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 – 4 #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

I/O of Step 1 –System Characterization

- Input
  - ❖ Hardware
  - ❖ Software
  - ❖ System Interfaces Data
  - ❖ and Information
  - ❖ People
  - ❖ System mission
- Output
  - ❖ System Boundary
  - ❖ System Functions
  - ❖ System and Data Criticality
  - ❖ System and Data Sensitivity

I/O of Step 2 –Threat Identification

- Input
  - History of system attack
  - Data from intelligence agencies, mass media
- Output
  - Threat Statement

I/O of Step 3 –Vulnerability Identification

- Input
  - ❖ Reports from prior risk assessments
  - ❖ Any audit comments
  - ❖ Security requirements
  - ❖ Security test results
- Output
  - ❖ List of Potential Vulnerabilities

I/O of Step 4 –Control Analysis

- Input
  - Current controls
  - Planned controls
- Output
  - List of Current and Planned Controls

I/O of Step 5 –Likelihood Determination

❖ Threat-source motivation Threat capacity

- Nature of vulnerability Current controls

- Input

❖

❖

❖

- Output

❖ Likelihood Rating

I/O of Step 6 –Impact Analysis

- List of impact :
  - Loss of Integrity
  - Loss of Availability
  - Loss of Confidentiality
- Input
  - Mission impact analysis
  - Asset criticality assessment
  - Data criticality
  - Data sensitivity
- Output
  - Impact Rating

I/O of Step 7 –RiskDetermination

- Input
  - Likelihood of threat exploitation
  - Magnitude of impact
  - Adequacy of planned or current controls
- Output
  - Risks and Associated Risk Levels

I/O of Step 8 –Control Recommendations

- Input
  - Results of Risk Determination Step.
- Output
  - Recommended Controls

I/O of Step 9 –Results Documentation

- Input
  - ❖ Results of Control Recommendation Step
- Output
  - ❖ Risk Assessment Report

Step 1 :System Characterization

- Identifies the boundaries of the IT systems :
  - ❖ Resources
  - ❖ Information
  - ➢ That constitute the system
- Establishes the scope of the risk assessment effort
- Delineates the operational authorization boundaries
- Provides information essential to defining the risk

The methodology of utilization

- Single or multiple, interrelated systems.
- Prior to applying the methodology :
  - ❖ The domain of interest
  - ❖ All interfaces
  - ❖ All dependencies Should
  - ➢ be well defined

System-Related Information

- Identifying risk for an IT system requires a keen understanding of the system’s processing environment.

System-Related Information Classification

- Hardware
- Software
- System interfaces (e.g., internal and external connectivity)
- Data and information
- Persons who support and use the IT system
- 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

Good Luck