Universitas Esa Unggul

Smart, Creative and Entrepreneurial

www.esaunggul.ac.id

RISK MANAGEMENT FOR INFORMATION TECHNOLOGY SYSTEMS

PROGRAM STUDI MAGISTER ILMU KOMPUTER

FAKULTAS ILMU KOMPUTER

Pertemuan – 9 #7329-Dr. Gerry Firmansyah

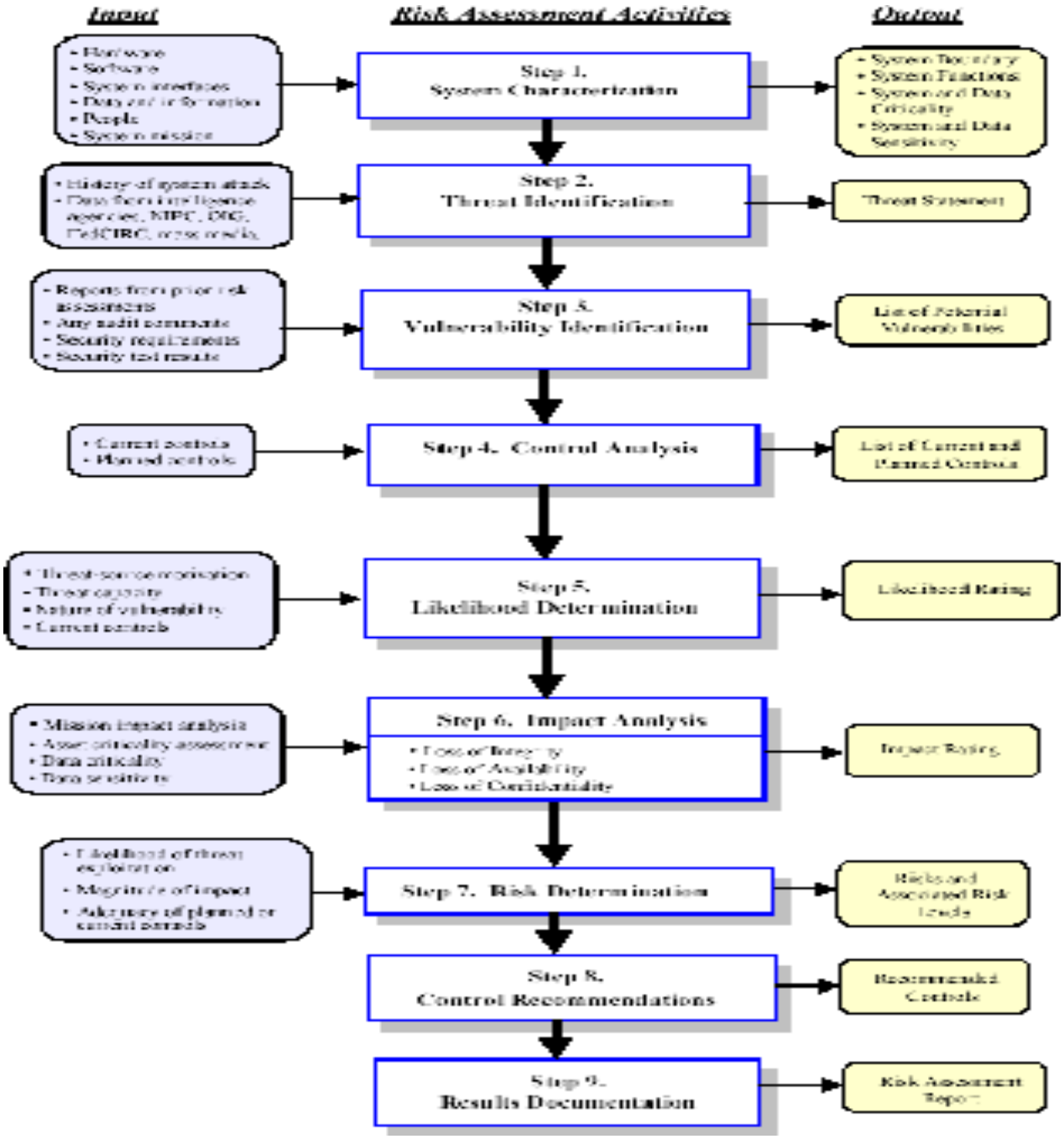
OUTLINE

I. Introduction
II. Risk Management Overview
III. Risk Assessment
IV. Risk Mitigation
V. Evaluation and Assessment

Risk Assessment Methodology

- Step 1 – System Characterization
- Step 2 – Threat Identification
- Step 3 – Vulnerability Identification
- Step 4 – Control Analysis
- Step 5 – Likelihood Determination
- Step 6 – Impact Analysis
- Step 7 – Risk Determination
- Step 8 – Control Recommendations
- Step 9 – Results Documentation

Risk Assessment Methodology Flowchart



Step 6 : Impact Analysis

The necessary information needed :

- System mission
  - (e.g., the processes performed by the IT system)
- System and data criticality
  - (e.g., the system's value or importance to an organization)
- System and data sensitivity.

Security goals

- The adverse impact of a security event can be described in terms of LOSS or DEGRADATION of any, or a combination of any, of the following three security goals :

- Integrity
- Availability
- Confidentiality

Loss of Integrity

- • System & data integrity refers to the requirement that information be protected from improper modification.
- • Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts.
- • If the loss of system or data is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions.
- • 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 an IT systems.

Loss of Availability

- If a mission critical IT system is unavailable to its end users, the organization's mission may be affected.
- Example :
  - Loss of system functionality
  - Loss of system operational effectiveness
  - ➢ Result in loss of productive time
  - ➢ Impeding the end user's performance of their functions in supporting the organization's mission.

Loss of Confidentiality

- • System & data confidentiality refers to the protection of information from unauthorized disclosure.
- • The impact of unauthorized disclosure of confidential information can range :
  - From the jeopardizing of national security
  - To the disclosure of Privacy Act data.
- Unauthorized, unanticipated, or unintentional disclosure could result in :
  - Loss of public confidence
  - Embarrassment
  - Legal action against the organization

Impacts Categories

- Some tangible impacts can be measured quantitatively in :
  - Lost revenue
  - The cost of repairing the system
  - The level of effort required to correct problems caused by a successful threat action
- Other impacts e.g :
  - Loss of public confidence
  - Loss of credibility
  - Damage to an organization's interest

➢ Cannot be measured in specific units, but can be qualified or described in terms of :
  - High impacts
  - Medium impacts
  - Low impacts

Magnitude of Impact Definitions

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

Qualitative Impact Analysis

- The main advantage :
  - It prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities.
- The disadvantage :
  - It does not provide specific quantifiable measurements of the magnitude of the impacts
  - Therefore making a cost-benefit analysis of any recommended controls difficult.

Quantitative Impact Analysis

- The major advantage :
  - It provides a measurement of the impacts' magnitude
  - Which can be used in the cost-benefit analysis of recommended controls.
- The disadvantage :
  - Depending on the numerical ranges used to express the measurement,
  - The meaning of the quantitative impact analysis may be unclear,
  - Requiring the result to be interpreted in a qualitative manner.

Additional Factors

- Estimation of the frequency of the threat-source's exercise of the vulnerability over a specific time period (e.g., 1 year).
- Approximate cost for each occurrence of the threat-source's exercise of the vulnerability.
- Weighted factor based on a subjective analysis of the relative impact of a specific threat's exercising a specific vulnerability.

Output from Step 6

- Magnitude of impact :
  - High
  - Medium
  - Low

Step 7 : Risk Determination

- The purpose of this step is to assess the level of risk to the IT system.

Risk Determination Components

- The determination of risk for a particular threat/vulnerability pair can be expressed as a function of :
  - The likelihood of a given threat-source's attempting to exercise a given vulnerability.
  - The magnitude of the impact should a threat-source successfully exercise the vulnerability.
  - The adequacy of planned or existing security controls for reducing or eliminating risks.

Risk Level Matrix

- Mission risk = threat likelihood ratings X threat impact ratings
- Next table shows how the overall risk ratings might be determined based on inputs from the threat likelihood and threat impact categories.
- The next matrix is a 3 x 3 matrix of threat likelihood (High, Medium, and Low) and threat impact (High, Medium, and Low).

Matrix Dimension

- Depending on the site's requirements and the granularity of the risk assessment desired, some sites may use a 4 x 4 or 5 x 5 matrix.
- The latter can include a Very Low / Very High threat likelihood and a Very Low / Very High threat impact to generate a Very Low / Very High risk level.
- A "Very High" risk level may require possible system shutdown or stopping of all IT system integration and testing efforts.

Determination of Risk Levels

- The next sample matrix shows how the overall risk levels of High, Medium, and Low are derived.
- The determination of these risk levels or ratings may be subjective.
- The rationale for this justification can be explained in terms of the probability assigned for each threat likelihood level and a value assigned for each impact level.
- For example :
  - The probability assigned for each threat likelihood level is 1.0 for High, 0.5 for Medium, 0.1 for Low.
  - The value assigned for each impact level is 100 for High, 50 for Medium, and 10 for Low.

Sample of Risk Level Matrix Table

Threat Likelihood	Impact		
	Low (10)	***Medium*** (50)	***High*** (100)
High (1.0)	**Low** 10 X 1.0 = 10	**Medium** 50 X 1.0 = 50	**High** 100 X 1.0 = 100
Medium (0.5)	**Low** 10 X 0.5 = 5	**Medium** 50 X 0.5 = 25	**Medium** 100 X 0.5 = 50
Low (0.1)	**Low** 10 X 0.1 = 1	**Low** 50 X 0.1 = 5	**Low** 100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)[8]

Description of Risk Level

- The next table describes the risk levels shown in the previous matrix.
- •This risk scale, with its ratings of High, Medium, and Low, represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised.
- •The risk scale also presents actions that senior management, the mission owners, must take for each risk level.

Risk Scale and Necessary Actions Table

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk.

Output from Step 7

- Risk Level :
  - High
  - Medium
  - Low

Step 8 : Control Recommendations

- • During this step of process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization's operations, are provided.
- • The goal of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level.
- • The control recommendations are the results of the risk assessment process and provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.

Factors should be considered

- Effectiveness of recommended options (e.g., system compatibility)
- Legislation and regulation
- Organizational policy
- Operational impact
- Safety and reliability

Additional consideration

- It should be noted that not all possible recommended controls can be implemented to reduce loss.
- To determine which ones are required and appropriate for a specific organization, a cost-benefit analysis should be conducted for the proposed recommended controls, to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk.
- The operational impact (e.g., effect on system performance) and feasibility (e.g., technical requirements, user acceptance) of introducing the recommended option should be evaluated carefully during the risk mitigation process.

Output from step 8

- Recommendation of control(s) and alternative solutions to mitigate risk.

Step 9 : Results Documentation

- Once the risk assessment has been completed :
  - Threat-sources and vulnerabilities identified
  - Risks assessed
  - Recommended controls provided
- The result should be documented in an official report or briefing.

Considerations

- A risk assessment report is a management report that helps senior management, the mission owners, make decisions on policy, procedural, budget, and system operational and management changes.
- A risk assessment report should be presented as a systematic and analytical approach to assessing risk so that senior management will understand the risks and allocate resources to reduce and correct potential losses.
- For this reasons, some people prefer to address the threat/vulnerability pairs as observations instead of findings in the risk assessment report.

Output from Step 9

- Risk assessment report that :
  - describes the threats and vulnerabilities,
  - measures the risk, and
  - provides recommendations for control implementation.

Good Luck