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 – 3 #7329-Dr. Gerry Firmansyah

OUTLINE

I. Introduction

II. Risk Management Overview

III. Risk Assessment

IV. Risk Mitigation

V. Evaluation and Assessment

II. Risk Management Overview

Importance of Risk Management

Integration of Risk Management into SDLC Key

Roles

3. Key Roles

- Senior Management
- Chief Information Officer (CIO)
- System and Information Owners
- Business and Functional Managers
- ISSO (Information System Security Officers) IT
- Security Practitioners
- Security Awareness Trainers (Security/Subject Matter Professionals)

Senior Management

- Under the standard of due care.
- Under the ultimate responsibility for mission accomplishment.
- Must ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the mission.
- Must assess and incorporate results of the risk assessment activity into the decision making process.
- Is required to support and be involved in an effective risk management program that assesses and mitigate IT-related mission risks.

Chief Information Officer (CIO)

- Is responsible for the agency’s IT planning, budgeting, and performance including its information security components.
- Decisions made in these areas should be based on an effective risk management program.

System and Information Owners

- Are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of the IT systems and data they own.
- Are responsible for changes to their IT systems.
- Have to approve and sign off on changes to their IT systems (e.g., system enhancement, major changes to the software and hardware).
- Must understand their role in the risk management process and fully support this process.

Business and Functional Managers

- Managers who are responsible for
  - Business operations
  - IT procurement process
  - ➢ Must take an active role in the risk management process.
- These managers have
  - The authority
  - Responsibility
  - ➢ For making the trade-off decisions essential to mission accomplishment.
- Their involvement in the risk management process
  - Enables the achievement of proper security for the IT systems
- Which, if managed properly,
  - Will provide mission effectiveness With
  - minimal expenditure of resources

ISSO (Information System Security Officer)

- IT security program managers
- Computer security officers
- Are responsible for their organizations’ security programs, including risk management.
- They play a leading role in introducing
  - An appropriate methodology A
  - structured methodology To
  - help
    - Identify
    - Evaluate
    - Minimize
    - Risks to the IT systems
    - That support their organizations’ missions
- Also act as major consultants

this activity takes place on an ongoing basis

IT Security Practitioners

- Who :
  - Network administrators
  - System administrators
  - Application administrators
  - Database administrators
  - Computer specialists
  - Security analysts
  - Security consultants

IT Security Practitioners

- Job :
  - Are responsible for proper implementation of security requirements in their IT systems.
  - Must support or use the risk management process (as changes occur in the existing IT system environment) :
    - To identify and assess new potential risks To
    - implement new security controls
    - As needed to safeguard their IT systems.

Changes in the IT system environment

- Expansion in network connectivity
- Changes to the existing infrastructure
- Changes to the organizational policies
- Introduction of new technologies

Security Awareness Trainers (Security/Subject Matter Professionals)

- The users of the IT systems are the organization’s personnel Use
- of the IT systems and data according to
  - An organization’s policies An
  - organization’s guidelines
  - An organization’s rules of behavior
  - Is critical to mitigating risk and protecting the organization’s IT resources.
- It is essential that system and application users be provided with security awareness training to minimize risk to the IT systems.
- Therefore the IT security trainers must understand the risk management process so that they can develop
  - Appropriate training materials
  - Incorporate risk assessment into training programs To
  - educate the end users.

III. Risk Assessment

- Is the first process in the risk management methodology.
- Is used to determine the extent of
  - the potential threat and
  - the risk
  - associated with an IT system
  - throughout its SDLC.
- The output of this process helps to identify appropriate controls for
  - reducing risk or
  - eliminating risk
  - during the risk mitigation process.

Risk

- Is a function of
- The **likelihood**
  - Of a given **threat-source's**
  - Exercising a particular potential **vulnerability**
- And the resulting **impact**
  - Of that adverse event
- On the organization

Likelihood

To determine the likelihood of a future adverse event,

- Threats to an IT system must be analyzed
- In conjunction with :
  - the potential vulnerability and
  - the controls in place
  - for the IT system

Impact

- Impact refers to **the magnitude of harm** that could be caused by a threat's exercise of a vulnerability.
- The level of impact is governed by the potential mission impacts and in turn produces a relative value for the IT assets and resources affected :

- The criticality
- And sensitivity
- Of the IT system components and data

Good Luck