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 – 10 #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.

Responsibility

- The elimination of all risks is usually impractical or close to impossible.
- It is the responsibility of :
  - Senior Management
  - Functional managers
  - Business managers
  - To use the least-cost approach
  - To implement the most appropriate controls To
  - decrease mission risk to an acceptable level
  - With minimal adverse impact on the organization's resources and mission.

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

1. Risk MitigationOptions

- Risk mitigation is a systematic methodology used by senior management to reduce mission risk.
- It can be achieved through any of the following risk mitigation options :
  - Risk Assumption
  - Risk Avoidance
  - Risk Limitation
  - Risk Planning
  - Research and Acknowledgment
  - Risk Transference

Explanation (1 of 2)

- 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).

Explanation (2 of 2)

- 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.

Considerations

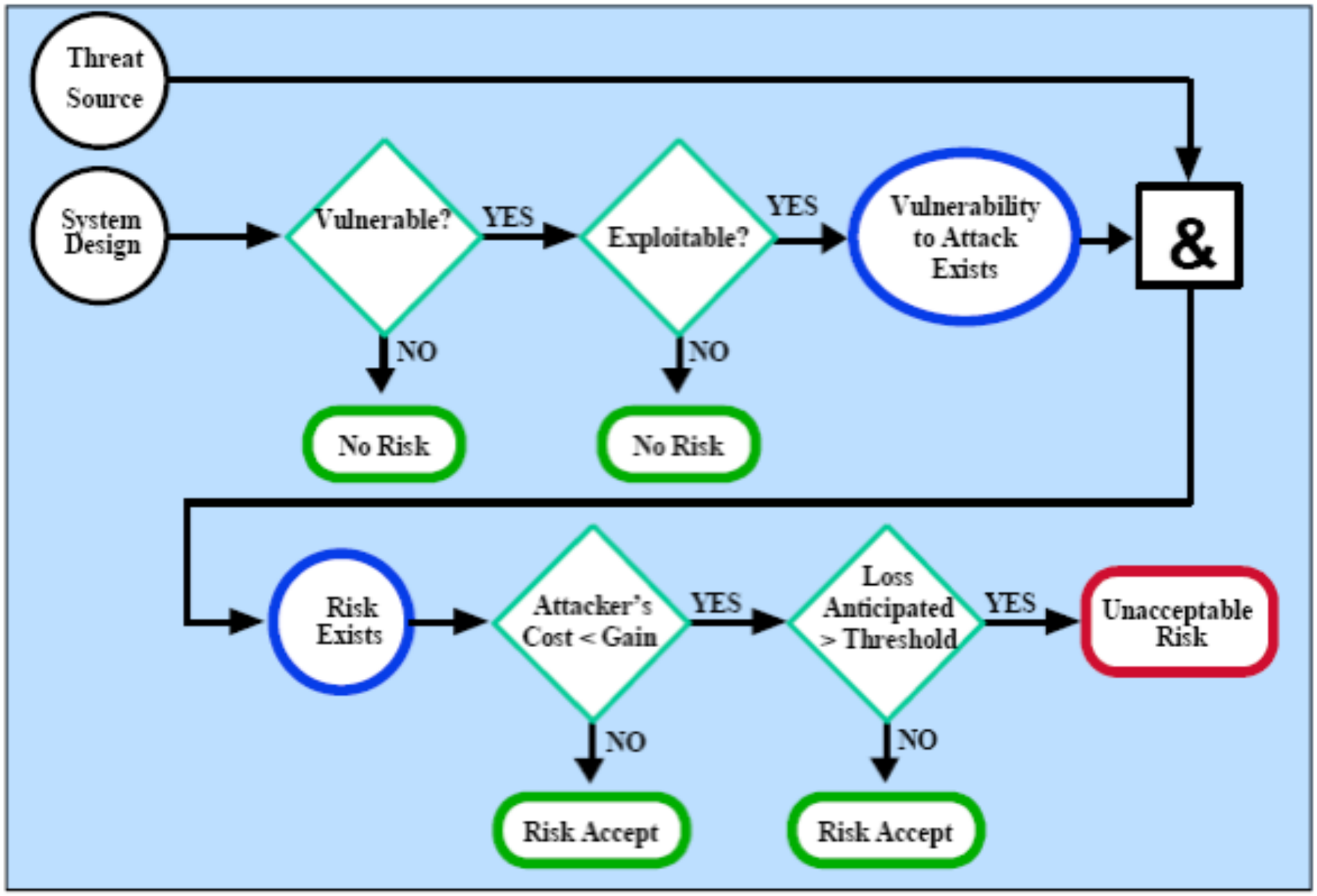
- The goals and mission of an organization should be considered in selecting any of these risk mitigation options.
  - It may not be practical to address all identified risks,
    - So priority should be given to the threat and vulnerability pairs that have the potential to cause significant mission impact or harm.
- Because of each organization's unique environment and objectives,
  - The option used to mitigate risk and the methods used to implement controls may vary.
- The best approach is :
  - To use appropriate technologies from among the various vendor security products,
  - with the appropriate risk mitigation option
  - and nontechnical, administrative measures.

2. Risk MitigationStrategy

Senior Management, the mission owners, knowing the potential risks and recommended controls, may ask :

- When and under what circumstances should I take actions?
- When shall I implement these controls to mitigate the risk and protect our organization?

Risk Mitigation ActionPoints



Guidance on actions to mitigate risks (1 of 2)

- When vulnerability (or flaw or weakness) exists :
  - Implement assurance techniques to reduce the likelihood of a vulnerability's being exercised.
- When a vulnerability can be exercised :
  - Apply :
    - layered protections,
    - architectural designs, and
    - administrative controls
  - to minimize the risk of or prevent this occurrence.

Guidance on actions to mitigate risks (2 of 2)

- When the attacker's cost is less than the potential gain :
  - Apply protections to decrease an attacker's motivation by increasing the attacker's cost (e.g., use of system controls such as limiting what a system user can access and do can significantly reduce an attacker's gain).
- When loss is too great :
  - Apply :
    - design principles,
    - architectural designs,
    - technical and non-technical protections
  - to limit the extent of the attack,
  - thereby reducing the potential of loss.

Additional explanation

- The previous strategy applies to risks from intentional human threats.
- Except the third list item, the strategy also applies to the mitigation of risks arising from environmental or unintentional human threat (e.g., system or human error), because there is
  - ❖ no ‘attacker’,
  - ❖ no motivation,
  - ❖ no gain
  - ➢ is involved.

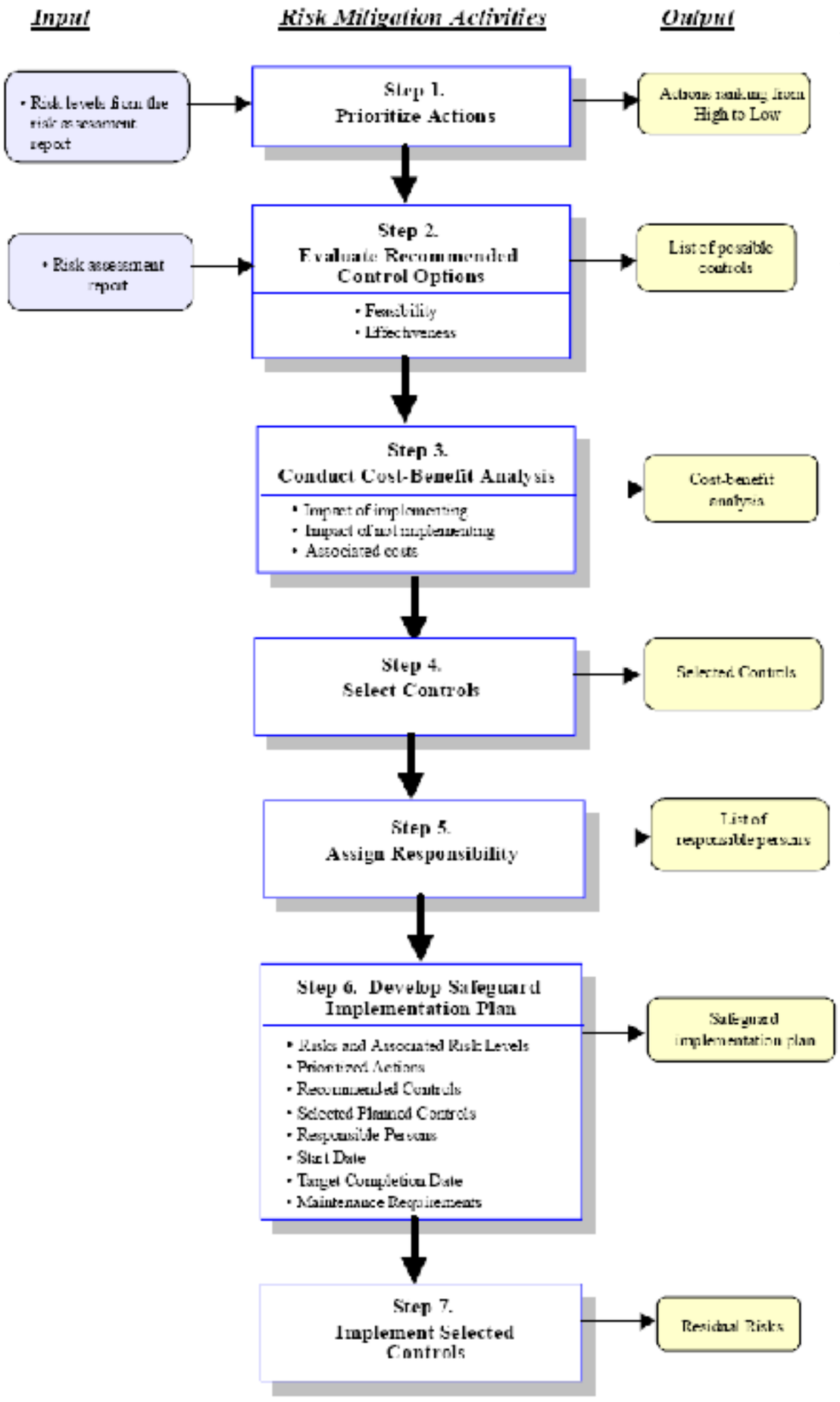
3. Approach for control implementation

The rule :

- Address the greatest risks
- Strive for sufficient risk mitigation
  - at the lowest cost
  - with minimal impact on other mission capabilities.

The Risk MitigationMethodology

- Step 1 : Prioritize Actions
- Step 2 : Evaluate Recommended Control Options
- Step 3 : Conduct Cost-Benefit Analysis
- Step 4 : Select Control
- Step 5 : Assign Responsibility
- Step 6 : Develop a Safeguard Implementation Plan
- Step 7 : Implement Selected Control(s)


Input
Risk Mitigation Activities
Output
• Risk levels from the risk assessment report
Step 1.
Prioritize Actions
Actions ranking from High to Low
• Risk assessment report
Step 2.
Evaluate Recommended Control Options
• Feasibility
• Effectiveness
List of possible controls
Step 3.
Conduct Cost-Benefit Analysis
• Impact of implementing
• Impact of not implementing
• Associated costs
Cost-benefit analysis
Step 4.
Select Controls
Selected Controls
Step 5.
Assign Responsibility
List of responsible persons
Step 6. Develop Safeguard Implementation Plan
• Risks and Associated Risk Levels
• Prioritized Actions
• Recommended Controls
• Selected Planned Controls
• Responsible Persons
• Start Date
• Target Completion Date
• Maintenance Requirements
Safeguard implementation plan
Step 7.
Implement Selected Controls
Residual Risks

Step 1 : Prioritize Actions

- • Based on the risk levels presented in the risk assessment report, implementation actions are prioritized.
- • In allocating resources, top priority should be given to risk items with unacceptably high risk rankings.
  - ❖ Risks assigned a Very High or High risk level.
- These vulnerability/threat pairs will require immediate corrective actions to protect an organization’s interest and mission.

Output from Step1

- Actions ranking from High to Low

Step 2 : Evaluate Recommended Control Options

- • Objective : select the most appropriate control option for minimizing risk.
- • The controls recommended may not be the most appropriate and feasible options for a specific organization and IT system.
- • They are analyzed :
  - Feasibility
    - Compatibility
    - User acceptance
  - Effectiveness
    - Degree of protection
    - Level of risk mitigation

Output from Step2

- List of feasible controls

Step 3 : Conduct Cost-Benefit Analysis

Objective :

- to aid management in decision making
- to identify cost effective controls

Section 5 details the objectives and method of conducting the cost-benefit analysis.

Output from Step3

- Cost-benefit analysis describing
  - The cost The
  - benefits

➢ of implementing or not implementing the controls.

Step 4 : Select Control

- Management determines :
  - **The most cost-effective control(s)**
  - For reducing risk to the organization's mission
  - Based on the results of the cost-benefit analysis.
- The controls selected should combine :
  - Technical control elements
  - Operational control elements
  - Management control elements
  - To ensure adequate security for the IT System and organization

Output from Step4

- Selected control(s)

Step 5 : Assign Responsibility

- Identify :
  - Appropriate persons who have :
    - The appropriate expertise
    - The appropriate skill-sets
  - To implement the selected controls.
- Assign :
  - responsibility

Output from Step5

- List of responsible persons

Step 6 : Develop a Safeguard Implementation Plan

The plan should, at a minimum, contain the following information :

- Risks (vulnerability/threat pairs) and associated risk levels (output from risk assessment report).
- Recommended controls (output from risk assessment report). Prioritized actions (with priority given to items with Very High and High risk level).
- Selected planned controls (determined in the basis of feasibility, effectiveness, benefits to the organization and cost).
- Required resources for implementing the selected planned controls. List of responsible teams and staff.
- Start date for implementation.
- Target completion date for the implementation.
- Maintenance requirements.
-

Output from Step6

- Safeguard implementation plan

Step 7 : Implement Selected Control(s)

- Depending on individual situations, the implemented controls may lower the risk level but not eliminate the risk.

Output from Step7

- Residual Risk

4. ControlCategories

- Introduction (1 of 2)
  - In implementing recommended controls to mitigate risk, an organization should consider :
    - Technical security control
    - Management security control
    - Operational security control
    - Combination of such controls
  - To maximize the effectiveness of controls for their IT system and organization.
  - Trade-offs that an organization will have to consider are illustrated by viewing the decisions involved in enforcing use of complex user password to minimize password guessing and cracking.

Comparison

- Introduction (2 of 2)
  - **A technical control** requiring add-on security software may be more complex and expensive than a procedural control,
    - But the technical control is likely to be more effective because the enforcement is automated by the system.
  - **A procedural control** might be implemented simply by means of a memorandum to all concerned individuals and an amendment to the security guidelines for the organization,
    - But ensuring that users consistently follow the memorandum and guideline will be difficult and will require security awareness training and user acceptance.

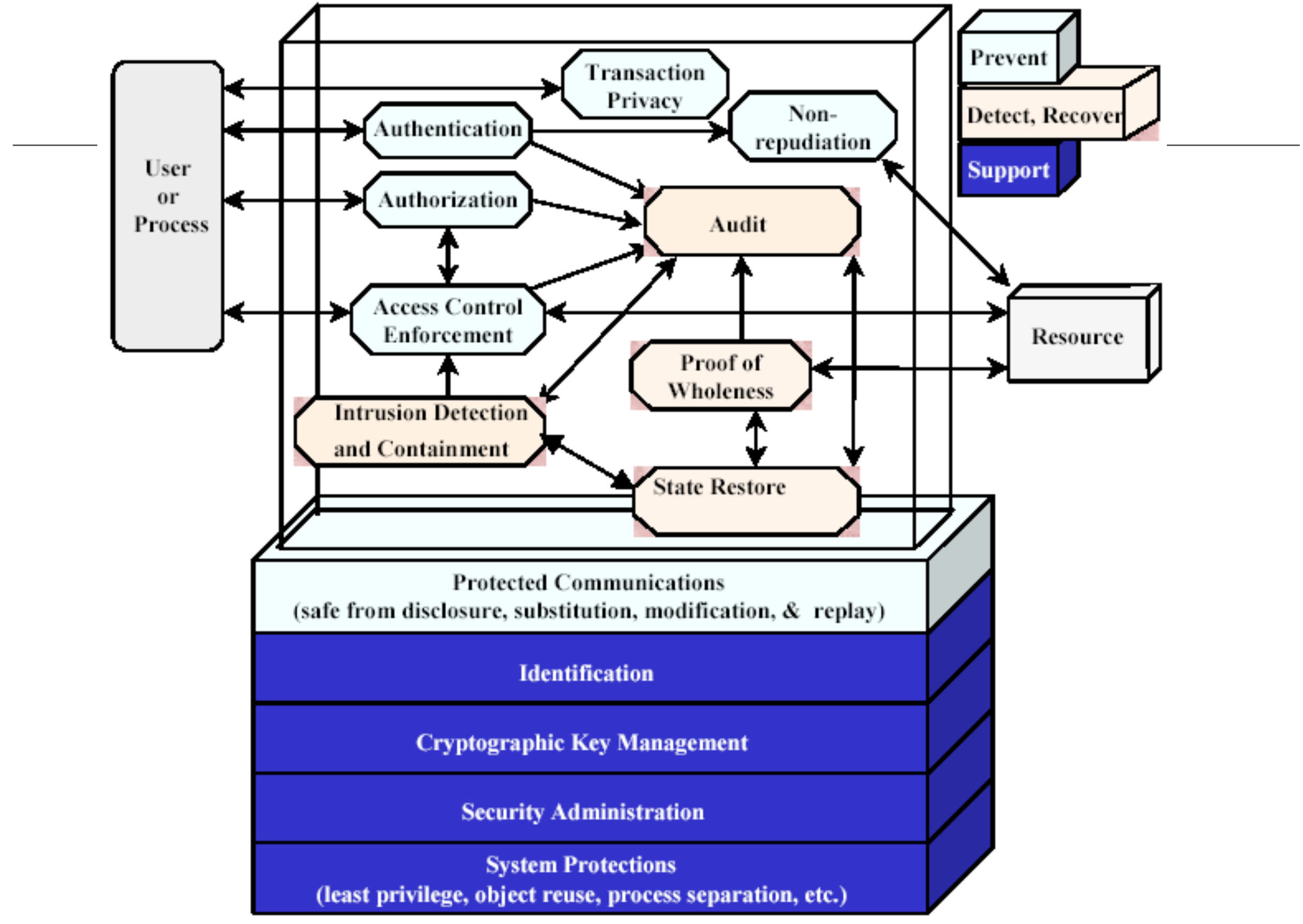
Technical Security Controls

- Range : simple to complex
- Items involved :
  - System Architectures
  - Engineering Disciplines
  - Security Packages
- Mix of :
  - Hardware
  - Software
  - Firmware
- All of these measures should work together to secure critical and sensitive :
  - Data
  - Information
  - IT system functions

Group of TechnicalControls

- Support
  - Supporting controls are generic and underlie most IT security capabilities.
  - These controls must be in place in order to implement other controls.
- Prevent
  - Preventive controls focus on preventing security breaches from occurring in the first place.
- Detect and Recover
  - These controls focus on detecting and recovering from a security breach.

y Controls Relationship



Supporting TechnicalControls

- 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

Good Luck