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 – 5 #7329-Dr. Gerry Firmansyah

OUTLINE

I. Introduction

II. Risk Management Overview

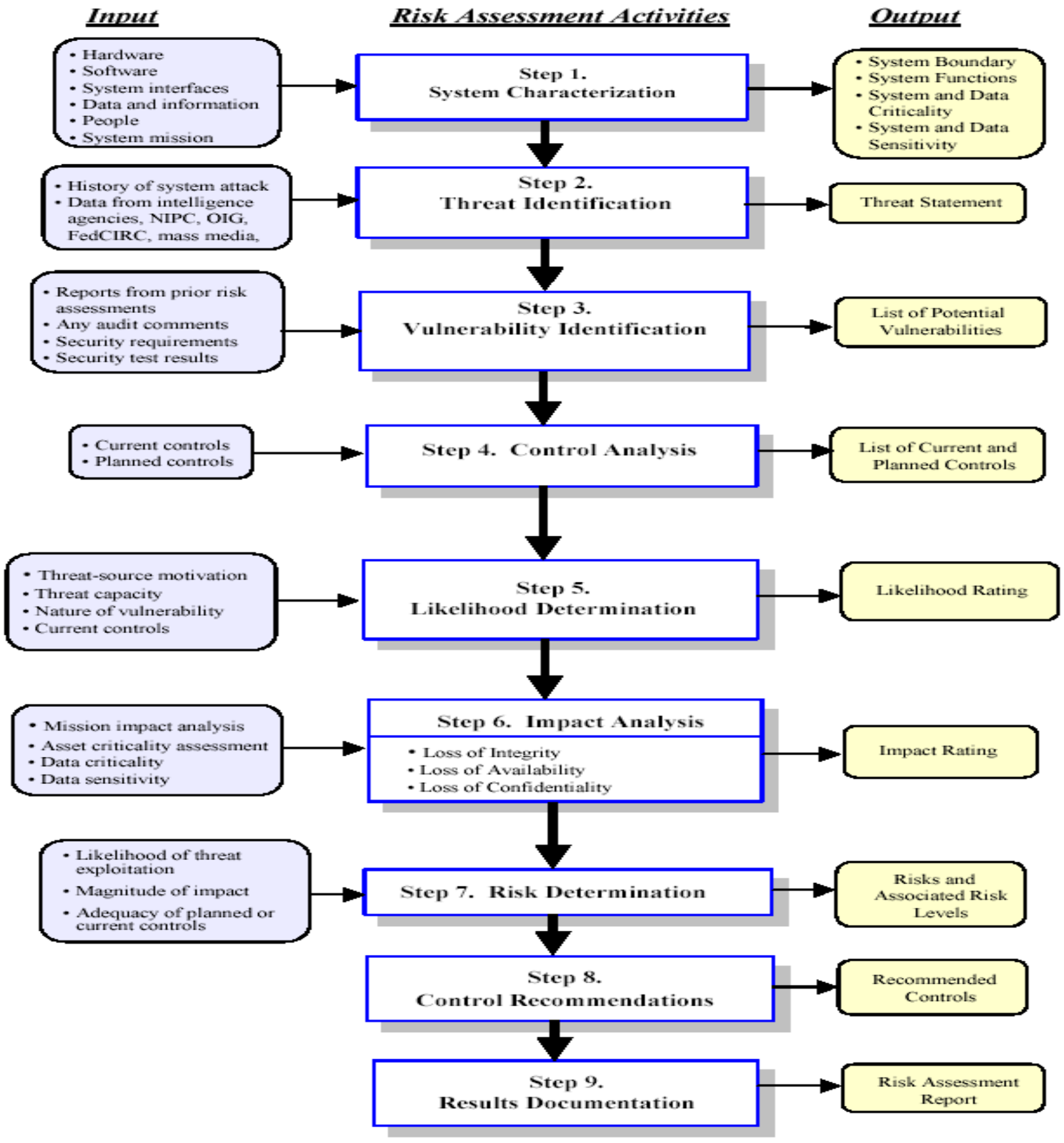
III. Risk Assessment

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


Input
Risk Assessment Activities
Output
• Hardware
• Software
• System interfaces
• Data and information
• People
• System mission
Step 1.
System Characterization
• System Boundary
• System Functions
• System and Data Criticality
• System and Data Sensitivity
• History of system attack
• Data from intelligence agencies, NIPC, OIG, FedCIRC, mass media,
Step 2.
Threat Identification
Threat Statement
• Reports from prior risk assessments
• Any audit comments
• Security requirements
• Security test results
Step 3.
Vulnerability Identification
List of Potential Vulnerabilities
• Current controls
• Planned controls
Step 4. Control Analysis
List of Current and Planned Controls
• Threat-source motivation
• Threat capacity
• Nature of vulnerability
• Current controls
Step 5.
Likelihood Determination
Likelihood Rating
• Mission impact analysis
• Asset criticality assessment
• Data criticality
• Data sensitivity
Step 6. Impact Analysis
• Loss of Integrity
• Loss of Availability
• Loss of Confidentiality
Impact Rating
• Likelihood of threat exploitation
• Magnitude of impact
• Adequacy of planned or current controls
Step 7. Risk Determination
Risks and Associated Risk Levels
Step 8.
Control Recommendations
Recommended Controls
Step 9.
Results Documentation
Risk Assessment Report

Information related to the operational environment

(1 of3)

- The functional requirements of the IT system
- Users of the system
  - System users who provide technical support to the IT system
  - Application users who use the IT system to perform business functions
- System security policies governing the IT system
  - Organizational policies
  - Regulatory requirements
  - Laws
  - Industry practices
- System security architecture
- Current network topology
  - network diagram

Information related to the operational environment

(2 of3)

- Information storage protection that safeguards
  - System and data availability
  - System and data integrity System
  - and data confidentiality
- Flow of information pertaining to the IT system
  - System interfaces
  - System input and output flowchart
- Technical controls used for the IT system
  - Built-in or add-on security product that supports identification and authentication
  - Discretionary or mandatory access control
  - Audit
  - Residual information protection
  - Encryption methods
- Management controls used for the IT system
  - Rules of behavior
  - Security planning

Information related to the operational environment

(3 of3)

- Operational controls used for the IT system
  - Personnel security
  - Backup
  - Contingency
  - Resumption and recovery operations
  - System maintenance
  - Off-site storage
  - User account establishment and deletion procedures
  - Controls for segregation of user functions :
    - Privileged user access
    - Standard user access
- Physical security environment of the IT system
  - Facility security Data
  - center policies
- Environmental security implemented for the IT system processing environment, e.g., controls for :
  - Humidity
  - Water Power
  - Pollution
  - Temperature
  - Chemicals
  -

For a system that is in the initiation or design phase

- System information can be derived from the design or requirements document.
- It is necessary to define :
  - Key security rules
  - Key security attributes
  - Planned for the future IT system
- System design documents and the system security plan can provide useful information about the security of an IT system that is in development

Foran operational IT system

- Data is collected about the IT system in its production environment, including data on:
  - System configuration
  - System connectivity
  - Documented and undocumented procedures
  - Documented and undocumented practices
- The system description can be based on the security provided :
  - By the underlying infrastructure
  - On future security plans for the IT system

Information-Gathering Techniques

Any, or a combination, of the following techniques can be used in gathering information relevant to the IT system within its operational boundary :

- Questionnaire
- On-site Interviews
- Document Review
- Use of Automated Scanning Tool.

Questionnaire

- To collect relevant information concerning:
  - The management controls
  - The operational controls
  - Planned or used for the IT system
- Should be distributed to
  - The applicable technical and non-technical management personnel who are designing or supporting the IT system.
- The questionnaire could also be used during on-site visits and interviews.

On-site Interviews

- Interviews with :
  - IT system support
  - Management personnel
- Collect useful information about IT system :
  - How the system is operated and managed
- Observe and gather information about :
  - Physical security of the IT system
  - Environmental security of the IT system
  - Operational security of the IT system
- Achieve a better understanding of the operational characteristics of an organization.
- For systems still in the design phase :
  - On-site visit would be face-to-face data gathering exercises
  - On-site visit could provide the opportunity to evaluate the physical environment In
  - which the IT system will operate

Document Review

- Good information about the security controls used by and planned for the IT system :
  - Policy documents
    - Legislative documentation
    - Directives
  - System documentation
    - System user guide
    - System administrative manual
    - System design and requirement document
    - Acquisition document
  - Security-related documentation
    - Previous audit report
    - Risk assessment report
    - System test results
    - System security plan
    - Security policies
- Information regarding system and data criticality and sensitivity :
  - An organization’s mission impact analysis An
  - organization’s asset criticality assessment

Use of Automated Scanning Tool

- Proactive technical methods can be used to collect system information efficiently.
- For example :
  - A network mapping tool :
    - Can identify the services that run on a large group of hosts
    - Can provide a quick way of building individual profiles of the target IT systems.

Output from Step 1

- Characterization of the IT system assessed
- A good picture of the IT system environment
- Delineation of system boundary

Step 2 : Threat Identification

- Threat :
  - The potential for a particular threat-source to successfully exercise a particular vulnerability
- Vulnerability :
  - Weakness that can be accidentally triggered or intentionally exploited.
- Threat-source :
  - Any circumstance or event with the potential to cause harm to an IT system.
    - Intent and method targeted at the intentional exploitation of a vulnerability A
    - situation and method that may accidentally trigger a vulnerability
- A threat-source does not present a risk when there is no vulnerability that can be exercised.
- Items that must be considered in determining the likelihood of a threat :
  - Threat-sources Potential
  - vulnerabilities Existing
  - controls

Threat-Source Identification

- To identify the potential threat-sources
  - To compile a threat statement listing potential threat- sources
  - That are applicable to the IT system being evaluated.
- The goal of this step is :

Good Luck