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 – 8 #7329-Dr. Gerry Firmansyah

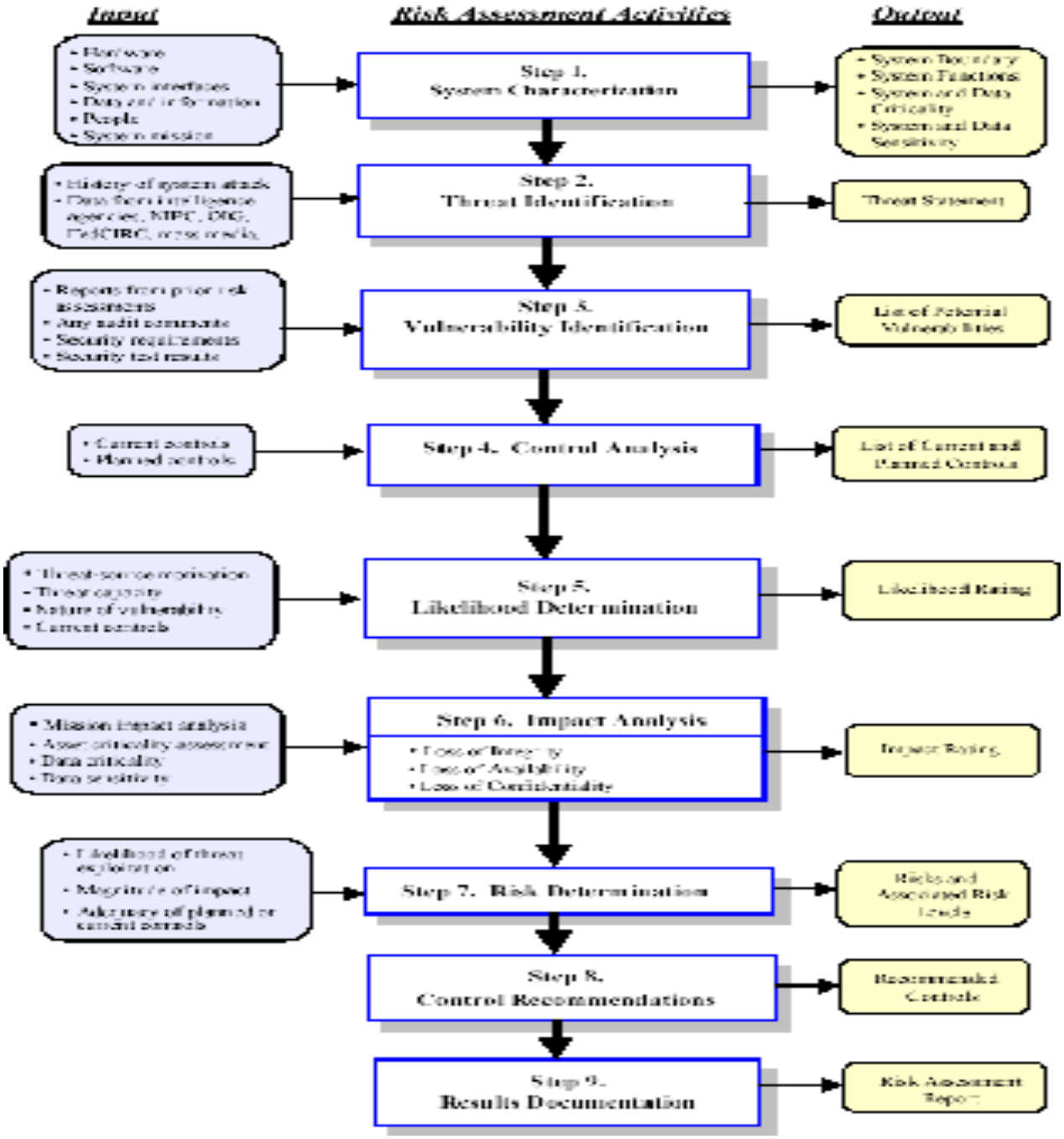
OUTLINE

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 4 : Control Analysis

- Goal :
  - analyze the controls
    - that have been implemented,
    - or are planned for implementation,
    - ➢ by the organization
  - to minimize
  - or eliminate
  - ➢ the likelihood (or probability) of a threat's exercising a system vulnerability.

Example of Control Analysis

- A vulnerability
  - is not likely to be exercised
  - or the likelihood is low
- if there is a low level of
  - threat-source interest
  - or capability
- or if there are effective security controls
  - that can eliminate,
  - or reduce the magnitude of ,
- harm.

Control Methods

- Technical controls
- Non-technical controls

Technical Controls

- Are safeguards that are incorporated into :
  - Computer hardware
  - Software
  - Firmware :
    - Access control mechanisms
    - Identification and authentication mechanisms
    - Encryption methods
    - Intrusion detection software

Non-Technical Controls

- Are management and operational controls such as :
  - Security policies
  - Operational procedures
  - Security of :
    - Personnel
    - Physic
    - Environment

Control Categories

- Preventive controls
- Detective controls

Preventive Controls

- Inhibit attempts to violate security policy
- Include such controls as :
  - access control enforcement,
  - encryption,
  - Authentication (keabsahan user yg menggunakan sistem)

Detective Controls

- Warn of violations or attempted violations of security policy
- Include such controls as :
  - audit trails, kemampuan sist menjelaskan apa yg telah terjadi (log) kejadian jam brp, user siapa, proses apa
  - intrusion detection methods, mendeteksi adanya penyusup
  - checksums. Data ditambah dengan digit tertentu, untuk dicek di penerima, apakah digit sesuai dg tg diterima, kalau tidak berarti ada gangguan

Control Analysis Technique

- Efficient and systematic control analysis :
  - Development of a security requirements checklist
    - Can be used to validate :
      - Security noncompliance
      - Security compliance
  - Use of an available checklist
- It is essential to update such checklists to reflect changes in an organization's control environment :
  - Changes in security policies
  - Changes in security methods
  - Changes in security requirements

➢ To ensure the checklist's validity

Output from Step 4

- List of current or planned controls
  - Used for the IT systems
- To mitigate the likelihood of a vulnerability's being exercised and
- To reduce the impact of such an adverse event.

Step 5 : Likelihood Determination

- To derive an overall likelihood rating
- that indicates the probability
- that a potential vulnerability may be exercised
- within the associated threat environment,
- the following factors must be considered :
  - Threat-source motivation and capability (motivasi dan capability dr sumber ancaman)
  - Nature of the vulnerability
  - Existence and effectiveness of current controls

Likelihood Level

- High
- Medium
- Low

Likelihood Definitions

- Likelihood Level : High
- Likelihood Definition :
  - The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective

Likelihood Definitions

- Likelihood Level : Medium
- Likelihood Definition :
  - The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.

Likelihood Definitions

- Likelihood Level : Low
- Likelihood Definition :
  - The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Output from Step 5

- Likelihood rating :
  - High
  - Medium
  - Low

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.

Mission Impact Analysis

- It prioritizes the impact levels
- associated with the compromise of an organization's information assets
- based on a qualitative or quantitative assessment
- of the sensitivity and criticality of those assets.

Asset criticality assessment

- Identifies and prioritizes the sensitive and critical organization information assets :
  - Hardware
  - Software
  - Systems
  - Services
  - Related technology assets
- That support organization’s critical missions.

Responsibility

- The system & information owners are the ones responsible for determining the impact level for their own system and information.
- Consequently, in analyzing impact, the appropriate approach is to interview the system & information owner(s).

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

Good Luck