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 – 6 #7329-Dr. Gerry Firmansyah

OUTLINE

I. Introduction

II. Risk Management Overview

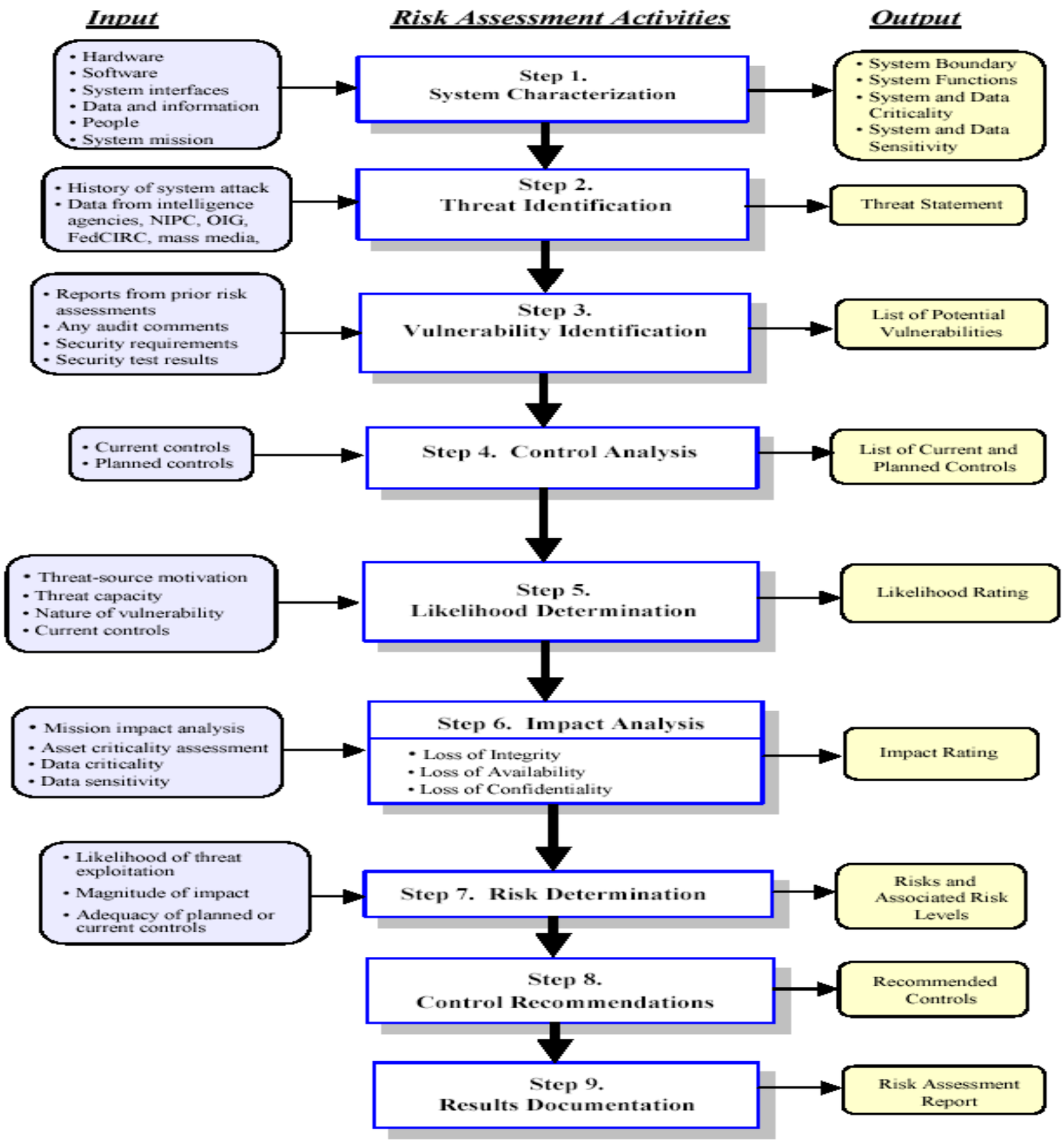
III. Risk Assessment

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

Threat-Source Identification

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

Common Threat-Sources

- Natural Threats
  - Floods
  - Earthquakes
  - Tornadoes
  - Landslides
  - Avalanches
  - Electrical storms
  - And other such events
- Human Threats
  - Events that are either enabled by or caused by human beings, such as :
    - Unintentional acts
      - Inadvertent data entry
    - Deliberate actions
      - Network based attacks
      - Malicious software upload
      - Unauthorized access to confidential information
- Environmental Threats
  - Long-term power failure
  - Pollution
  - Chemicals
  - Liquid leakage

In assessingthreat-sources

- It is important to consider
  - All potential threat-sources
  - Its processing environment
- For example :
  - An IT system located in a desert
  - Low likelihood of ‘natural flood’
  - A bursting pipe can quickly flood a computer room
- Humans can be threat-sources through :
  - Intentional acts :
    - A malicious attempt to gain unauthorized access to an IT system in order to compromise system and data integrity, availability, or confidentiality
    - A benign attempt to bypass system security
      - For example : a programmer’s writing a Trojan horse program.
  - Unintentional acts :
    - Negligence
    - errors

Motivation and ThreatActions

- Motivation and the resources for carrying out an attack make humans potentially dangerous threat-sources.
- This information will be useful to organizations :
  - Studying their human threat environments
  - Customizing their human threat statements

Additional information

- Reviews of the history of system break-ins
- Security violation reports
- Incident reports
- Interviews with
  - System administrators
  - Help desk personnel
  - User community
  - During information gathering
- Will help identify human threat-sources

Human Threat-Source

- Hacker, cracker
- Computer criminal
- Terrorist
- Industrial espionage
  - Companies
  - Foreign governments Other
  - government interests
- Insiders
  - Poorly trained
  - Disgruntled
  - Malicious
  - Negligent
  - Dishonest
  - Terminated employees

Hacker, Cracker

- Motivation :
  - Challenge
  - Ego
  - Rebellion
- Threat Actions :
  - Hacking
  - Social engineering
  - System intrusion, break-ins
  - Unauthorized system access

Computer Criminal

- Motivation :
  - Destruction on information
  - Illegal information disclosure
  - Monetary gain
  - Unauthorized data alteration
- Threat Actions :
  - Computer crime
    - Cyber stalking
  - Fraudulent act
    - Replay
    - Impersonation
    - Interception
  - Information bribery
  - Spoofing
  - System intrusion

Terrorist

- Motivation :
  - Blackmail
  - Destruction
  - Exploitation
  - Revenge
- Threat Actions :
  - Bomb/Terrorism
  - Information warfare
  - System attack
    - Distributed denial of service
  - System penetration
  - System tampering

Industrial Espionage

- Motivation :
  - Competitive advantage
  - Economic espionage
- Threat Actions :
  - Economic exploitation
  - Information theft
  - Intrusion on personal privacy
  - Social engineering
  - System penetration
  - Unauthorized system access
    - Access to classified information
    - Access to proprietary information
    - Access to technology-related information

Insiders

- Motivation :
  - Curiosity
  - Ego
  - Intelligence
  - Monetary gain
  - Revenge
  - Unintentional errors and omissions :
    - Data entry error
    - Programming error

Insiders

- Threat Actions :
  - Assault on an employee
  - Blackmail
  - Browsing of proprietary information
  - Computer abuse
  - Fraud and theft
  - Information bribery
  - Input of falsified, corrupted data
  - Malicious code :
    - Virus
    - Logic bomb
    - Trojan horse
  - Sale of personal information
  - System bugs
  - System intrusion
  - System sabotage
  - Unauthorized system access

After the potential threat-sources have been identified

- An estimate of the
  - Motivation
  - Resources
  - Capabilities
  - That may be required to carry out a successful attack
- Should be developed
- In order to determine the likelihood of a threat's exercising a system vulnerability.

After the potential threat-sources have been identified

- The threat statement, or the list of potential threat-sources
- Should be tailored
- To the individual organization and its processing environment
  - End-user computing habits.
- Information on natural threats
  - Floods
  - Earthquakes
  - Storms
- Should be readily available.

Additional information

- • Known threats have been identified by many government and private organizations.
- • Intrusion detection tools also are becoming more prevalent.
- • Government and industry organizations continually collect data on security events.
- • Sources of information :

  - Intelligence agencies
  - Mass media, particularly web-based resources such as SecurityFocus.com, SecurityWatch.com, SANS.org

➢ Improving the ability to realistically asses threats.

Output from Step2

- A threat statement containing a list of threat-sources that could exploit system vulnerabilities

Good Luck