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 – 7 #7329-Dr. Gerry Firmansyah

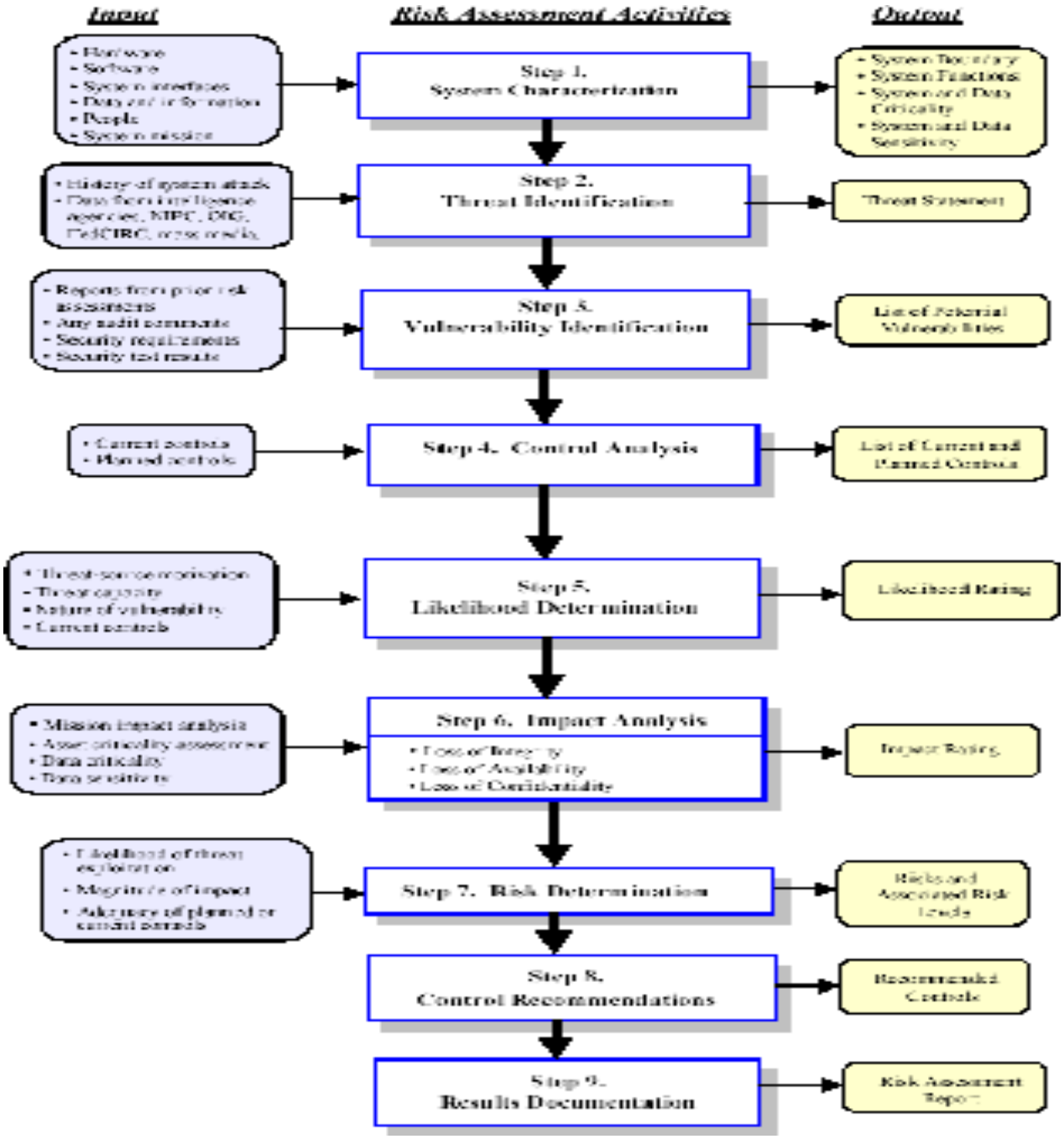
OUTLINE

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 3 : Vulnerability Identification

- The goal of this step is :
  - To develop a list of system vulnerabilities
    - Flaws
    - Weaknesses
  - ➢ That could be exploited by the potential threat-sources.

Vulnerability

- A flaw or weakness
- In :
  - System security procedures
  - Design
  - Implementation
  - Internal control
- That could be exercised
  - Accidentally triggered
  - Intentionally exploited
- Result in
  - A Security breach
  - A violation
- Of the system’s security policy

Example of Vulnerability/Threat Pair 1 of 4

- Vulnerability :
  - Terminated employees' system identifiers (ID) are not removed from the system
- Threat-source :
  - Terminated employees
- Threat Action :
  - Dialing into the company's network and accessing company proprietary data

Example of Vulnerability/Threat Pair 2 of 4

- Vulnerability :
  - Company firewall allows inbound telnet, and guest ID is enabled on XYZ server
- Threat-source :
  - Unauthorized users :
    - Hackers
    - Terminated employees
    - Computer criminals
    - Terrorists
- Threat Action :
  - Using telnet to XYZ server and browsing system files with the guest ID

Example of Vulnerability/Threat Pair 3 of 4

- Vulnerability :
  - The vendor has identified flaws in the security design of the system; however, new patches have not been applied to the system
- Threat-source :
  - Unauthorized users :
    - Hackers
    - Disgruntled employees
    - Computer criminals
    - Terrorists
- Threat Action :
  - Obtaining unauthorized access to sensitive system files based on known system vulnerabilities.

Example of Vulnerability/Threat Pair 4 of 4

- Vulnerability :
  - Data center uses water sprinklers to suppress fire; tarpaulins to protect hardware and equipment from water damage are not in place
- Threat-source :
  - Fire
  - Negligent persons
- Threat Action :
  - Water sprinklers being turned on in the data center

Recommended Methods

- For identifying system vulnerabilities are the use of :
  - Vulnerability sources
  - The performance of system security testing
  - The development of a security requirements checklist

Variety of the vulnerability identification

- The IT system has not yet been designed
- The IT system is being implemented
- The IT system is operational

If the IT system has not yet been designed

- The search for vulnerabilities should focus on :
  - The organization's security policies
  - The planned security procedures
  - The system requirement definitions
  - The vendors' or developers' security product analyses

If the IT system is being implemented

- The identification of vulnerabilities should be expanded to include more specific information :
  - The planned security features described in the security design documentation
  - The results of system certification test and evaluation

If the IT system is operational

- The process of identifying vulnerabilities should include an analysis of
  - The IT system security features
  - The IT system security controls
  - The IT system technical and procedural
    - Used to protect the system

Vulnerability Sources

- Can be identified via the information-gathering techniques
- A review of other industry sources
- The Internet
- Documented vulnerability sources

Documented Vulnerability Sources

- Previous risk assessment documentation of the IT system assessed
- Reports :
  - The IT system's audit
  - System anomaly
  - Security review
  - System test and evaluation
- Vulnerability lists
- Security advisories (arahan)
- Vendor advisories
- Commercial computer incident/emergency response teams and post lists
- Information Assurance Vulnerability Alerts and bulletins for military systems. Militer pemacu kemajuan teknologi
- System software security analyses

System Security Testing

- Proactive methods, employing system testing, can be used to identify system vulnerability efficiently, depending on :
  - The criticality of the IT system
  - Available resources :
    - Allocated funds
    - Available technology
    - Persons with the expertise to conduct the test

Test Method

-
  - Automated vulnerability scanning tool Security test and evaluation
- (ST&E) Penetration testing
-

➢ The results will help identify a system's vulnerabilities.

Automated Vulnerability Scanning Tool

- It is used to scan a group of hosts or a network for known vulnerable services :
  - System allows anonymous File Transfer Protocol (FTP)
- Some of the potential vulnerabilities identified by the automated scanning tool may not represent real vulnerabilities in the context of the system environment.
  - Some of these scanning tools rate potential vulnerabilities without considering the site's environments and requirements.

ST & E

- It includes the development and execution of a test plan
  - Test script
  - Test procedures
  - Expected test results
- The purpose is :
  - To test the effectiveness of the security controls of an IT system as they have been applied in an operational environment
  - To ensure that the applied controls :
    - Meet the approved security specification for the software and hardware
    - Implement the organization's security policy
    - Meet industry standards

Penetration Testing

- It can be used to complement the review of security controls
- It can ensure that different facets of the IT system are secured.
- It can be used to assess an IT system's ability to :
  - Withstand intentional attempts
  - Circumvent system security
- The objective is to :
  - Test the IT system from the viewpoint of a threat-source
  - Identify potential failures in the IT system protection schemes.

Development of Security Requirements Checklist

- During this step, the risk assessment personnel determine whether the security requirements
  - Stipulated for the IT system
  - Collected during system characterization
- ➢ Are being met by existing or planned security controls.
- The system security requirements can be presented in table form, with each requirement accompanied by an explanation of how the system design or implementation does or does not satisfy that security control requirement.

Security Requirement Checklist

- Contains the basic security standard that can be used to systematically
  - evaluate
  - identify
- The vulnerability of
  - Assets
    - personnel
    - hardware
    - software
    - information
  - Non automated procedures
  - Processes
  - Information transfers
  - associated with a given IT system in the following security areas :
    - Management
    - Operational
    - Technical

Security Criteria of Management Security

- Assignment of responsibilities
- Continuity of support
- Incident response capability
- Periodic review of security controls
- Personnel clearance and background investigations
- Risk assessment
- Security and technical training
- Separation of duties
- System authorization and reauthorization
- System or application security plan

Security Criteria of Operational Security

- Control of airborne contaminants (smoke, dust, chemicals)
- Controls to ensure the quality of the electrical power supply.
- Data media access and disposal
- External data distribution and labeling
- Facility protection (e.g., computer room, data center, office)
- Humidity control
- Workstations, laptops, and stand-alone personal computers

Security Criteria
of Technical Security

- Communication (e.g., dial-in, system
- interconnection, routers) Cryptography (pengacakan data)
- • Discretionary access control Identification and authentication
- (seseorg bisa masuk kalau pny id dan kewenangan)
  • Intrusion detection
-
- Object reuse (objek yang dipakai ulang, cth workstation, control monitor, satu workstation dapat digunakan untuk beberapa org/id, bahayanya : lupa keluar dari id, maka data dapat dilihat oleh orang lain)
- System audit

Outcome & Sources

- The outcome of this process is the security requirements checklist.
- Sources that can be used in compiling such a checklist include :
  - System security plan of the IT system assessed.
  - The organization's security policies, guidelines and standards.
  - Industry practices.
- The result of the checklist can be used as input for an evaluation of compliance and noncompliance.
- This evaluation process identifies :
  - System weaknesses
  - Process weaknesses
  - Procedural weaknesses

➢ That represent potential vulnerabilities.

Output from Step 3

- A list of the system vulnerabilities (observations) that could be exercised by the potential threat-sources.

Good Luck