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 – 12 #7329-Dr. Gerry Firmansyah

OUTLINE

I. Introduction
II. Risk Management Overview
III. Risk Assessment
IV. Risk Mitigation
V. Evaluation and Assessment

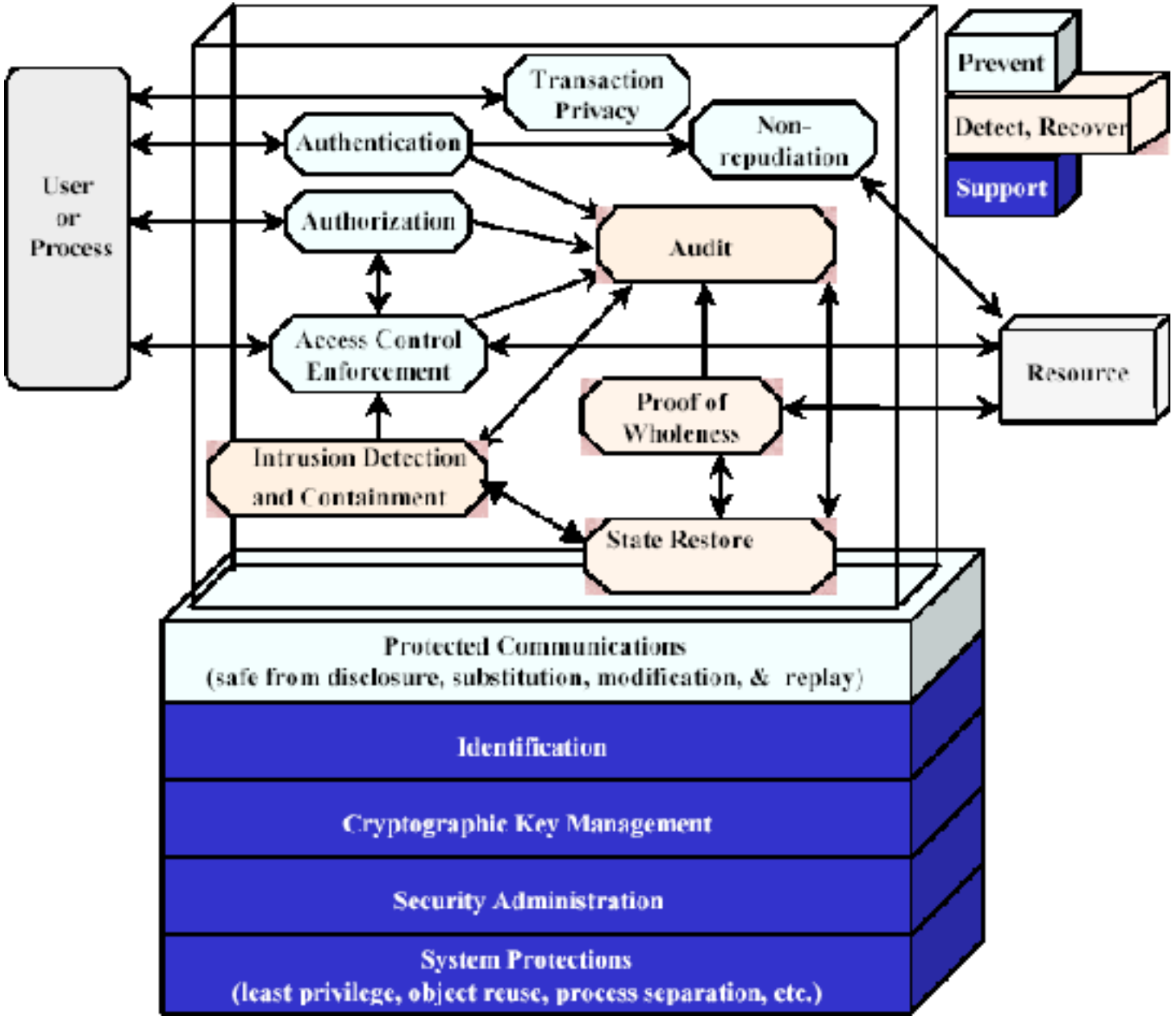
IV. Risk Mitigation

- 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
3. Approach for control implementation
4. Control categories
5. The cost benefit analysis
6. Residual risk

Technical Security Controls Relationship



Operational Security Controls (1 of 4)

- Operational controls, implemented in accordance with
  - a base set of requirements (e.g., technical controls)
  - good industry practices,
  - ➢ are used to correct operational deficiencies that could be exercised by potential threat-sources.
- To ensure consistency and uniformity in security operations,
  - ➢ step-by-step procedures and methods for implementing operational controls must be clearly
    - defined
    - documented
    - maintained.
- These operational controls includes :
  - Preventive Operational Security Controls
  - Detection Operational Security Controls

Operational Security Controls (2 of 4)

- Preventive Operational Controls :
  - Control data media access and disposal (e.g., physical access control, degaussing method)
  - Limit external data distribution (e.g., use of labeling)
  - Control software viruses
  - Safeguard computing facility, e.g. :
    - security guards
    - site procedures for visitors
    - electronic badge system
    - biometrics access control
    - management and distribution of locks and keys
    - barriers and fences
  - Secure wiring closets that house hubs and cables

Operational Security Controls (3 of 4)

- Preventive Operational Controls :
  - Provide backup capability e.g. :
    - procedures for regular data and system backups
    - archive logs that save all database changes to be used in various recovery scenarios
  - Establish off-site storage procedures and security
  - Protect laptops, personal computers (PC), workstations
  - Protect IT assets from fire damage :
    - requirements and procedures for the use of :
      - fire extinguishers
      - tarpaulins
      - dry sprinkler systems
      - halon fire suppression system
  - Provide emergency power source
    - requirements for uninterruptible power supplies
    - on-site power generators
  - Control the humidity and temperature of the computing facility
    - operation of air conditioners
    - operation of heat dispersal

Operational Security Controls (4 of 4)

- Detection Operational Controls :
  - Provide physical security :
    - use of motion detectors
    - closed-circuit television monitoring
    - sensors and alarms
  - Ensure environmental security :
    - use of smoke and fire detectors
    - sensors and alarms

5. Cost – Benefit Analysis (1 of 8)

- To allocate resources and implement cost-effective controls, organizations should conduct a cost-benefit analysis for each proposed control to determine which controls are required and appropriate for their circumstances.
- The cost-benefit analysis can be :
  - qualitative
  - quantitative
- Its purpose is to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk.
- For example, the organization may not want to spend $1,000 on a control to reduce a $200 risk.

Cost – Benefit Analysis (2 of 8)

- A cost-benefit analysis for proposed new controls or enhanced controls encompasses the following :
  - Determining the impact of implementing the new or enhanced controls
  - Determining the impact of *not* implementing the new or enhanced controls
  - Estimating the costs of the implementation. These may include, but are not limited to, the following:
    - Hardware and software purchases
    - Reduced operational effectiveness if system performance or functionality is reduced for increased security
    - Cost of implementing additional policies and procedures
    - Cost of hiring additional personnel to implement proposed policies, procedures, or services
    - Training costs
    - Maintenance costs
  - Assessing the implementation costs and benefits against system and data criticality to determine the importance to the organization of implementing the new controls, given their costs and relative impact.

Cost – Benefit Analysis (3 of 8)

- The organization will need to assess the benefits of the controls in terms of maintaining an acceptable mission posture for the organization.
- Just as there is a cost for implementing a needed control, there is a cost for not implementing it.
- By relating the result of not implementing the control to the mission, organizations can determine whether it is feasible to forgo its implementation.

Cost – Benefit Analysis (4 of 8)

- ***Cost-Benefit Analysis Example***:
  - System X stores and processes mission-critical and sensitive employee privacy information;
  - however, auditing has not been enabled for the system.
  - A cost benefit analysis is conducted to determine whether the audit feature should be enabled for System X

Cost – Benefit Analysis (5 of 8)

1) Impact of enabling system audit feature: pertimbangan jika sist audit dipasang
   - The system audit feature allows the system security administrator to monitor users' system activities
   - but will slow down system performance
   - ➢ therefore affect user productivity.
   - ➢ Also the implementation will require additional resources.
2) Impact of not enabling system audit feature: pertimbangan jika sist audit tdk dipasang
   - User system activities and violations cannot be monitored and tracked if the system audit function is disabled,
   - and security cannot be maximized to protect the organization's confidential data and mission.

Cost – Benefit Analysis (6 of 8)

3) Cost estimation for enabling the system audit feature:

• Cost for enabling system audit feature—No cost, built-in feature	$ 0
• Additional staff to perform audit review and archive, per year	$ XX,XXX
• Training (e.g., system audit configuration, report generation)	$ X,XXX
• Add-on audit reporting software	$ X,XXX
• Audit data maintenance (e.g., storage, archiving), per year	$ X,XXX
• Total Estimated Costs	$ XX,XXX

Cost – Benefit Analysis (7 of 8)

- Next Steps :
  - The organization's managers must determine what constitutes an acceptable level of mission risk.
  - The impact of a control may then be assessed.
  - The control either included or excluded, after the organization determines a range of feasible risk levels.
  - This range will vary among organizations.

Cost – Benefit Analysis (8 of 8)

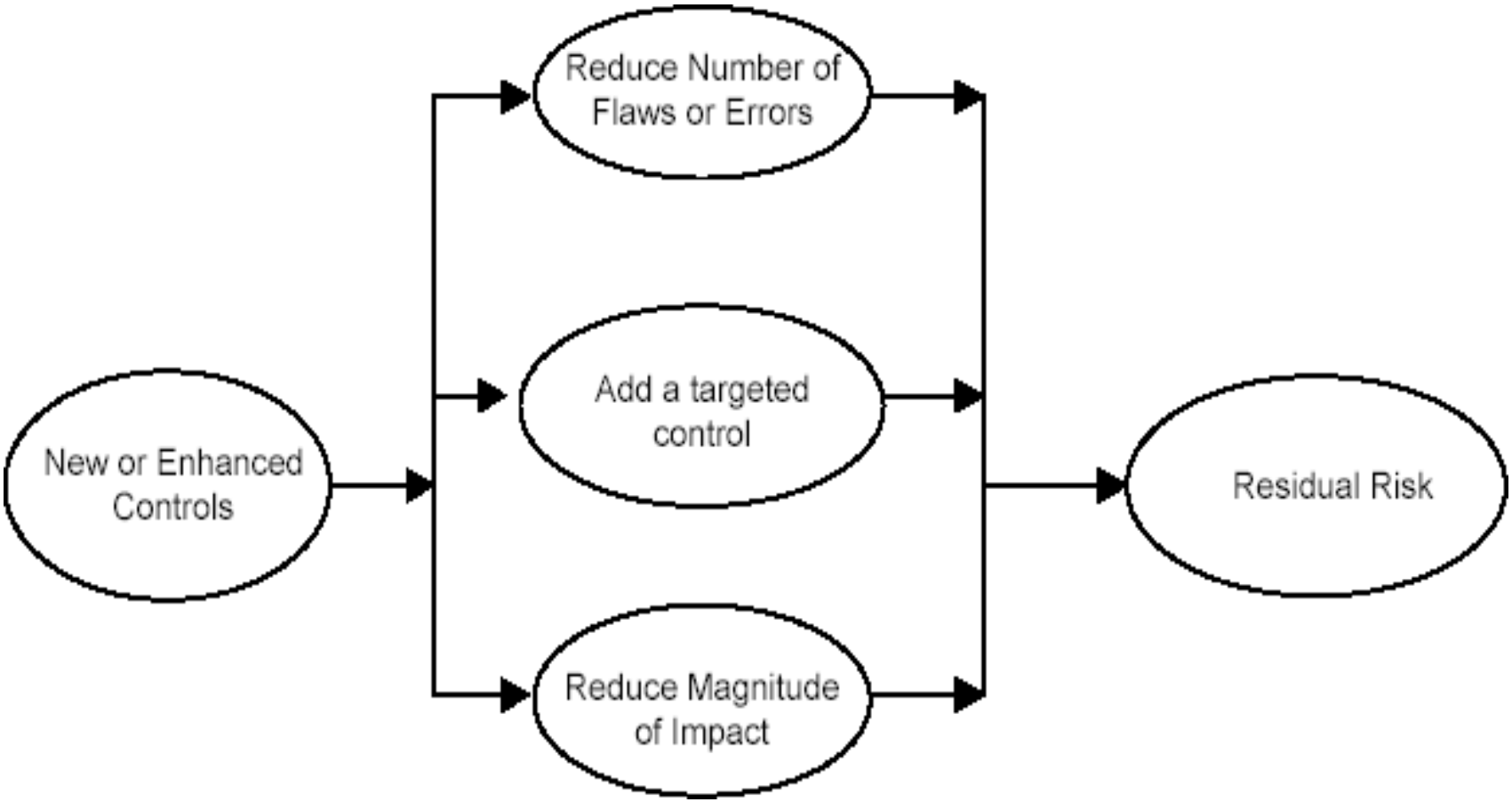
- The following rules apply in determining the use of new controls: pedoman pengambilan keputusan
  - If control would reduce risk more than needed, then see whether a less expensive alternative exists.
  - If control would cost more than the risk reduction provided, then find something else. Harga control lebih mahal drpd resiko
  - If control does not reduce risk sufficiently, then look for more controls or a different control. Tdk cukup bagus utk mengatasi risk. Pilih control yg lain
  - If control provides enough risk reduction and is cost-effective, then use it.

6. Residual Risk

Implementation of new or enhanced controls can mitigate risk by :

- Eliminating some of the system's vulnerabilities (flaws and weakness), thereby reducing the number of possible threat-source/vulnerability pairs.
- Adding a targeted control to reduce the capacity and motivation of a threat-source.
  - For example, a department determines that the cost for installing and maintaining add-on security software for the stand-alone PC that stores its sensitive files is not justifiable, but that administrative and physical controls should be implemented to make physical access to that PC more difficult (e.g., store the PC in a locked room with the key kept by the manager).
- Reducing the magnitude of the adverse impact
  - For example, limiting the extent of a vulnerability or modifying the nature of the relationship between the IT system and the organization's mission.

Implemented Controls and Residual Risk



Explanation (1 of 2)

- The risk remaining after the implementation of new or enhanced controls is the **residual risk**.
- Practically no IT system is risk free, and not all implemented controls can eliminate the risk they are intended to address or reduce the risk level to zero.
- An organization's senior management, who are responsible for protecting the organization's IT asset and mission, must authorize (or accredit) the IT system to begin or continue to operate.
- This authorization or accreditation must occur
  - at least every 3 years or
  - whenever major changes are made to the IT system.

Explanation (2 of 2)

- The intent of this process is
  - to identify risks that are not fully addressed and
  - to determine whether additional controls are needed to mitigate the risks identified in the IT system.
- After the appropriate controls have been put in place for the identified risks, the senior management will sign a statement
  - accepting any residual risk and
  - authorizing the operation of the new IT system or the continued processing of the existing IT system.
- If the residual risk has not been reduced to an acceptable level, the risk management cycle must be repeated to identify a way of lowering the residual risk to an acceptable level.

V. Evaluation & Assessment

- In most organizations :
  - the network itself will continually be expanded and updated
  - its components changed
  - its software applications replaced or updated with newer versions
  - personnel changes will occur
  - security policies are likely to change over time
- These changes mean that
  - new risks will surface
  - risks previously mitigated may again become a concern
- Thus, the risk management process is ongoing and evolving.

V.1. Good Security Practice

- The risk assessment process is usually repeated at least every 3 years.
- Risk management should be conducted and integrated in the SDLC for IT systems, not because it is required by law or regulation, but because it is a good practice and supports the organization's business objectives or mission.
- There should be a specific schedule for assessing and mitigating mission risks.
- The periodically performed process should also be flexible enough to allow changes where warranted,
  - such as major changes to the IT system and processing environment due to changes resulting from policies and new technologies.

V.2. Keys for Success

A successful risk management program will rely on :

- senior management's commitment;
- the full support and participation of the IT team
- the competence of the risk assessment team, which must
  - have the expertise to apply the risk assessment methodology to a specific site and system,
  - identify mission risks,
  - provide cost-effective safeguards that meet the needs of the organization,
- the awareness and cooperation of members of the user community, who must
  - follow procedures
  - comply with the implemented controls to safeguard the mission of their organization,
- an ongoing evaluation and assessment of the IT-related mission risks.

Good Luck