10. Then determine what level of risk that is acceptable by RA Team. Refer Section 4: Criteria for Accepting Risks.

In the High-Level Recommendations, there are two (2) outputs:

- i) Decision on Option; and
- ii) Protection Strategy.

#### Decision on Options

In the 'Decision on Option', the RA team will propose to the management of ICT Compliance Division whether to accept, reduce, transfer, or avoid the risk level of a particular threat that exists in a specific asset. The descriptions for each decision options are as follows:

- a) **Accept:** to accept risks associated with the assets without implementing any safeguards or controls.
- b) **Reduce:** to implement controls to mitigate risks. When risks are high, it is essential to reduce the risk levels.
- c) **Transfer:** to transfer risks to another entity.
- d) **Avoid:** to avoid risks when there is no other available options.

The RA team shall accept, reduce, transfer or avoid risk for the following criteria:

- a) Check and assess whether the risk can be accepted or not. The RA team could propose to the management to accept all assets with risk levels of Low and there is no immediate action taken to protect the asset; and
- b) If the risks cannot be accepted, then check and assess whether they should be reduced, transferred or avoided.

Version: (Date)		Page:
--------------------	--	-------

**RISK ASSESSMENT GUIDELINE**

- i. If the implication of the risks is catastrophic and critical (High), then the risks should be reduced. Risk reduction shall be achieved through the implementation of the following components: operational, procedural, physical, personnel, and technical security to ensure that critical operations continue with no downtime; and
- ii. If the implication of the risks is of an average criticality (Medium), then the risks may also be transferred on the following conditions.
  - Risks must be transferred fairly. Risks can be shared by the asset owners and third parties. For example, if a communication line breaks down, and the Service Level Agreement (SLA) with the provider of the line states that the line will be available within 24 hours; unforeseen disasters that may strike the third party is a shared risk the agency is prepared to take; and
  - The risks should be avoided altogether if there are no reasonable controls that can be implemented for risk mitigation. Example, to avoid risks is to totally disconnect the system.

Refer to Appendix 1(l): Decision on Options for more details.

**Protection Strategy**

The RA team now develops a protection strategy to be presented to the management. For 'Protection Strategy', the RA team needs to look whether the current safeguards are sufficient to protect the assets or not. If the current safeguards are not sufficient, SPSS and SPS shall select appropriate control objectives and controls available in Annex A, ISO/IEC 27001:2005 ISMS Requirements. Justification must be elaborated to support reasoning to implement the safeguard.

Refer to Appendix 1(m): Protection Strategy for more details.



MAMPU-BPICT-ISMS-P1-008



**RISK ASSESSMENT GUIDELINE**

**14. MANAGEMENT APPROVAL**

The document presented to ISMS Committee for approval on risk analysis information has the following items:

- a) Any terms and concepts that may be new or different - for example, assets, threats, risk and risk profile - are explained.
- b) The following data should be presented to and summarized for managers:
  - i. Threat, risk and vulnerability information for each critical asset;
  - ii. Composite, analyzed results of the risk analysis. These should be presented in a table or graphical easy-to-read information. Each identified level of risk should also state clear implications;
  - iii. Protection strategy practices and organisational vulnerabilities grouped by practice areas; and
  - iv. Justification on planned safeguards.

Refer to Appendix 1(n): Protection Strategy for more details.

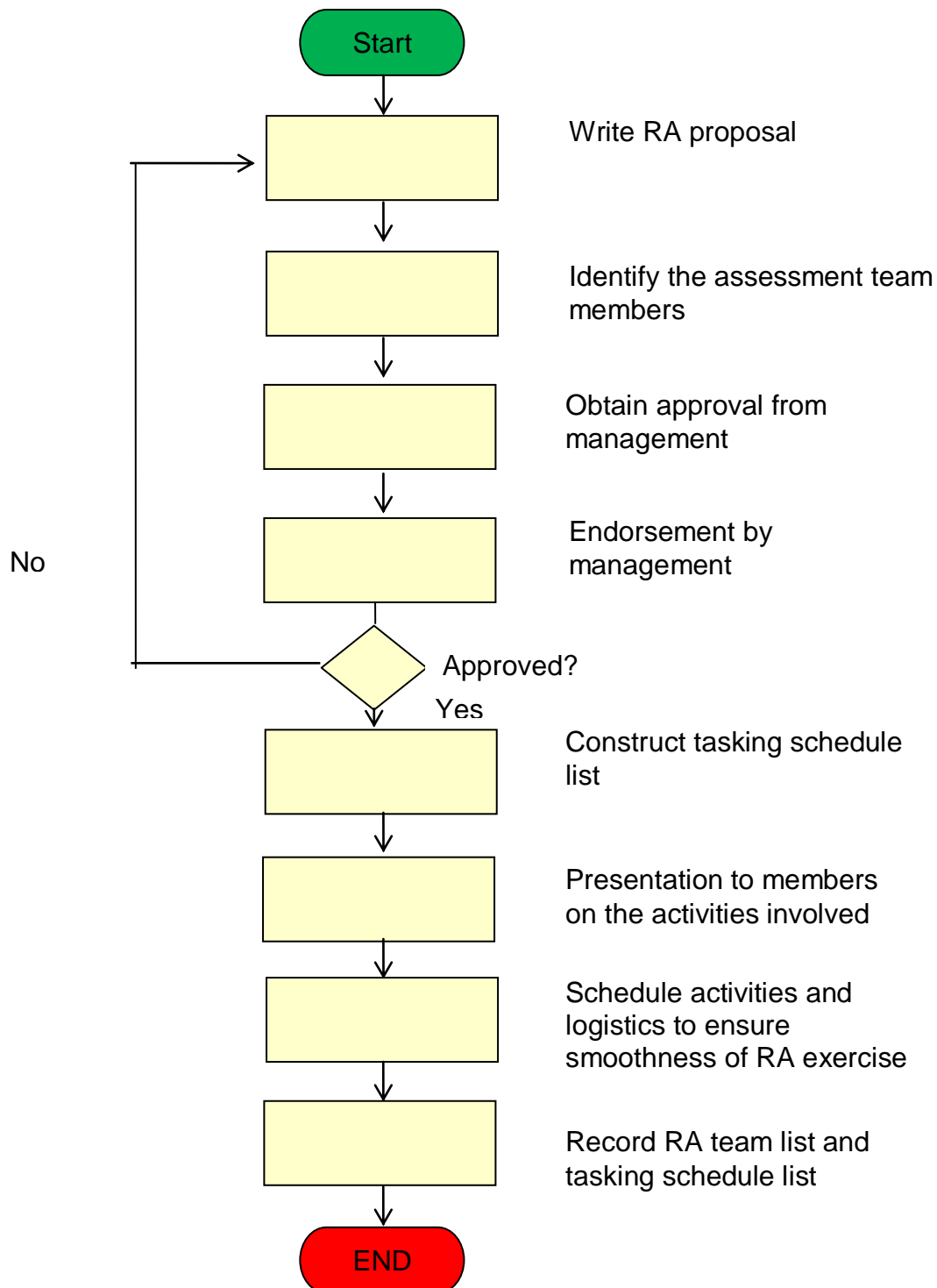
Version:  
(Date)

Page:



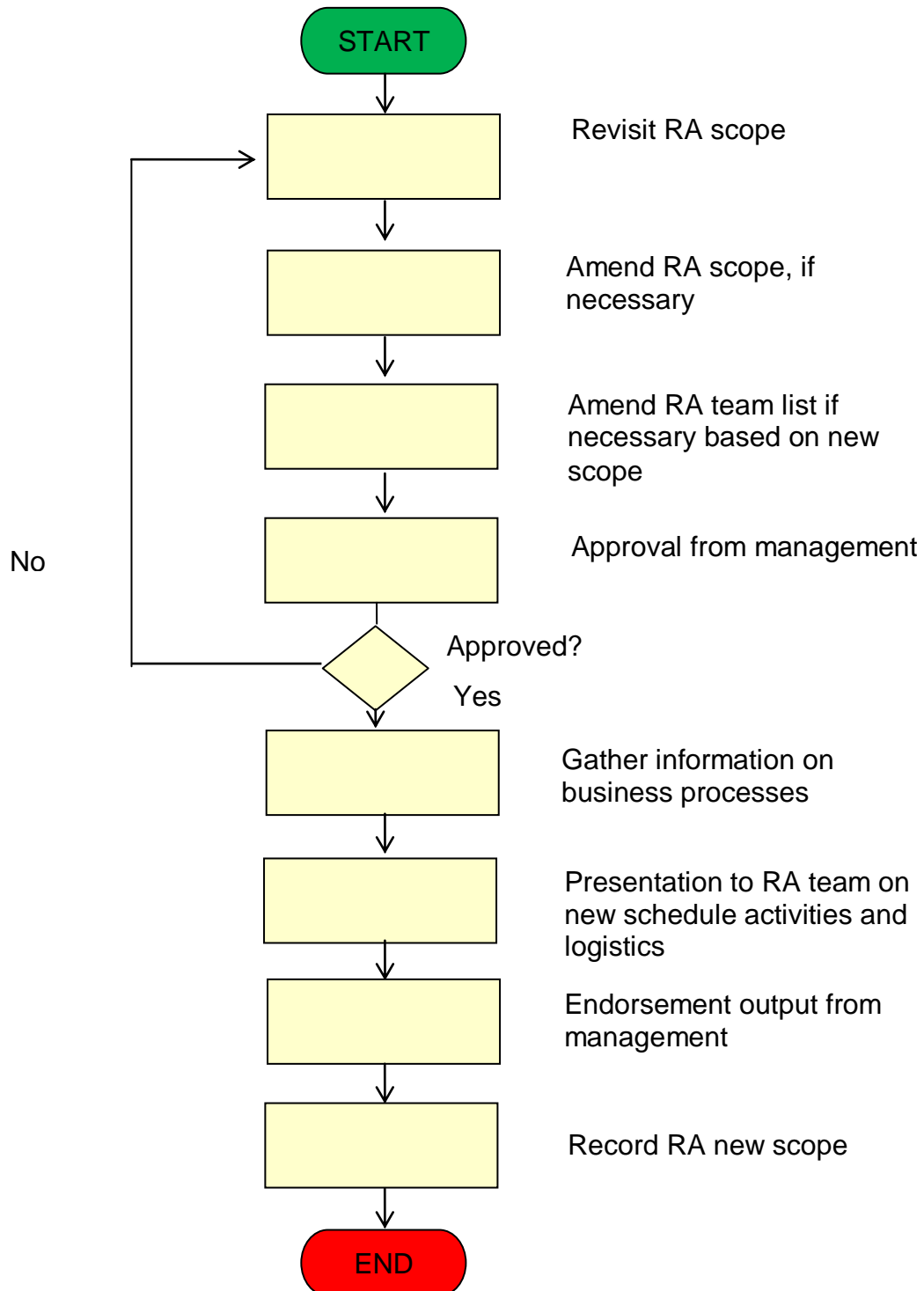
### 15. WORK FLOW DIAGRAM

#### a. Establishment of Team





b. Risk Assessment Boundary

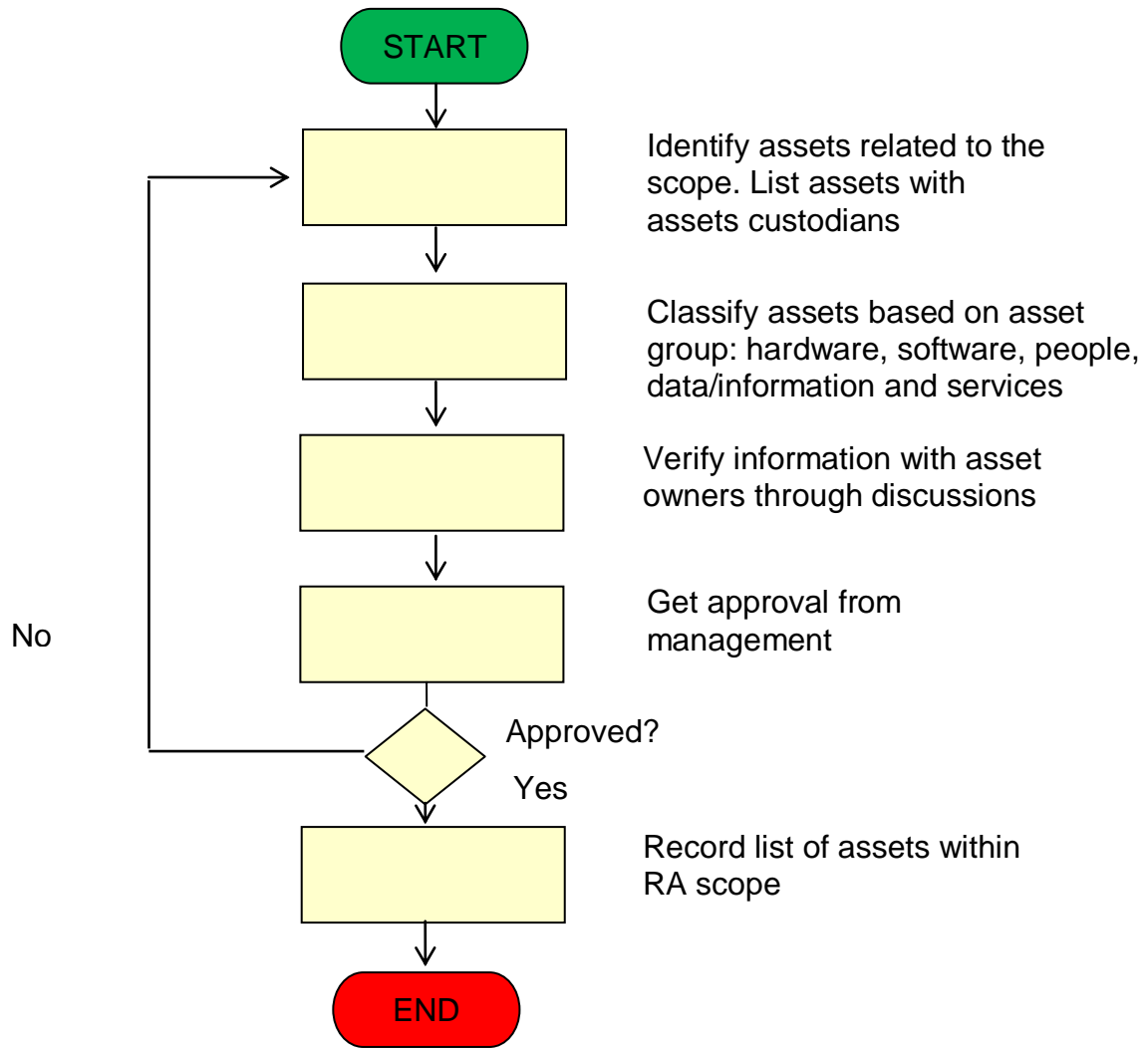






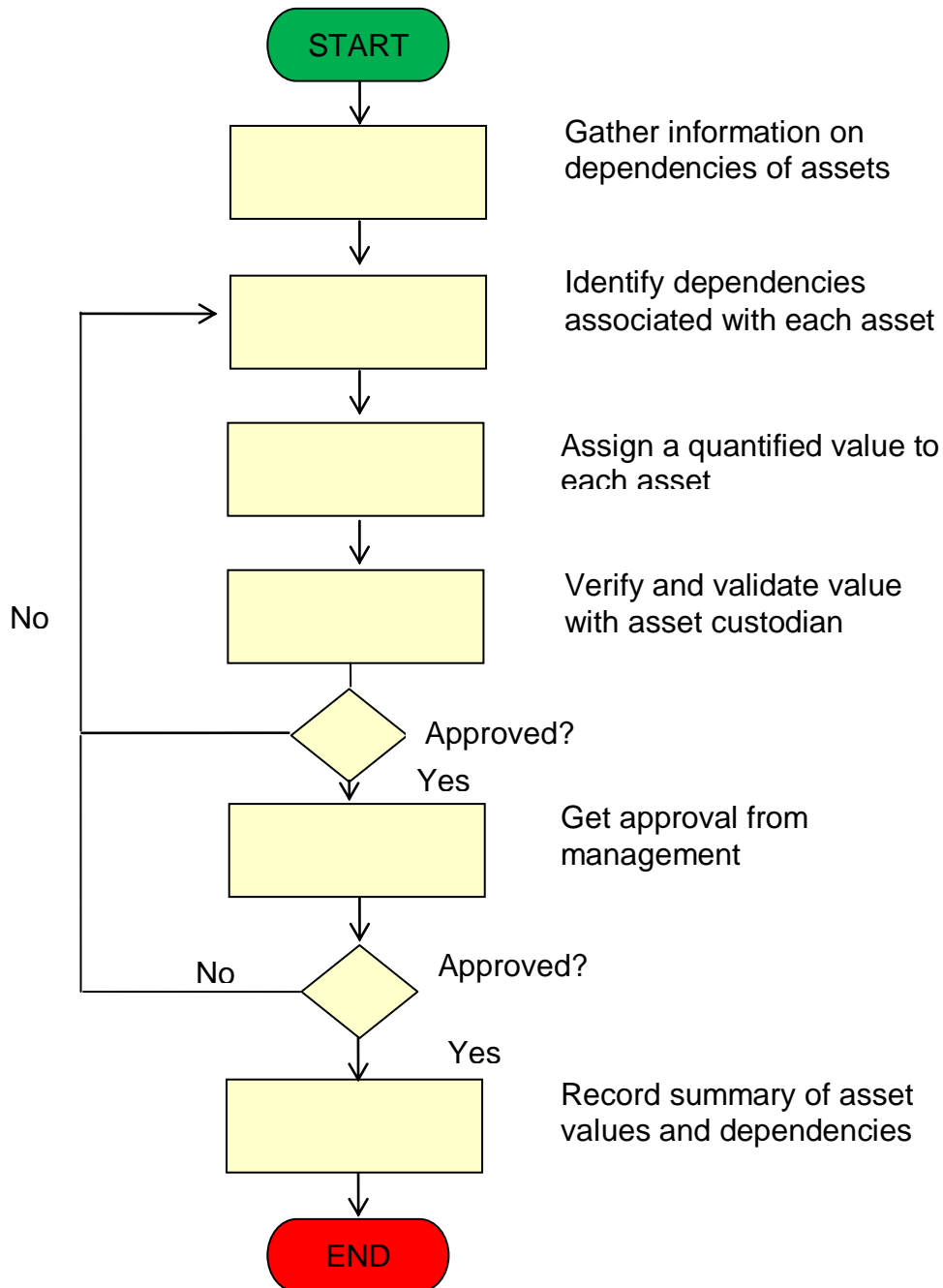
**RISK ASSESSMENT GUIDELINE**

c. Identification of Assets within RA scope



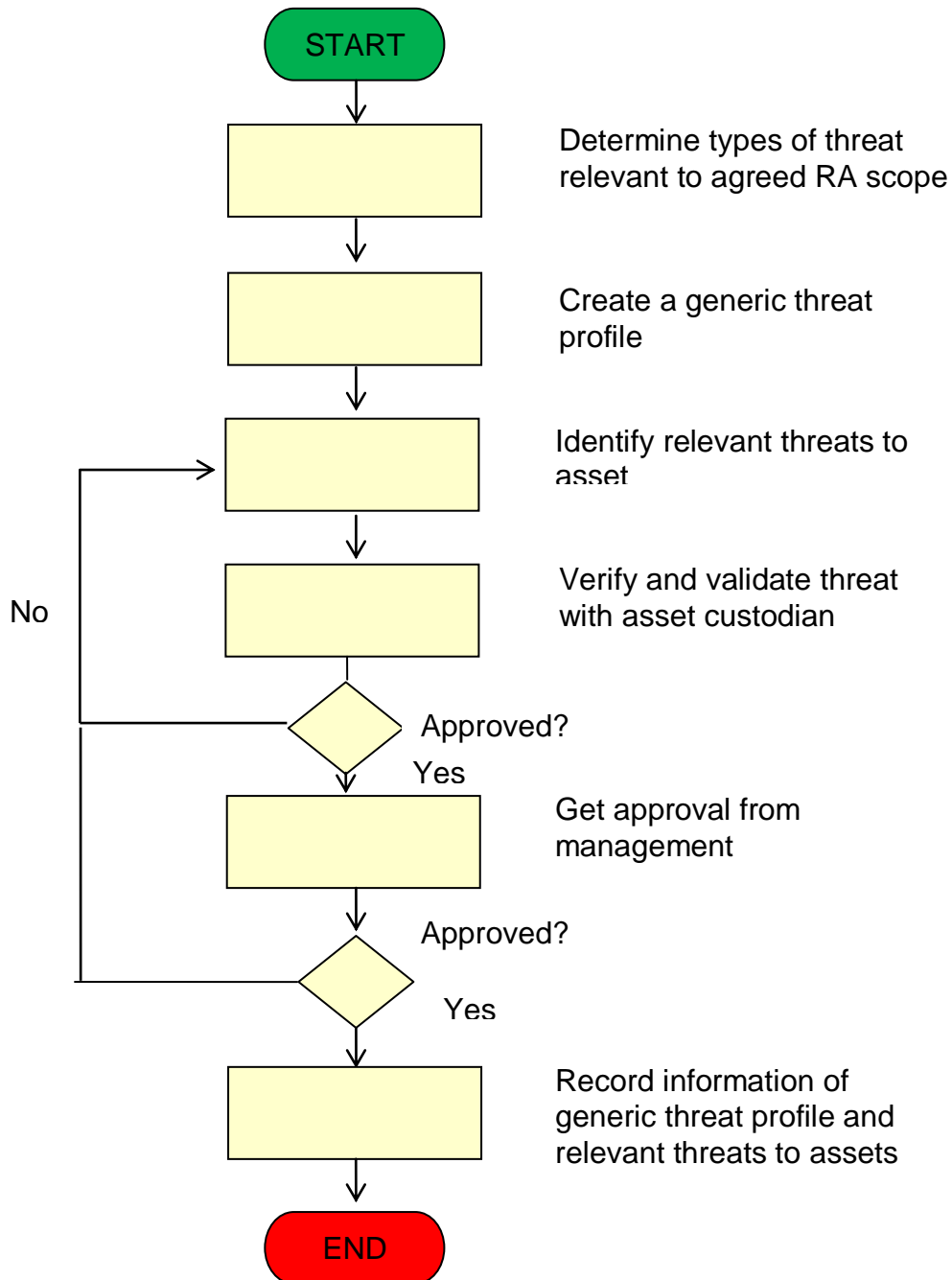


d. Valuation of Assets and Establishment of Dependencies Between Assets



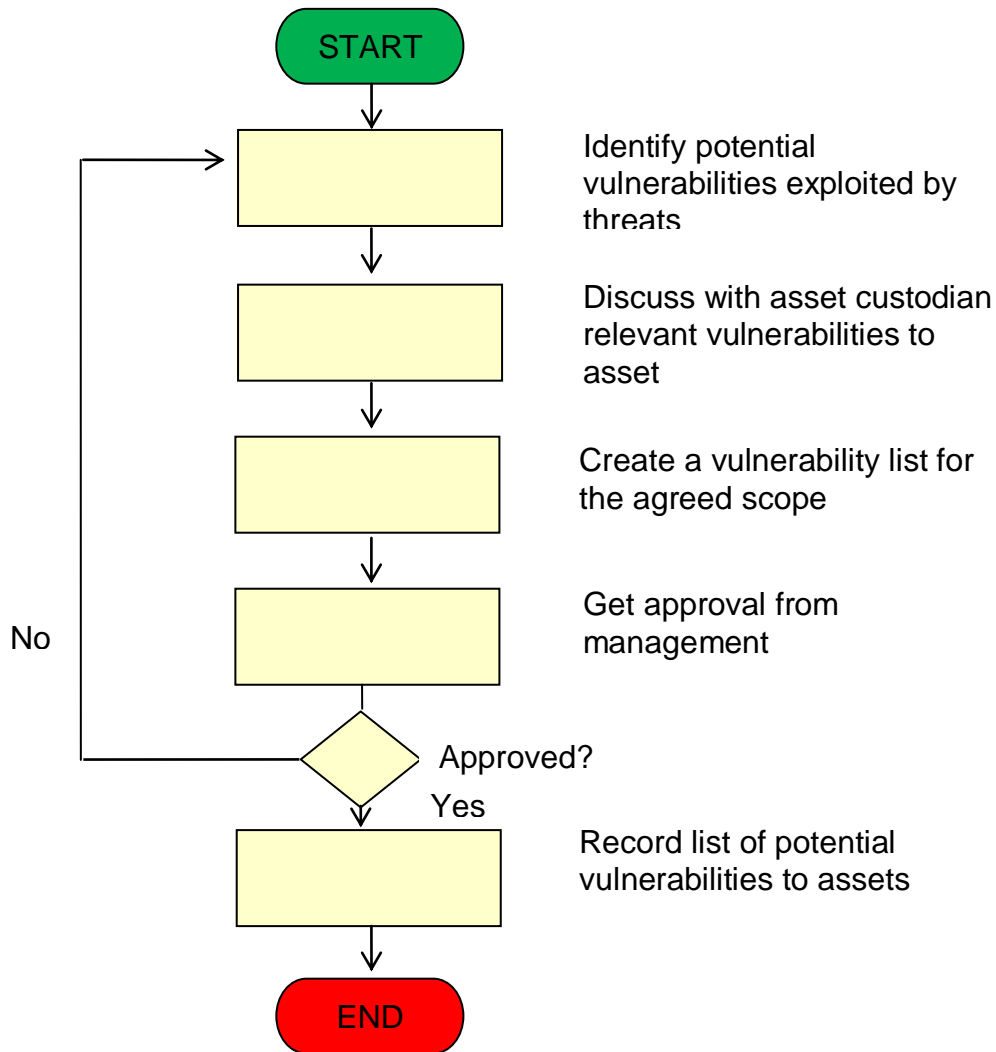


e. Assessment of Threat



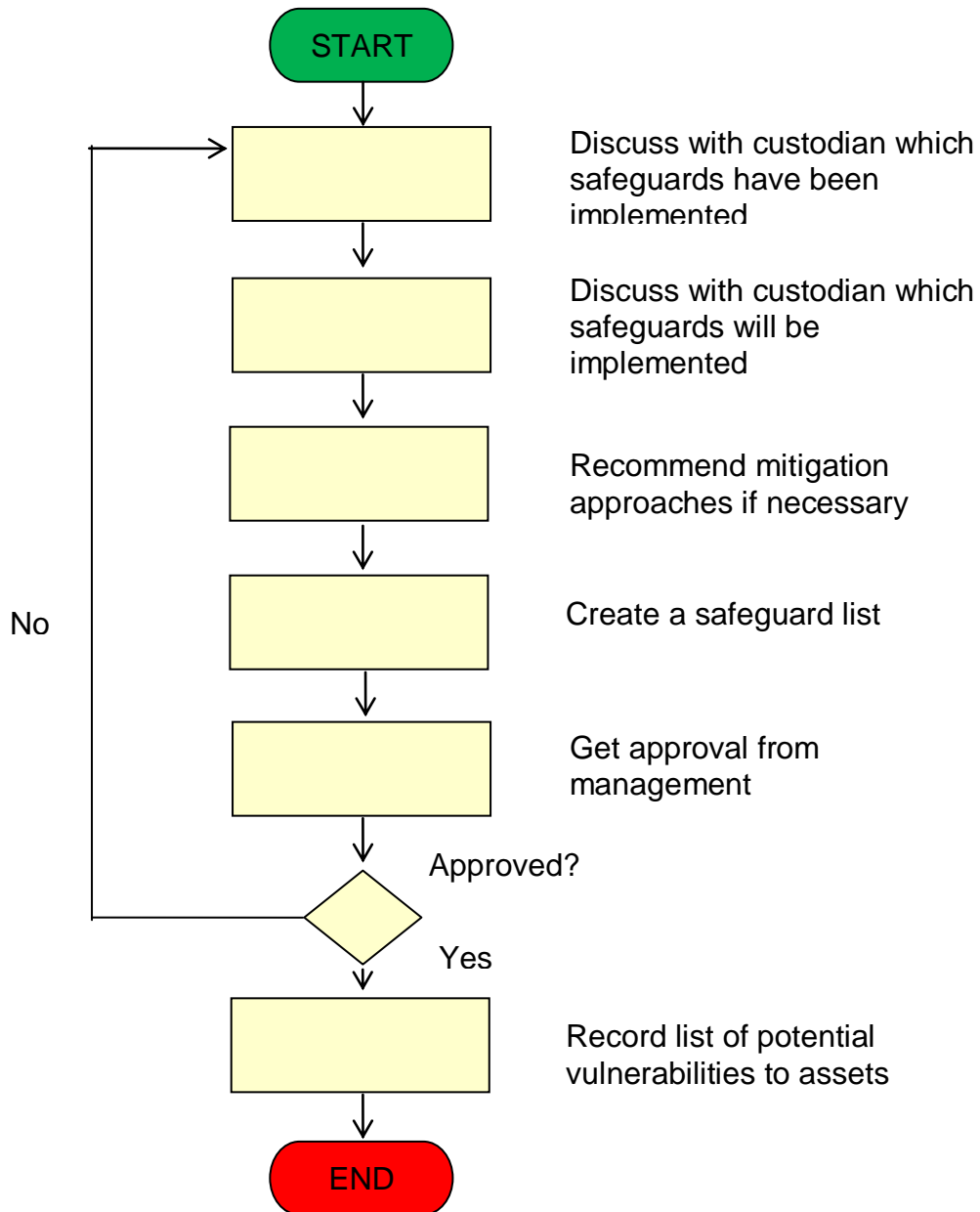


f. Assessment of Vulnerability



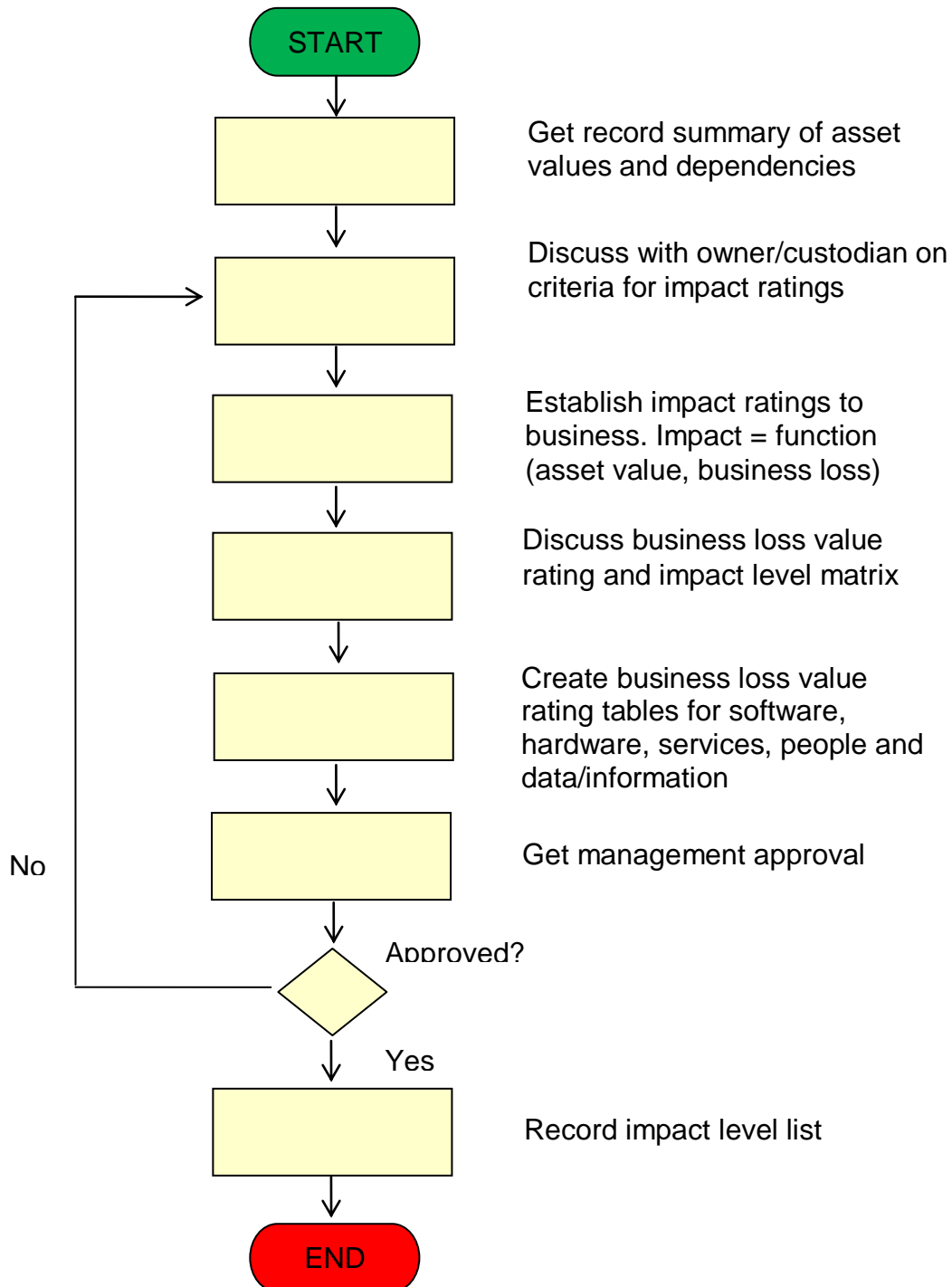


g. Identification of Existing & Planned Safeguards



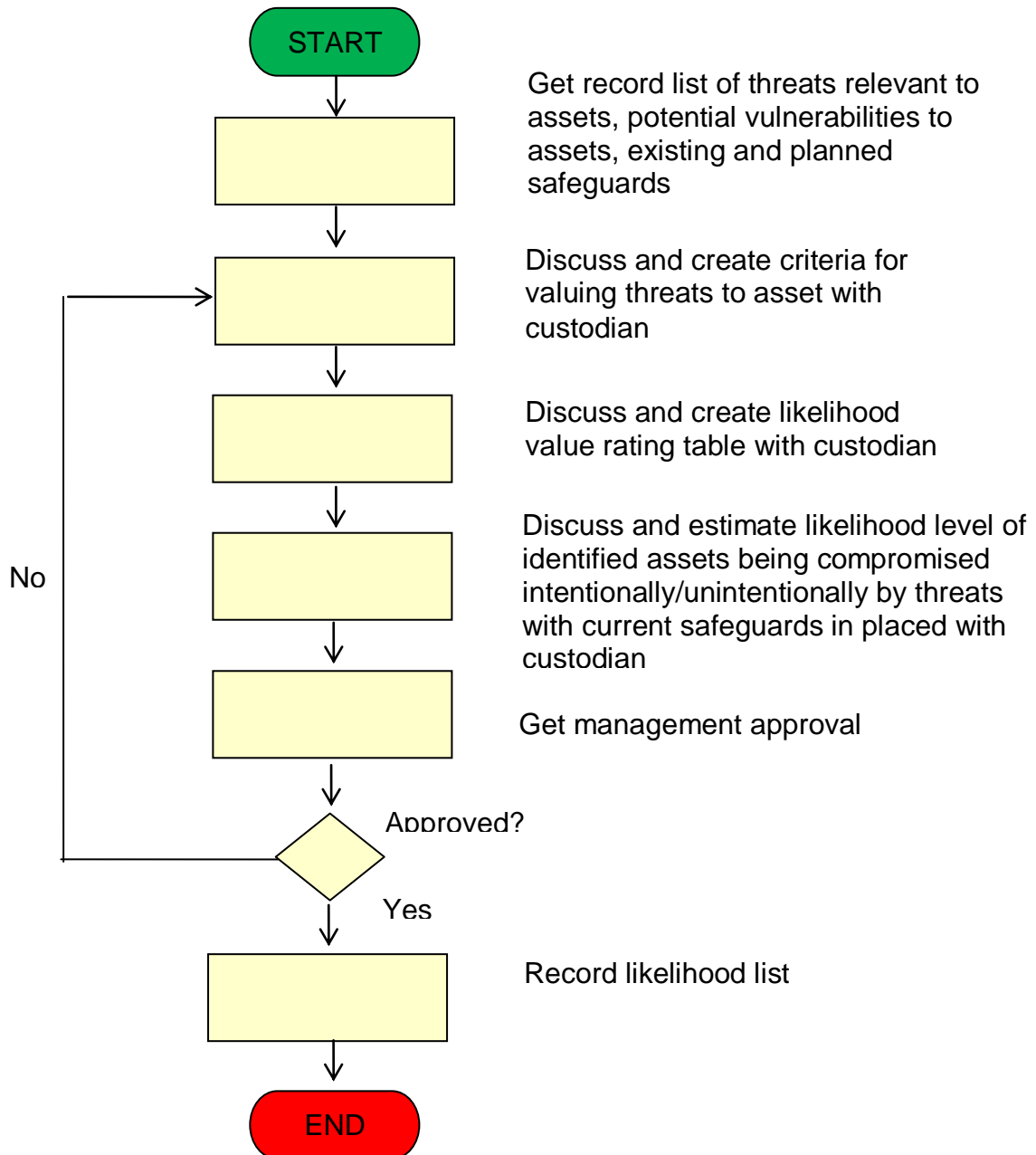


## h. Analysis of Impact





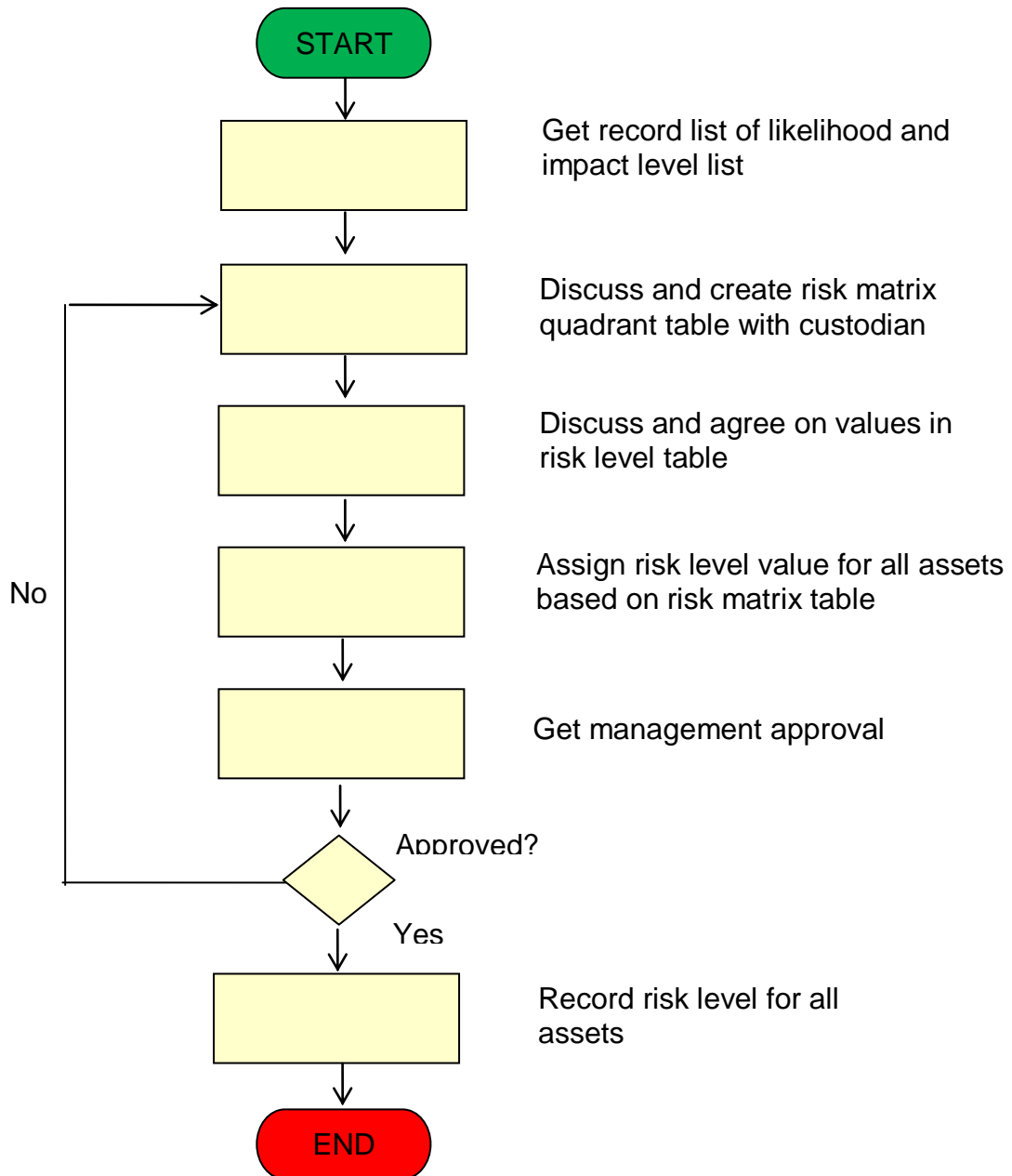
i. Analysis of Likelihood





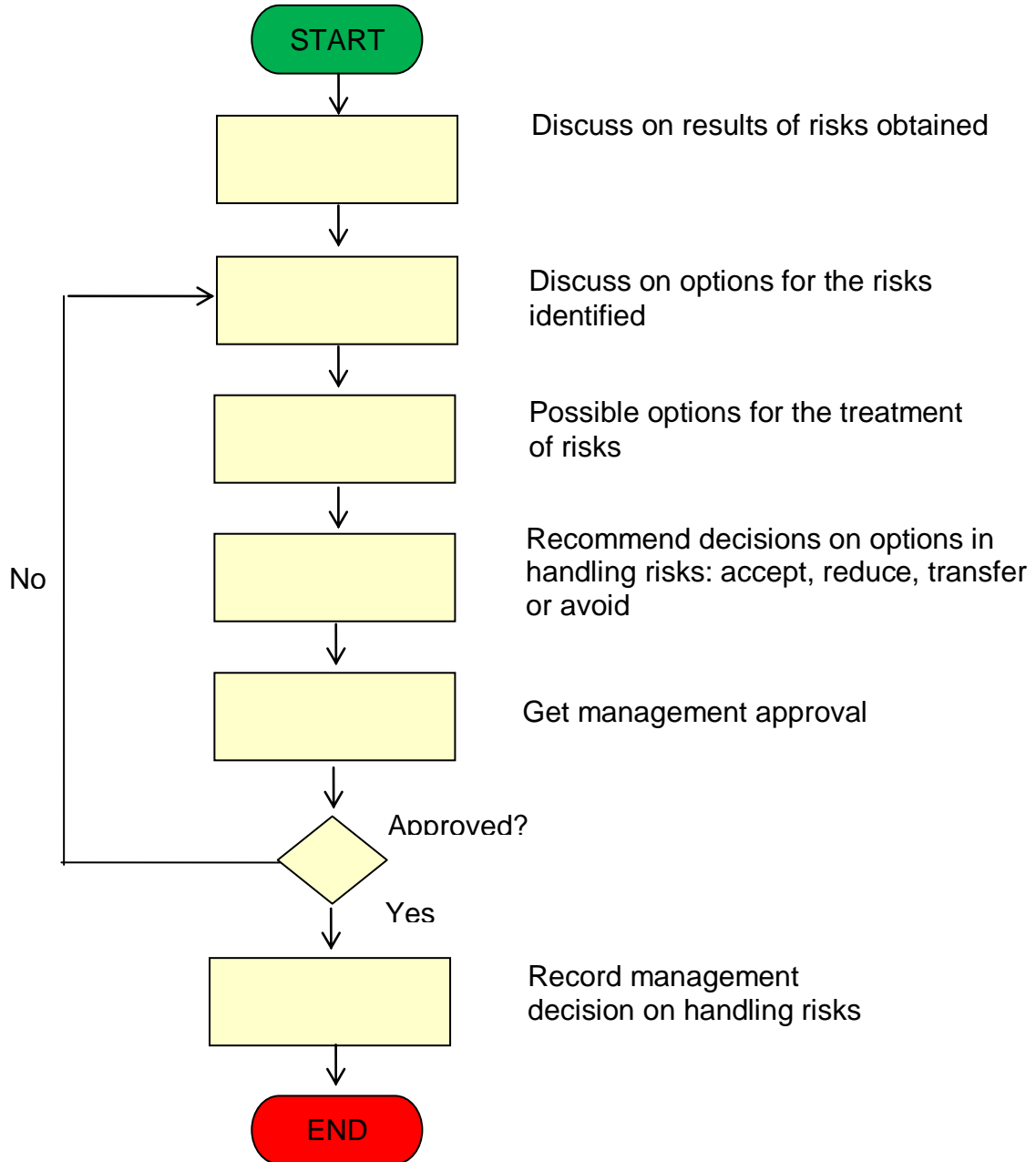


j. Calculation of Risk





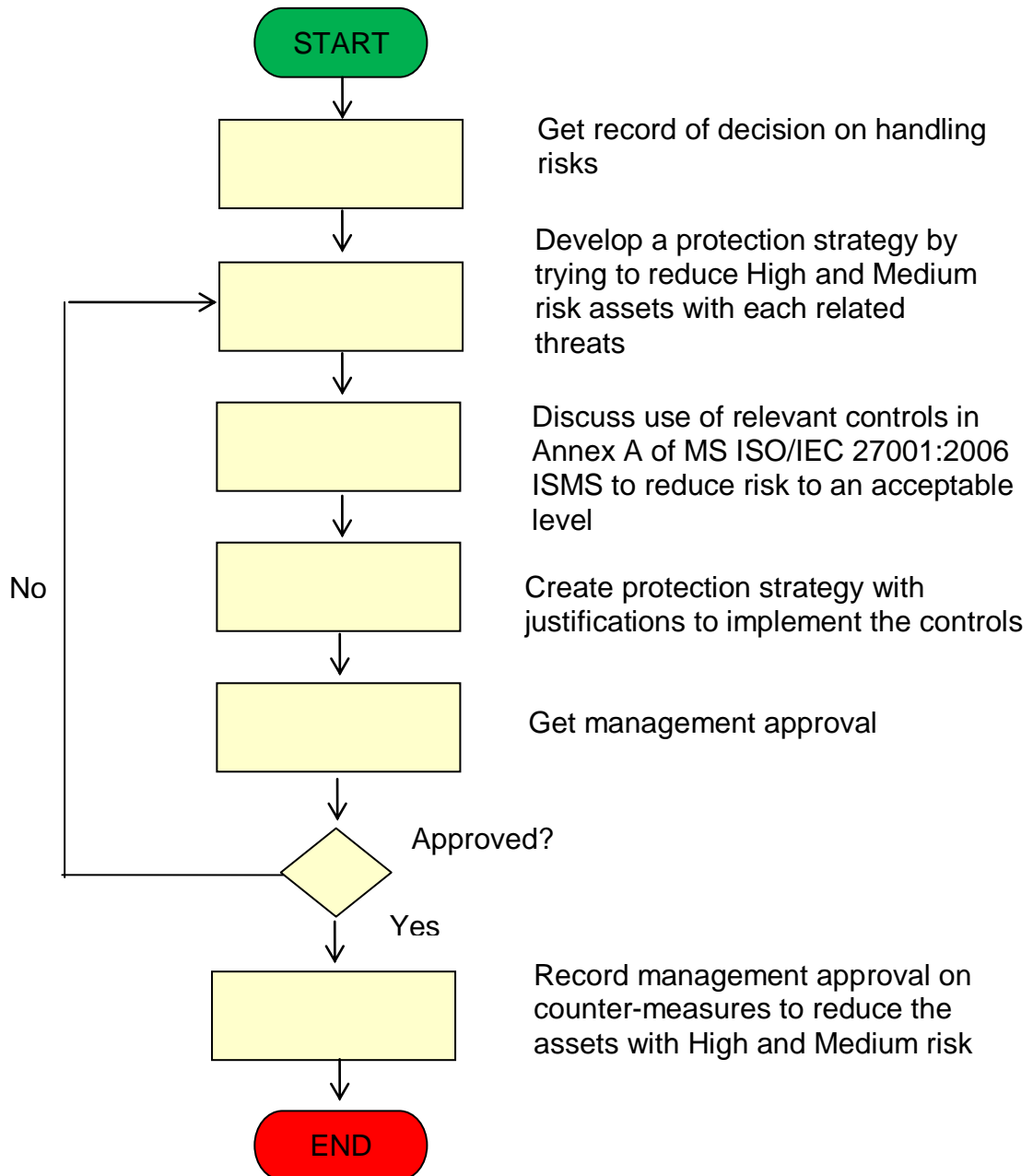
k. Recommendation on Option Handling Risks





**RISK ASSESSMENT GUIDELINE**

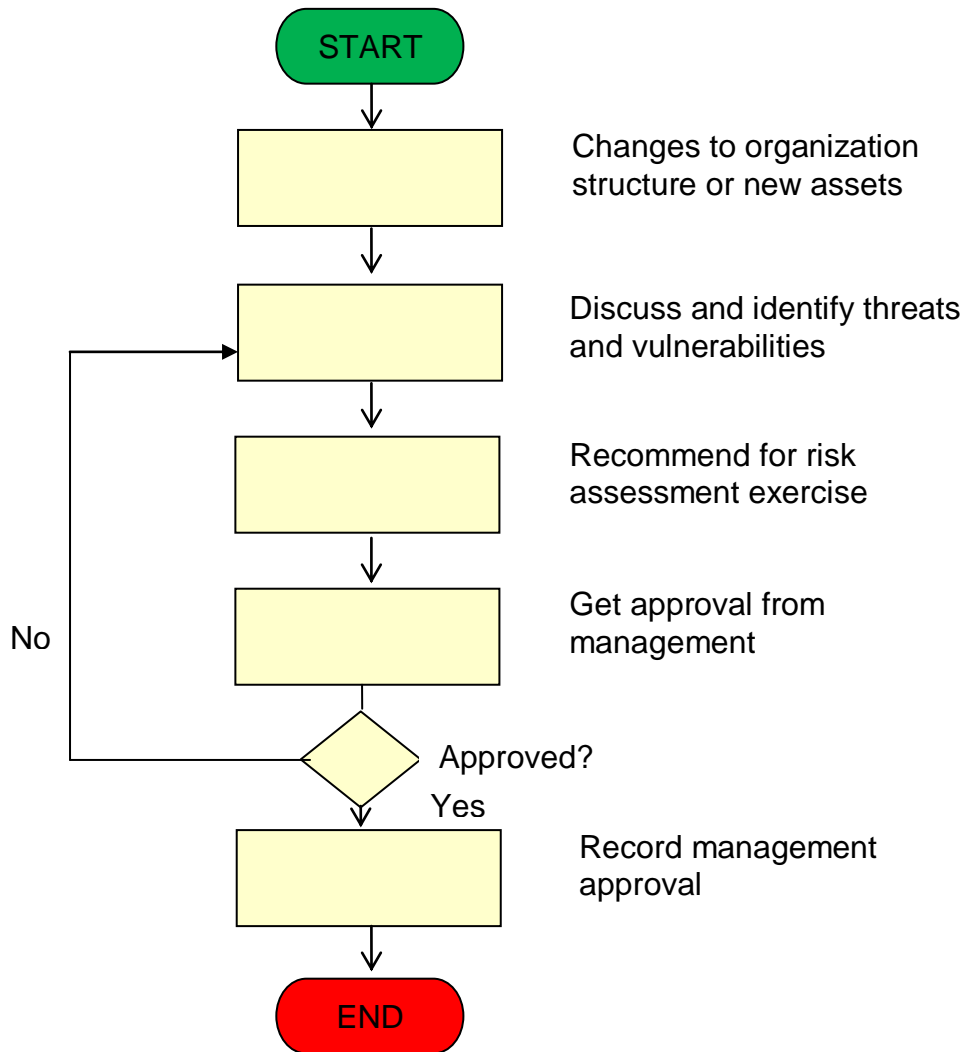
I. Protection Strategy





**RISK ASSESSMENT GUIDELINE**

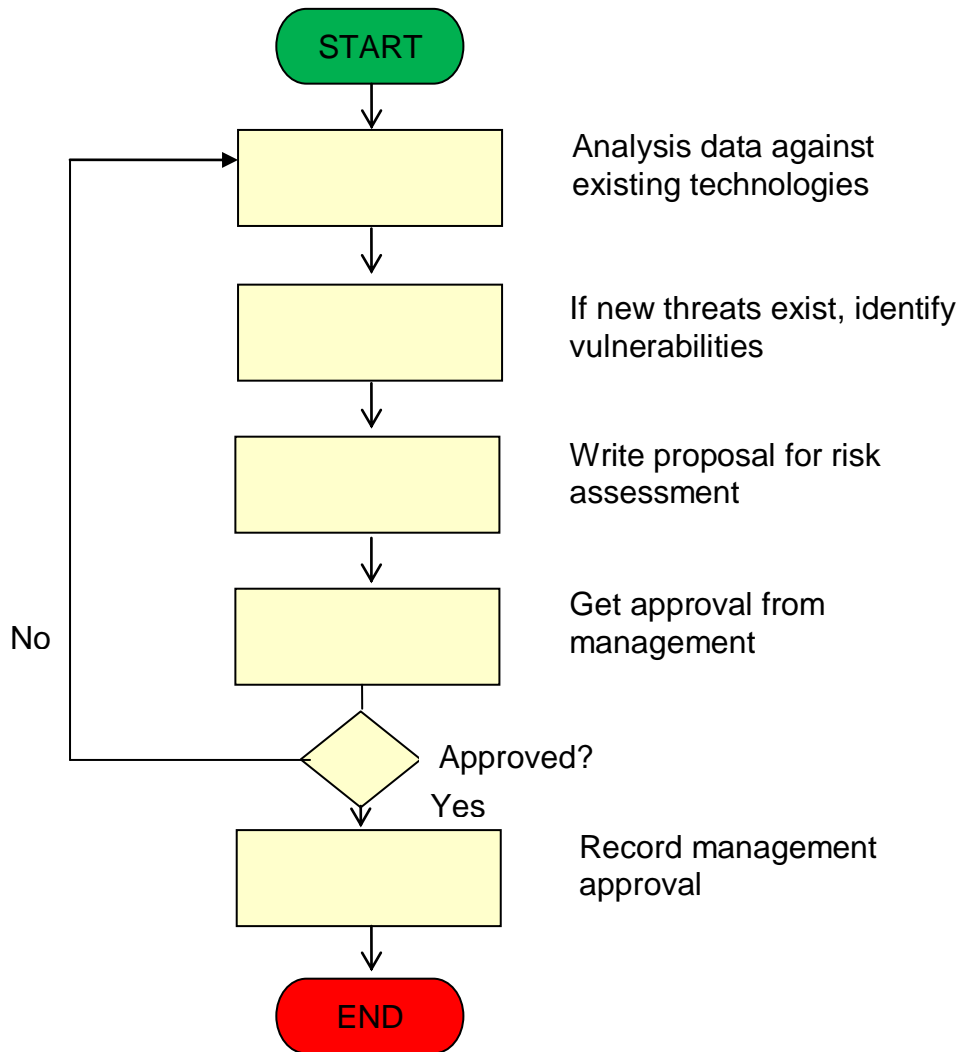
m. Criteria for risk assessment: (i)





**RISK ASSESSMENT GUIDELINE**

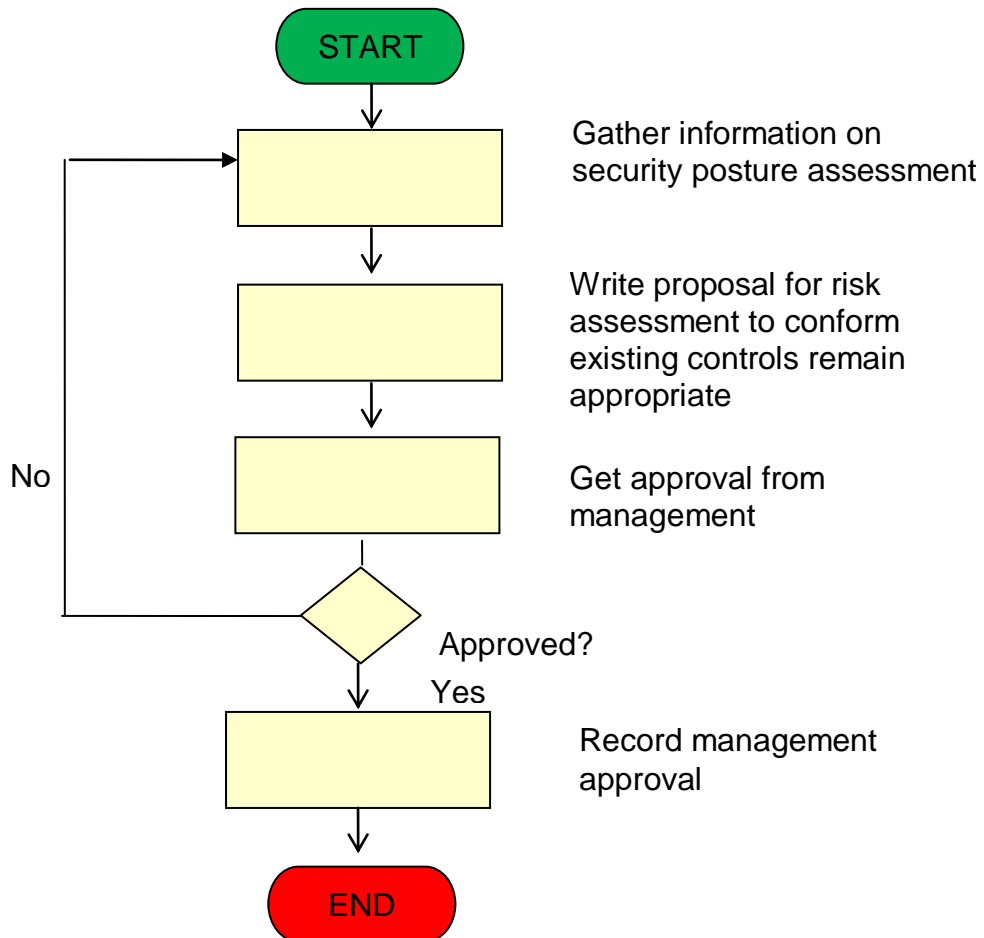
n. Risk assessment based on criteria (ii):





**RISK ASSESSMENT GUIDELINE**

o. Risk assessment based on criteria (iii):



**RISK ASSESSMENT GUIDELINE****16. RECORDS**

No.	Type of Record	Location	Retention Period
1.	Project Team List	ICT Compliance Division	5 years
2.	Risk Assessment Boundary	ICT Compliance Division	5 years
3.	List of Assets	ICT Compliance Division	5 years
4.	Assets Value Rating Table	ICT Compliance Division	5 years
5.	Summary of Asset Value and Dependencies	ICT Compliance Division	5 years
6.	Generic Threat Profile	ICT Compliance Division	5 years
7.	Relevant Threats to Assets	ICT Compliance Division	5 years
8.	Vulnerability List	ICT Compliance Division	5 years
9.	Existing and Planned Safeguards	ICT Compliance Division	5 years
10.	Business Loss Value Rating	ICT Compliance Division	5 years
11.	Impact Level List	ICT Compliance Division	5 years
12.	Likelihood Value Rating	ICT Compliance Division	5 years
13.	Likelihood List	ICT Compliance Division	5 years
14.	Risk Matrix	ICT Compliance Division	5 years
15.	Decision on Options	ICT Compliance Division	5 years
16.	Protection Strategy	ICT Compliance Division	5 years
17.	Management Approval on RA	ICT Compliance Division	5 years

Note:

Location of ICT Compliance Division:

SPSS Level 3 Block B2;

SPS Level 5 Block B5; and

Director ICT Compliance Division Office, Level 4 Block B2.





MAMPU-BPICT-ISMS-P1-008



**RISK ASSESSMENT GUIDELINE**

**4. APPENDIX**

- a) Appendix 1(a) – Project Team List Report Format
- b) Appendix 1(b) – Risk Assessment Boundary Report Format
- c) Appendix 1(c) – List of Assets Report Format
- d) Appendix 1(d) – Summary of Asset Value and Dependencies Report Format
- e) Appendix 1(e) – Generic Threat Profile Report Format
- f) Appendix 1(f) – Relevant Threats to Assets Report Format
- g) Appendix 1(g) – Vulnerability List Report Format
- h) Appendix 1(h) – Existing and Planned Safeguards Report Format
- i) Appendix 1(i) – Impact Level List Report Format
- j) Appendix 1(j) – Likelihood List Report Format
- k) Appendix 1(k) – Risk Matrix Report Format
- l) Appendix 1(l) – Decision on Options Report Format
- m) Appendix 1(m) – Protection Strategy Report Format
- n) Appendix 1(n) – Management Risk Assessment Report Format



MAMPU-BPICT-ISMS-P1-008



**RISK ASSESSMENT GUIDELINE**

**SULIT**

Appendix 1(a)

Project Team List Report Format

No.	Name	Job Function	Sect/Unit/Dept/ Div/Vendor	RA Function

Prepared by:

\_\_\_\_\_  
<Team Leader>

Reviewed by:

\_\_\_\_\_  
<Project Manager>

Approved by:

\_\_\_\_\_  
<Project Advisor>

**Notes: The sign-offs should be with the official stamp.**

**SULIT**

Version:  
(Date)

Page:



MAMPU-BPICT-ISMS-P1-008



**RISK ASSESSMENT GUIDELINE**

**SULIT**

Tasking Schedule List Report Format

No	Activity			Venue	SRA Team
	Date	Task	Details		
1.0	Activity Name (Y Days : Start Date – End Date)				
<u>Output:</u> 1. Output A					

Prepared by:  
\_\_\_\_\_  
<Team Leader>

Reviewed by:  
\_\_\_\_\_  
<Project Manager>

Approved by:  
\_\_\_\_\_  
<Project Advisor>

**Notes: The sign-offs should be with the official stamp.**

**SULIT**

Version: (Date)		Page:
--------------------	--	-------



MAMPU-BPICT-ISMS-P1-008



**RISK ASSESSMENT GUIDELINE**

**SULIT**

Appendix 1(b)

**Risk Assessment Boundary Report Format**

Table of Content  
Acronyms  
List of Figures  
List of Tables

1.0 Purpose  
2.0 Background of Review Boundary  
3.0 Review Boundary Statement  
4.0 Key Business Processes and Functions  
5.0 Supporting Business Processes  
6.0 External Interfaces  
7.0 Personnel  
8.0 Information Assets  
9.0 Sites/ Buildings  
10.0 Conclusion

Prepared by:

Reviewed by:

Approved by:

<Team Leader>

<Project Manager>

< Project Advisor >>

**Notes: The sign-offs should be with the official stamp.**

**List of Related Materials Used Report Format**

**SULIT**

Version:  
(Date)

Page:



MAMPU-BPICT-ISMS-P1-008



**RISK ASSESSMENT GUIDELINE**

**SULIT**

Name	Description

Prepared by:

< Team Leader >

Approved by:

< Project Manager >

**Notes: The sign-offs should be with the official stamp.**

**SULIT**

Version:  
(Date)

Page:



SULIT

Appendix 1(c)

**Asset Classification and Description**

<b>Classification</b>	<b>Definitions</b>
<b>Hardware</b>	<p>A tangible asset which is used to support the information-processing and storage facilities of the organisation.</p> <p>Examples: computers, servers, communication equipment, safes, etc.</p>
<b>Software</b>	<p>Application software or system software such as operating systems, database systems, networking system software, or office applications that provide information-processing facilities to the organisation.</p> <p>Examples: applications, development tools, utilities, system software, etc.</p>
<b>Services (Accessibility Services and Supporting Services)</b>	<p>Services or systems (not in nature of standalones physical hardware or software) that support other assets to perform their functions. For examples:</p> <p>(a) Accessibility services</p> <ol style="list-style-type: none"> <li>i. Network services such as LAN, WAN, etc.</li> <li>ii. Access Restriction System such as card access system.</li> </ol> <p>(b) Supporting services – utilities such as electricity, air-condition, and suppression fire system, etc.</p>
<b>Data or Information</b>	Documented (paper or electronic) information or

SULIT



MAMPU-BPICT-ISMS-P1-008



**RISK ASSESSMENT GUIDELINE**

**SULIT**

	intellectual information which is used to meet the missions and/or objectives of the organisation. Examples: system documentation, operational procedures, business records, clients' profiles, etc.
People	Persons who have knowledge and skills to conduct the daily in-scope business functions of agencies in order to achieve business objectives or missions. The People assets are listed based on their respective job functions, instead of the individual personnel members. Examples: general managers, software engineers, system administrators, etc.

**List of Assets Report Format**

No.	Asset Group	Asset ID	Asset Name	Owner	Custodian	Location	Description of Asset

Prepared by:

Reviewed by:

Approved by:

< Team Leader >

< Project Manager >

<Project Advisor>

**Notes: The sign-offs should be with the official stamp.**

**SULIT**

Version: (Date)		Page:
--------------------	--	-------

**RISK ASSESSMENT GUIDELINE****SULIT**

Appendix 1(d)

Descriptions of CIA listed in MyRAM document, Chapter 8 page 58 apply.

<b>CIA</b>	<b>Description</b>
<b>Confidentiality</b>	This is the effect on the system and/or the organisation that would result from the deliberate, unauthorized or inadvertent disclosure of the asset. The effect of unauthorized disclosure of confidential information can result in loss of public confidence, embarrassment, or legal action against the organisation.
<b>Integrity</b>	This is the effect on the system and/or the organisation that would result from deliberate, unauthorized or inadvertent modification of the asset. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of a system.
<b>Availability</b>	This is the effect on the system and/or the organisation that would result from deliberate or accidental denial of the asset's use. If a mission-critical system is unavailable to its end users, the organisation's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting the organisation's mission.

**SULIT**



**RISK ASSESSMENT GUIDELINE****SULIT**

Assets Group with their respective CIA in MyRAM document chapter 8 page 59 apply and must be considered.

Asset Group	Confidentiality	Integrity	Availability
Hardware	√	√	√
Software	√	√	√
Accessibility Services	√	√	√
Supporting Services	N/A	N/A	√
Information/Data	√	√	√
People	√	N/A	√

Note:

- i. Integrity is not applicable for People Asset Group as it is immeasurable or unquantifiable.
- ii. Confidentiality and integrity for Supporting Services Asset Group is immeasurable or unquantifiable.

**Legend:**

- √ Take into consideration  
N/A Not applicable (Not taken into consideration)

The following value-rating tables are used in evaluating the CIA values and the highest value among CIA is the final value for the asset.

**SULIT**Version:  
(Date)

Page:



SULIT

Table 1: Hardware Value Rating

Value Rating	Description
Low	<b>C:</b> The hardware device is used maximally in processing and/or storing information that is classified as “Terbuka”.
	<b>I:</b> Security breaches to the device could result in loss of public confidence; however, information is insignificantly affected and the loss of functionality is minimal.
	<b>A:</b> The processes will still be operational or functional but slow if the time of unavailability of the devices is more than 2 weeks.
Medium	<b>C:</b> The hardware device is used maximally in processing and/or storing information that is classified as “Terhad” and/or “Sulit”.
	<b>I:</b> Security breaches to the device could result in loss of public confidence, inaccuracy, fraud, or erroneous decisions, as well as cause the organisation’s mission to be affected with some losses of functionality and operational effectiveness.
	<b>A:</b> Some of the operations/functions will be suspended if the time of unavailability of the device is between 1 to 2 weeks.
High	<b>C:</b> The hardware device is used maximally in processing and/or storing information that is classified as “Rahsia” and/or “Rahsia

SULIT

**RISK ASSESSMENT GUIDELINE****SULIT**

	<b>Besar”.</b>
	<b>I:</b> Security breaches to the device could result in loss of public confidence, inaccuracy, fraud, or erroneous decisions, as well as cause significant loss of core functions and operational effectiveness.
	<b>A:</b> The operations/functions will stop if the time of unavailability of the device is less than or equal to 1 week.

Table 3: Software Value Rating

<b>Value Rating</b>	<b>Descriptions</b>
<b>Low</b>	<b>C:</b> The software package or application is used maximally in processing and/or storing information that is classified as “Terbuka”.
	<b>I:</b> Security breaches to the software could result in loss of public confidence; however, information is insignificantly affected and the loss of functionality is minimal.
	<b>A:</b> The processes will still be operational or functional but slow if the time of unavailability of the software is more then 2 weeks.
<b>Medium</b>	<b>C:</b> The software package or application is used maximally in processing and/or storing information that is classified as “Terhad” and/or “Sulit”.

**SULIT**

**RISK ASSESSMENT GUIDELINE****SULIT**

	<p><b>I:</b> Security breaches to the software could result in loss of public confidence, inaccuracy, fraud, or erroneous decisions, as well as cause the organisation's mission to be affected with some losses of functionality and operational effectiveness.</p> <p><b>A:</b> Some of the operations/functions will be suspended if the time of unavailability of the software is between 1 to 2 weeks.</p>
<b>High</b>	<p><b>C:</b> The software package or application is used maximally in processing and/or storing information that is classified as "Rahsia" and/or "Rahsia Besar".</p> <p><b>I:</b> Security breaches to the software could result in loss of public confidence, inaccuracy, fraud, or erroneous decisions, as well as cause significant loss of core functions and operational effectiveness.</p> <p><b>A:</b> The operations/functions will stop if the time of unavailability of the software is less than or equal to 1 week.</p>

**SULIT**

**RISK ASSESSMENT GUIDELINE****SULIT**

Table 4: Accessibility Services Value Rating

<b>Value Rating</b>	<b>Description</b>
<b>Low</b>	<b>C:</b> The services are used maximally in transferring information that is classified as “Terbuka”.
	<b>I:</b> Security breaches to the services component could result in loss of public confidence; however, information is insignificantly affected and the loss of functionality is minimal.
	<b>A:</b> The processes will still be operational or functional but slow if the time of unavailability of the services is more than 2 weeks.
<b>Medium</b>	<b>C:</b> The services are used maximally in transferring information that is classified as “Terhad” and/or “Sulit”.
	<b>I:</b> Security breaches to the services could result in loss of public confidence, inaccuracy, fraud, or erroneous decisions, as well as cause the organisation’s mission to be affected with some losses of functionality and operational effectiveness.
	<b>A:</b> Some of the operations/functions will be suspended if the time of unavailability of the services is between 1 to 2 weeks.
<b>High</b>	<b>C:</b> The services are used maximally in transferring information that is classified as “Rahsia” and/or “Rahsia Besar”.
	<b>I:</b>

**SULIT**

**RISK ASSESSMENT GUIDELINE****SULIT**

	<p>Security breaches to the services could result in loss of public confidence, inaccuracy, fraud, or erroneous decisions, as well as cause significant loss of core functions and operational effectiveness.</p>
	<p><b>A:</b></p> <p>The operations/functions will stop if the time of unavailability of the services are less than or equal to 1 week.</p>

Table 5: Supporting Services Value Rating

Value Rating	Description
Low	<p><b>A:</b></p> <p>The processes will still be operational or functional but slow if the time of unavailability of the services is more than 24 hours.</p>
Medium	<p><b>A:</b></p> <p>Some of the operations/functions will be suspended if the time of unavailability of the services is between 6 to 24 hours.</p>
High	<p><b>A:</b></p> <p>The operations/functions will stop if the time of unavailability of the services are less than or equal to 5 hours.</p>

Table 6: Data/Information Value Rating

Value Rating	Descriptions
Low	<p><b>C:</b></p> <p>The data/information that is classified as “Terbuka”.</p>
	<p><b>I:</b></p> <p>Any security breaches would affect the security objectives of the organisation; however, they would NOT introduce operational issues.</p>

**SULIT**

**RISK ASSESSMENT GUIDELINE****SULIT**

	<p><b>A:</b> The processes will still be operational or functional but slow if the time of unavailability of information is more than 2 weeks.</p>
<b>Medium</b>	<p><b>C:</b> The information/data that classified as “Terhad” and/or “Sulit”.</p>
	<p><b>I:</b> Any security breaches would not cause significant damages; however, they would introduce operational issues as well as insignificant loss of public confidence.</p>
	<p><b>A:</b> The non-critical operations/functions will be temporarily suspended if the time of unavailability of information is between 1 to 2 weeks.</p>
<b>High</b>	<p><b>C:</b> The information/data that classified as “Rahsia” and/or “Rahsia Besar”.</p>
	<p><b>I:</b> Any security breaches would cause significant damages to some of the business functions and threaten the survival of the organisation.</p>
	<p><b>A:</b> The operations/functions will stop if the time of unavailability of information is less than or equal to 1 week.</p>

Table 7: People Value Rating

**SULIT**

Version: (Date)		Page:
--------------------	--	-------

**RISK ASSESSMENT GUIDELINE****SULIT**

Value Rating	Descriptions
<b>Low</b>	<b>C:</b> The role of the personnel requires him/her to handle* “Rahsia” and/or “Rahsia Besar” information less than 10% of the time, and “Sulit” and/or “Terhad” information less than 10% of the time, and “Terbuka” information most of the time.
	<b>A:</b> If the personnel is unavailable, <ul style="list-style-type: none"> <li>• operations in the organisation will meet objectives, however</li> <li>• operations are slow compared to normal/usual.</li> </ul>

Value Rating	Descriptions
<b>Medium</b>	<b>C:</b> The role of the personnel requires him/her to handle* “Rahsia” and/or “Rahsia Besar” information less than 20% of the time, and “Sulit” and/or “Terhad” information less than 20% of the time.
	<b>A:</b> If the personnel is unavailable: <ul style="list-style-type: none"> <li>• operations in the organisation will meet objectives, however</li> <li>• certain operations will be put on hold temporarily, nevertheless, it can still be passed on to another personnel member with the same role for handling.</li> </ul>
<b>High</b>	<b>C:</b> The role of the personnel requires him/her to handle* “Rahsia” and “Rahsia Besar” information more than 20% of the time.

**SULIT**

Version: (Date)		Page:
--------------------	--	-------



**RISK ASSESSMENT GUIDELINE****SULIT****A:****If the personnel is unavailable:**

- **Operations in the organisation will fail to meet their objectives.**
- **Most or all critical processes will have to be suspended with no substitutions.**

\*: The term “handle” here does NOT refer to handling by couriers. It refers to handling of information by authorized personnel who can read or see the information.

**SULIT**



MAMPU-BPICT-ISMS-P1-008



**RISK ASSESSMENT GUIDELINE**

**SULIT**

No.	Asset Group	Asset ID	Asset Name	Value			Asset Depended On	Dependent Asset	Asset Value
				C	I	A			

**Summary of Asset Value and Dependencies Report Format**

Prepared by:

Reviewed by:

Approved by:

< Team Leader >

<Project Manager >

<Project Advisor>

**Notes: The sign-offs should be with the official stamp.**

**SULIT**

Version:  
(Date)

Page:



**RISK ASSESSMENT GUIDELINE**

**SULIT**

Appendix 1(e)

Generic Threat Profile Report Format

Threat Group	Threat ID	Threat Name	Threat Description

Prepared by: \_\_\_\_\_ Reviewed by: \_\_\_\_\_ Approved by: \_\_\_\_\_  
 < Team Leader >      < Project Manager >      <Project Advisor>

**Notes: The sign-offs should be with the official stamp.**

Appendix 1(f)

Relevant Threats to Assets Report Format

No.	Asset Group	Asset ID	Asset Name	Threat Group	Threat ID	Threat Name

Prepared by: \_\_\_\_\_ Reviewed by: \_\_\_\_\_ Approved by: \_\_\_\_\_  
 < Team Leader >      < Project Manager >      <Project Advisor>

**Notes: The sign-offs should be with the official stamp.**

**SULIT**

**SULIT**

Appendix 1(g)

Vulnerability List Report Format

No.	Asset Group	Asset ID	Asset Name	Threat Group	Threat ID	Threat Name	Vulnerability Group	Vulnerability ID	Vulnerability Name

Prepared by:

\_\_\_\_\_

< Team Leader >

Reviewed by:

\_\_\_\_\_

< Project Manager >

Approved by:

\_\_\_\_\_

<Project Advisor>

**Notes: The sign-offs should be with the official stamp.**

**SULIT**



MAMPU-BPICT-ISMS-P1-008



RISK ASSESSMENT GUIDELINE

SULIT

Appendix 1(h)

Existing and Planned Safeguards Report Format

No.	Asset Group	Asset ID	Asset Name	Threat Group	Threat ID	Threat Name	Safeguard ID	Safeguard Name	Planned Safeguard	Existing Safeguard

Prepared by:

< Team Leader >

Reviewed by:

< Project Manager >

Approved by:

<Project Advisor>

**Notes: The sign-offs should be with the official stamp.**

SULIT

Version:  
(Date)

Page:

**RISK ASSESSMENT GUIDELINE****SULIT**

Appendix 1(i)

Following are criteria used in determining the business loss on assets:

Table 1: Business Loss Value Rating – Hardware

<b>Business Loss Level</b>	<b>Explanation and Outcome</b>
<b>Low</b>	The impact of loss or unavailability of the asset is minor or negligible and will NOT bring any financial loss. Security breaches to the device will NOT cause disruptions to conduct daily operations of the organisations.
<b>Medium</b>	The impact of loss or unavailability of the asset is considerable and could possibly bring financial loss. Security breaches to the device could result in inconveniences/disruptions to conduct daily operations of the organisations.
<b>High</b>	The impact of loss or unavailability of the asset is intolerable and could bring high financial loss. Security breaches to the device could result in total disruptions to conduct daily operations of the organisations.

Table 2: Business Loss Value Rating – Software

<b>Business Loss Level</b>	<b>Explanation and Outcome</b>
<b>Low</b>	The impact of loss or unavailability of the software package or application is minor or negligible and will NOT bring any financial loss. Security breaches to the software will NOT cause disruptions to conduct daily operations of the organisations.
<b>Medium</b>	The impact of loss or unavailability of the software package or

**SULIT**

**RISK ASSESSMENT GUIDELINE****SULIT**

	application is considerable and could possibly bring financial loss. Security breaches to the software could result in inconveniences /disruptions to conduct daily operations of the organisations.
<b>High</b>	The impact of loss or unavailability of the software package or application is intolerable and could bring high financial loss. Security breaches to the software could result in total disruptions to conduct daily operations of the organisations.

Table 3: Business Loss Value Rating – Services

<b>Business Loss Level</b>	<b>Explanation and Outcome</b>
<b>Low</b>	The impact of loss or unavailability of the asset is minor or negligible and will NOT bring any financial loss. Security breaches or interruption to the service(s) will NOT cause disruptions to conduct daily operations of the organisations.
<b>Medium</b>	The impact of loss or unavailability of the asset is considerable and could possibly bring financial loss. Security breaches or interruption to the service(s) could result in inconveniences /disruptions to conduct daily operations of the organisations.
<b>High</b>	The impact of loss or unavailability of the asset is intolerable and could bring high financial loss. Security breaches or interruption to the service(s) could result in total disruptions to conduct daily operations of the organisations.

Table 4: Business Loss Value Rating – Information/Data

<b>Business</b>	<b>Explanation and Outcome</b>
Version: (Date)	

**SULIT**

Page:

**RISK ASSESSMENT GUIDELINE****SULIT**

<b>Loss Level</b>	
<b>Low</b>	No loss of confidence by the public or other parties; requires very minimal resources in terms of time, with personnel having minimal skills to replace and/or recover the information.
<b>Medium</b>	Some loss of confidence by the public or other parties; requires some resources, in terms of time, with personnel having minimal skills are needed to replace and/or recover the information.
<b>High</b>	Total loss of confidence by the public or other parties; requires significance resources in terms of time, with skilful and qualified personnel are needed to replace and/or recover the information.

Table 5: Business Loss Rating – People

<b>Business Loss Level</b>	<b>Explanation and Outcome</b>
<b>Low</b>	Understanding of the business processes and some skills required.
<b>Medium</b>	Substantial knowledge and skills in handling business process with minimal guidance required.
<b>High</b>	Must be extremely knowledgeable and the only reference for the subject matters with vast skills in relation to the business processes.

**SULIT**



**RISK ASSESSMENT GUIDELINE****SULIT****Impact = Function (Asset Value, Business Loss)**

Business Loss	Asset Value		
	Low	Medium	High
Low	L	L	M
Medium	L	M	H
High	M	H	H

**Legend of Impact Level:**

Low



Medium



High

Impact Level List Report Format

No.	Asset Group	Asset ID	Asset Name	Asset Value	Business Loss	Impact Level

Prepared by:

&lt; Team Leader &gt;

Reviewed by:

&lt; Project Manager &gt;

Approved by:

&lt;Project Advisor&gt;

**Notes: The sign-offs should be with the official stamp.****SULIT**Version:  
(Date)

Page:

**RISK ASSESSMENT GUIDELINE****SULIT**

Appendix 1(l)

Get result from selected step:

From Step	Result
Step 5	Threats
Step 6	Vulnerabilities
Step 7	Safeguards

Following are the criteria used in evaluating the likelihood that a specific asset may be compromised.

Table 1: Likelihood Value Rating Table

Likelihood Level	Explanation and Outcome
<b>Low</b>	<ul style="list-style-type: none"> <li>• Threats seldom occur and the type of threats that occur may cause minimal operational danger.</li> <li>• Little or not capable in exploiting vulnerabilities, however, would act if provoked. Or, possesses knowledge and skills to exploit vulnerabilities (with not enough resources), or has enough resources with lack of knowledge and skills but not inclined to breach the security.</li> <li>• Security controls in placed have been tested and effective.</li> </ul>
<b>Medium</b>	<ul style="list-style-type: none"> <li>• Threats often occur and they may slow down some operations.</li> <li>• Possesses knowledge, skills, and resources to exploit vulnerabilities but not inclined to breach the security. Or, little or not capable in exploiting vulnerabilities but very motivated to attempt attacks. Or, possesses knowledge and skills to exploit vulnerabilities (with not enough resources), or has enough resources with lack of knowledge and skills and</li> </ul>

**SULIT**Version:  
(Date)



Page:

**RISK ASSESSMENT GUIDELINE****SULIT**

	<p>would attempt to attack if provoked.</p> <ul style="list-style-type: none"><li>• Security controls exist; however, they are not very effective.</li></ul>
<b>High</b>	<ul style="list-style-type: none"><li>• Threats occur frequently and they may suspend most of critical operations.</li><li>• Possesses knowledge, skills, and resources to exploit vulnerabilities and would attempt to attack if provoked. Or, possesses knowledge and skills to exploit vulnerabilities (with not enough resources), or has enough resources with lack of knowledge and skills and very motivated to attempt attacks.</li><li>• Security controls are not planned yet.</li></ul>

**SULIT**Version:  
(Date)

Page:

	<b>MAMPU-BPICT-ISMS-P1-008</b>	
<b>RISK ASSESSMENT GUIDELINE</b>		

**SULIT**

Likelihood List Report Format

No.	Asset Group	Asset ID	Asset Name	Threat ID	Threat Name	Vulnerability ID	Vulnerability Name	Safeguard Solution	Likelihood

Prepared by:  
 \_\_\_\_\_  
 < Team Leader >

Reviewed by:  
 \_\_\_\_\_  
 < Project Manager >

Approved by:  
 \_\_\_\_\_  
 <Project Advisor>

**Notes: The sign-offs should be with the official stamp.**

**SULIT**

**RISK ASSESSMENT GUIDELINE****SULIT**

Appendix 1(k)

Three (3) quadrant risk matrix table and risk is expressed as a function of:

**Risk = Function (Impact, Likelihood)**

Impact	Likelihood		
	Low	Medium	High
Low	L	L	M
Medium	L	M	H
High	M	H	H

**Legend of Risk Level:****L** Low**M** Medium**H** High

## Risk Level Report Format

No.	Asset Group	Asset ID	Asset Name	Threat ID	Threat Name	Impact Level	Likelihood	Risk Level

Prepared by:

Reviewed by:

Approved by:

&lt; Team Leader &gt;

&lt; Project Manager &gt;

&lt;Project Advisor&gt;

**Notes: The sign-offs should be with the official stamp.****SULIT**Version:  
(Date)

Page:

**SULIT**

Appendix 1(l)

**Decision on Options report format**

No.	Asset Group	Asset ID	Asset Name	Threat ID	Threat Name	Current Safeguard	Risk Level	Recommendation	Decision

Prepared by:  
 \_\_\_\_\_  
 < Team Leader >

Reviewed by:  
 \_\_\_\_\_  
 < Project Manager >

Approved by:  
 \_\_\_\_\_  
 <Project Advisor >

**Notes: The sign-offs should be with the official stamp.**

**SULIT**

**SULIT**

Appendix 1(m)

**Protection Strategy Report Format**

No.	Asset Group	Asset ID	Asset Name	Threat ID	Threat Name	Current Safeguard Solution	Risk Level	Recommendation	Protection Strategy	Justification

Prepared by:

\_\_\_\_\_

< Team Leader >

Reviewed by:

\_\_\_\_\_

< Project Manager >

Approved by:

\_\_\_\_\_

<Project Advisor >

**Notes: The sign-offs should be with the official stamp.**

**SULIT**

**RISK ASSESSMENT OUTPUT****SULIT**

Appendix 1(n)

Management Risk Assessment Report should consist of:

- a) Analysis of Findings
  - i) Asset value based on asset group

Asset Group	Asset Value			Asset Count
	Low	Medium	High	

- ii) Asset group against threat group occurrence

Asset Group	Asset Group					Threat Group Occurrence
	Hardware	Software	Services	Data / Information	People	

- iii) Asset group against vulnerability group occurrence

Vulnerability Group	Asset Group					Vulnerability Group Occurrence
	Hardware	Software	Services	Data / Information	People	

- iv) Asset group against impact level

Asset Group	Impact Level		
	Low	Medium	High

**SULIT**Version:  
(Date)

Page:





**RISK ASSESSMENT OUTPUT**

**SULIT**

- v) Risk level for all assets

Asset Group	Risk Level		
	Low	Medium	High

- b) Recommendations
  - i) Decision on Options Report  
Refer to appendix 1(l)]
  - ii) Protection Strategy Report  
[Refer to appendix 1(m)