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 – 11 #7329-Dr. Gerry Firmansyah

OUTLINE

I. Introduction

II. Risk Management Overview

III. Risk Assessment

IV. Risk Mitigation

V. Evaluation and Assessment

IV. Risk Mitigation

- Risk mitigation, the second process of Risk Management, involves :
  - Prioritizing
  - Evaluating
  - Implementing

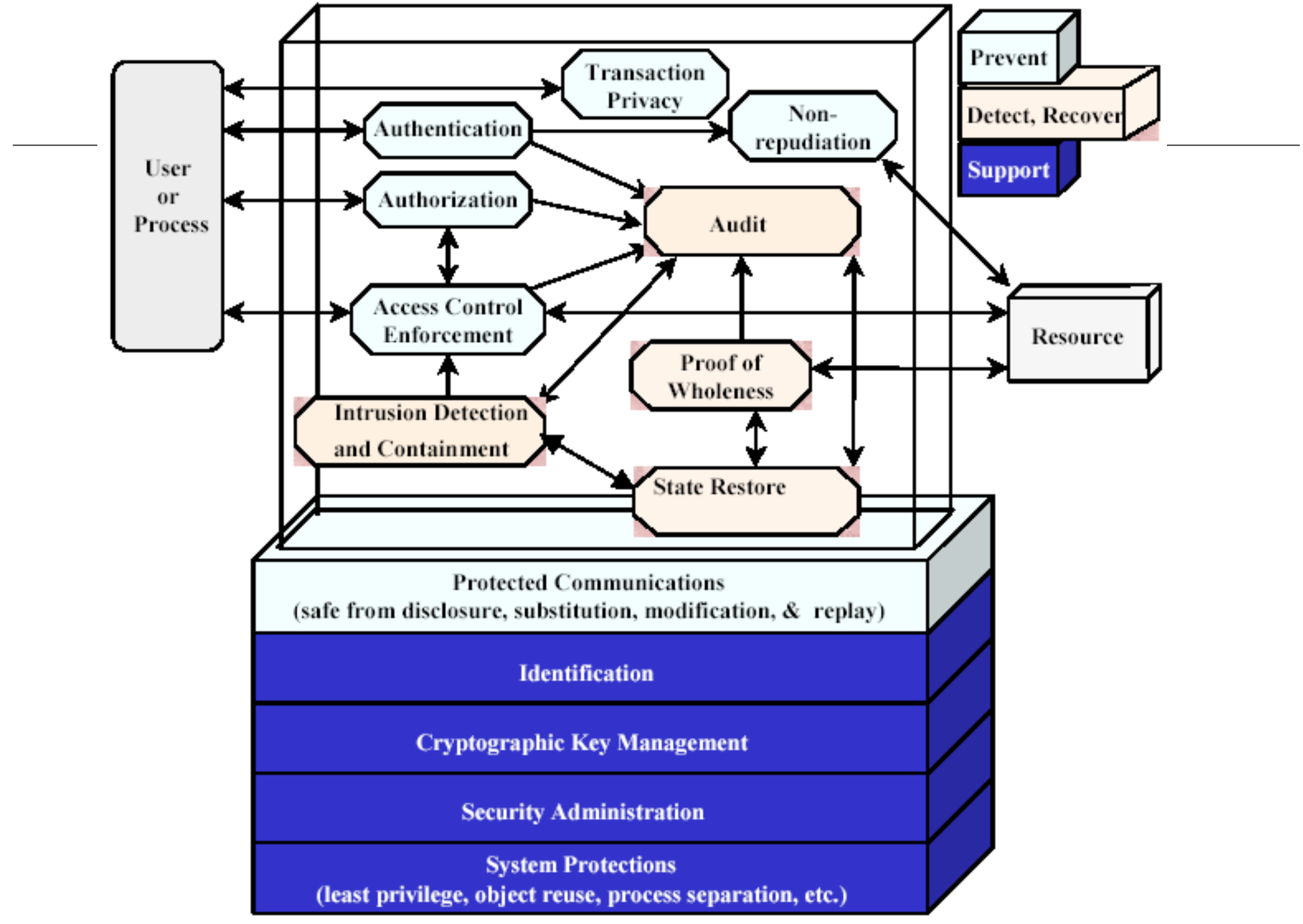
➢ The appropriate risk-reducing controls

➢ Recommended from the risk assessment process.

Items to discuss

1. Risk mitigation options
2. The risk mitigation strategy Approach
3. for control implementation Control
4. categories
5. The cost benefit analysis
6. Residual risk

y Controls Relationship



Supporting Technical Controls (1 of 2)

- Identification
  - This control provides the ability to uniquely identify :
    - Users
    - Processes
    - Information resources
  - To implement other security controls e.g. :
    - Discretionary Access Control (DAC)
    - Mandatory Access Control (MAC)
    - Accountability
    - It is mandatory that both subjects and objects be identifiable.
- Cryptographic Key Management
  - Cryptographic keys must be securely managed when cryptographic functions are implemented in various other controls.
  - Cryptographic key management includes :
    - Key generation
    - Key distribution
    - Key storage
    - Key maintenance

Supporting Technical Controls (2 of 2)

- Security Administration
  - The security features of an IT system must be configured :
    - To meet the needs of a specific installation
    - To account for changes in the operational environment
  - System security can be built into :
    - Operating system security
    - The application
- System protections
  - Underlying a system's various security functional capabilities is a base of confidence in the technical implementation.
  - This represents the quality of the implementation from the perspective both of :
    - The design processes used
    - The manner in which the implementation was accomplished.
  - Some examples of system protections are :
    - Residual information protection
    - Least privilege
    - Process separation
    - Modularity
    - Layering
    - Minimization of what needs to be trusted

Preventive Technical Controls (1 of 5)

- Authentication
  - This control provides the means of verifying the identity of a subject to ensure that a claimed identity is valid.
  - Authentication mechanism includes :
    - Passwords
    - Personal Identification Numbers (PINs)
    - Emerging authentication technology that provides strong authentication, e.g. :
      - Token
      - Smart card
      - Digital certificate
- Authorization
  - The authorization control enables
    - Specification
    - Subsequent management
    - Of the allowed actions for a given system, e.g. :
      - The information owner or the database administrator determines who can update a shared file accessed by a group of online users.

Preventive Technical Controls (2 of 5)

- Access Control Enforcement
  - Data integrity and confidentiality are enforced by access controls. When
  - the subject requesting for access has been authorized to access particular processes, it is necessary to enforce the defined security policy. These policy-based controls are enforced via access control
  - mechanism distributed throughout the system, e.g. :
    - MAC sensitivity labels DAC
    - file permission sets Access
    - control lists Roles
    -
    - User profiles
  - The effectiveness and the strength of access control depend on :
    - The access control decisions, e.g. :
      - How the security rules are configured
    - The strength of access control enforcement, e.g. :
      - The design of software or hardware security

Preventive Technical Controls (3 of 5)

- Nonrepudiation
  - System accountability depends on the ability to ensure that :
    - senders cannot deny sending information
    - receivers cannot deny receiving it
  - Nonrepudiation spans both :
    - prevention
    - detection.
- It has been placed in the prevention category in this guide because the mechanisms implemented prevent the successful repudiation of an action, e.g. :
  - The digital certificate that contains the owner’s private key is known only to the owner.
- As a result, this control is typically applied at the point of transmission or reception.

Preventive Technical Controls (4 of 5)

- Protected Communications
  - In a distributed system, the ability to accomplish security objectives is highly dependent on trustworthy communications.
  - The protected communications control ensures :
    - integrity
    - availability
    - confidentiality
    - of sensitive and critical information while it is in transit.
  - Protected communications use :
    - Data encryption methods
    - Deployment of cryptographic technologies To
    - minimize network threats, such as :
      - Replay
      - Interception
      - Packet sniffing
      - Wiretapping
      - eavesdropping

Preventive Technical Controls (5 of 5)

- Transaction Privacy
  - Both government and private sector systems are increasingly required to maintain the privacy of individuals.
  - Transaction Privacy Controls protect against loss of privacy with respect to transactions performed by individual.

Detection and Recovery TechnicalControls

(1 of4)

- Detection Controls warn of violations or attempted violations of security policy.
- Recovery Controls can be used to restore lost computing resources.
- They are needed as a complement to the supporting and preventive measures, because none of the measures in these other areas is perfect.
- DRTC includes :
  - Audit
  - Intrusion Detection and Containment
  - Proof of wholeness
  - Restore secure state
  - Virus detection and Eradication

Detection and Recovery TechnicalControls

(2 of4)

- Audit
  - Key elements in the after-the-fact
    - Detection of
    - Recovery from
    - Security breaches are :
      - The auditing of security-relevant events
      - The monitoring of system abnormalities
      - The tracking of system abnormalities
- Intrusion detection and Containment
  - Detect security breaches so that a response can occur in a timely manner.
  - Detect a security breach so that an effective response can be initiated.

Detection and Recovery TechnicalControls

(3 of4)

- Proof of wholeness
  - Analyzes system integrity
  - Analyzes system irregularities
  - Identifies exposure threats
  - Identifies potential threats
  - Does not prevent violation of security policy but:
    - Detects violation
    - Helps determine the type of correction action needed.
- Restore Secure State
  - Enables a system to return to a state that is known to be secure, after a security breach occurs.

Detection and Recovery TechnicalControls

(4 of4)

- Virus detection and Eradication
  - VDE software installed in a server or user workstation :
    - Detects Identifies
    - Removes
    - Software viruses
    -
  - To ensure system and data integrity

Management Security Controls (1 of 5)

- Management controls focus on the stipulation of :
  - Information protection policy
  - Information protection guidelines
  - Information protection standards

➢ Which are carried out through operational procedures To

➢ fulfill the organization’s goals and missions.

Management Security Controls

(2 of5)

- Preventive
- Detection
- Recovery

Management Security Controls

(3 of5)

- **Preventive** Management Security Controls :
  - Assign security responsibility to ensure that adequate security is provided for the mission-critical IT systems.
  - Develop and maintain system security plans to document current controls and address planned controls for IT systems in support of the organization's mission.
  - Implement personnel security controls, including :
    - separation of duties
    - least privilege
    - user computer access registration and termination
  - Conduct security awareness and technical training to ensure that end users and system users are aware of the rules of behavior and their responsibilities in protecting the organization's mission.

Management Security Controls

(4 of5)

- **Detection** Management Security Controls :
  - Implement personnel security controls, including
    - personnel clearance
    - background investigations
    - rotation of duties
  - Conduct periodic review of security controls to ensure that the controls are effective.
  - Perform periodic system audits.
  - Conduct ongoing risk management to assess and mitigate risk.
  - Authorize IT systems to address and accept residual risk.

Management Security Controls

(5 of5)

- Provide continuity of support
- **Recovery**, Management Security Controls
  - Develop, test, and maintain the continuity of operations plan to provide for business resumption
  - Ensure continuity of operations during emergencies or disasters.
- Establish an incident response capability to prepare for, recognize,
  - report, and respond to the incident and return the IT system to operational status.
  -

Good Luck