Universitas Esa Unggul

Smart, Creative and Entrepreneurial

www.esaunggul.ac.id

CME 201 TOPIK DALAM IT GOVERNANCE

PERTEMUAN 14

PROGRAM STUDI MAGISTER ILMU KOMPUTER

FAKULTAS ILMU KOMPUTER

MANAJEMEN KINERJA DAN MANAJEMEN RISIKO DALAM TATA KELOLA IT

Pertemuan 14

INDIKATOR

Mahasiswa dapat :

- Memahami prinsip performance excellence
- Memahami konsep *key performance indicators* (KPI)
- Memahami konsep manajemen risiko, mitigasi, asesmen dalam tata kelola IT

Integration of Risk Management into the SDLC

Phase 1—Initiation	The need for an IT system is expressed and the purpose and scope of the IT system is documented	Identified risks are used to support the development of the system requirements, including security requirements, and a security concept of operations (strategy)
Phase 2—Development or Acquisition	The IT system is designed, purchased, programmed, developed, or otherwise constructed	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 trade- offs during system development
Phase 3—Implementation	The system security features should be configured, enabled, tested, and verified	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
Phase 4—Operation or Maintenance	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	Risk management activities are performed for periodic system reauthorization (or reaccreditation) or whenever major changes are made to an IT system in its operational, production environment (e.g., new system interfaces)
Phase 5—Disposal	This 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	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

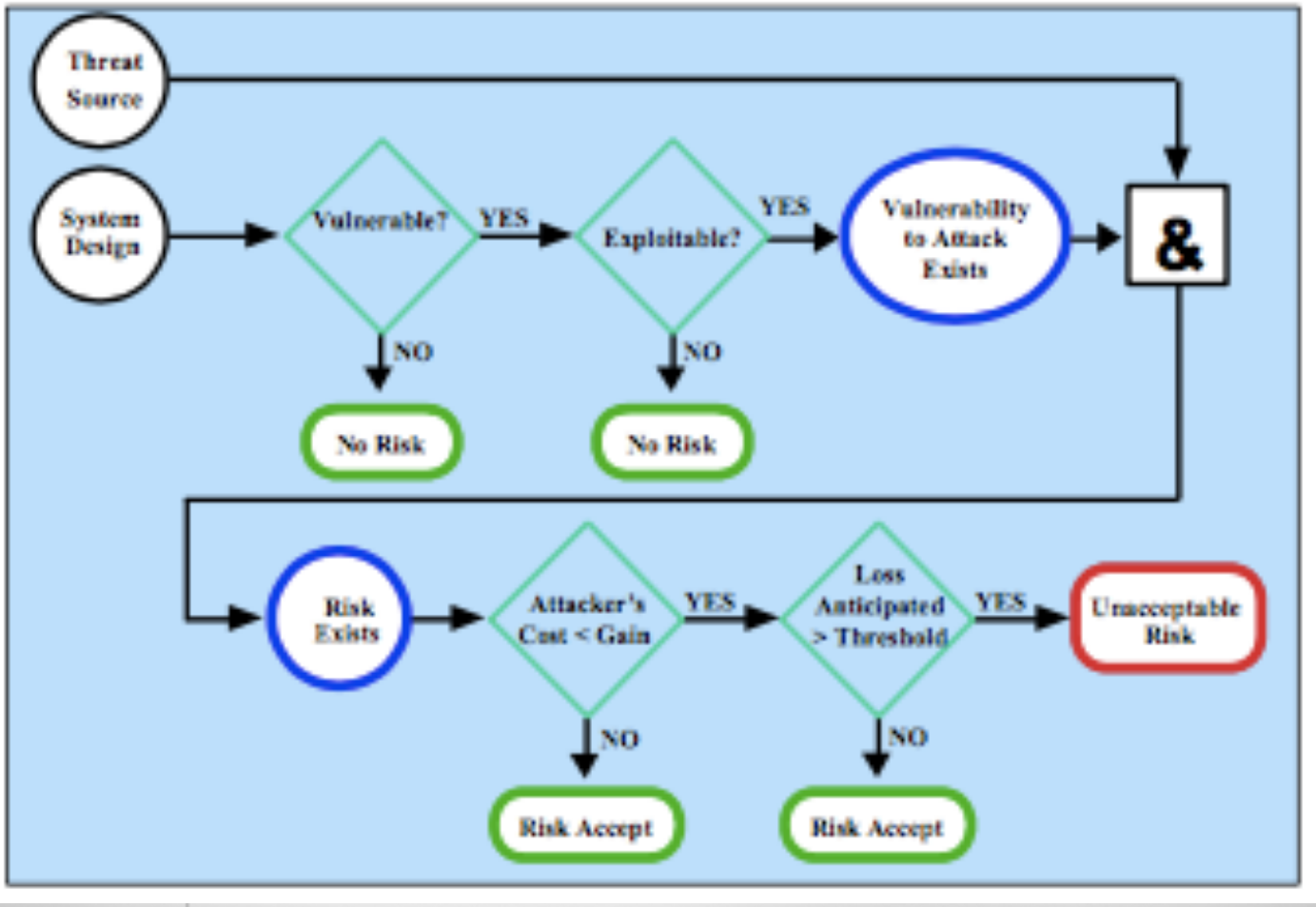
Risk Assessment Methodology (NIST 800-30)

- Step 1 System Characterization (Section 3.1)
- Step 2 Threat Identification (Section 3.2)
- Step 3 Vulnerability Identification (Section 3.3)
- Step 4 Control Analysis (Section 3.4)
- Step 5 Likelihood Determination (Section 3.5)
- Step 6 Impact Analysis (Section 3.6)
- Step 7 Risk Determination (Section 3.7)
- Step 8 Control Recommendations (Section 3.8)
- Step 9 Results Documentation (Section 3.9).

Risk Mitigation Options

- **Risk Assumption**. To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level
- **Risk Avoidance**. To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified)
- **Risk Limitation**. To limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls)
- **Risk Planning**. To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls
- **Research and Acknowledgment**. To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability
- **Risk Transference**. To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

Risk Mitigation Strategy



Approach For Control Implementation

- **Step 1 Prioritize Actions** : Output from Step 1 Actions ranking from High to Low
- **Step 2 Evaluate Recommended Control Options** : Output from Step 2 List of feasible controls
- **Step 3 Conduct Cost-Benefit Analysis** : Output from Step 3 Cost-benefit analysis describing the cost and benefits of implementing or not implementing the controls
- **Step 4 Select Control** : Output from Step 4 Selected control(s)
- **Step 5 Assign Responsibility** : Output from Step 5 List of responsible persons
- **Step 6 Develop a Safeguard Implementation Plan** : Output from Step 6 Safeguard implementation plan
- **Step 7 Implement Selected Control(s)** : Output from Step 7 Residual risk

TERIMA KASIH