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 – 2 #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

1. Importance of Risk Management
2. Integration of Risk Management into SDLC Key
3. Roles

1. Importance of Risk Management

- Three processes :
  - Risk assessment
  - Risk mitigation
  - Evaluation and assessment
- Risk assessment
  - Identification and evaluation of risks and risk impacts
  - Recommendation of risk reducing measures
- Risk mitigation
  - Prioritizing
  - Implementing
  - Maintaining
  - ➢ The appropriate risk reducing measures recommended from the risk assessment process.
- Evaluation and assessment
  - Continual evaluation process
  - Keys for implementing a successful risk management program

DAA Responsibility

- DAA (Designated Approving Authority) or System Authorizing Official is responsible for determining
- whether the remaining risk is at an acceptable level or whether additional security controls should be
- implemented to further reduce or eliminate the residual risk

  before authorizing the IT system for operation.
-

Owners' Responsibility

- The head of organizational unit must ensure that the organization has the capabilities needed to accomplish its mission.
- The mission owners must determine the security capabilities that their IT systems must have to provide the desired level of mission support in the face of real world threats.

Risk Management

- Is the process
- That allows IT Managers
- To balance the operational and economic costs
  - Of protective measures
- And achieve gains
  - In mission capability
- By protecting the IT systems and data
- That support their organizations' missions.

Budget

- Most organizations have tight budgets for IT security
- Therefore IT security spending must be reviewed as thoroughly as other management decisions.

The Benefit of RiskManagement

- A well structured risk management methodology, when used effectively, can help management identify appropriate controls for providing the mission-essential security capabilities.

2. Integration of Risk Management into SDLC

- Effective risk management must be totally integrated into the SDLC An IT
- system's SDLC has five phases :
  - Initiation
  - Development or acquisition
  - Implementation
  - Operation or maintenance
  - Disposal
- In some cases, an IT system may occupy several of these phases at the same time.
- However, the risk management methodology is the same regardless of the SDLC phase for which the assessment is being conducted.
- Risk Management is an iterative process that can be performed during each major phase of the SDLC.

SDLC

- Phase 1 – Initiation
- Phase 2 – Development or Acquisition
- Phase 3 – implementation
- Phase 4 – Operation or Maintenance
- Phase 5 – Disposal

SDLC Phase 1 - Initiation

- Phase Characteristics
  - The need for an IT system is expressed and the purpose and scope of the IT system is documented
- Support from Risk Management Activities
  - Identified risks are used to support the development of the system requirements, including security requirements, and a security concept of operations (strategy)

SDLC Phase 2 – Development or Acquisition

- Phase Characteristics
  - The IT system is designed, purchased, programmed, developed, or otherwise constructed
- Support from Risk Management Activities
  - The risks identified during this phase can be used to support the security analyses of the IT system that may lead to architecture and design tradeoffs during system development

SDLC Phase 3 - Implementation

- Phase Characteristics
  - The system security features should be configured, enabled, tested, and verified
- Support from Risk Management Activities
  - The risk management process supports the assessment of the system implementation against its requirements and within its modeled operational environment. Decisions regarding risks identified must be made prior to system operation

SDLC Phase 4 – Operation or Maintenance

- Phase Characteristics
  - The system performs its functions. Typically the system is being modified on an ongoing basis through the addition of hardware and software and by changes to organizational processes, policies, and procedures
- Support from Risk Management Activities
  - Risk management activities are performed for periodic system reauthorization or whenever major changes are made to an IT system in its operational, production environment (e.g. new system interfaces)

SDLC Phase 5 - Disposal

- Phase Characteristics
  - The phase may involve the disposition of information, hardware, and software. Activities may include moving, archiving, discarding, or
  - destroying information and sanitizing the hardware and software
- Support from Risk Management Activities

- Risk management activities are performed for system components that will be disposed of or replaced to ensure that the hardware and software are properly disposed of, that residual data is appropriately handled, and that system migration is conducted in a secure and systematic manner

Thank You