Security Controls & Safeguards

Ch. 15.2.

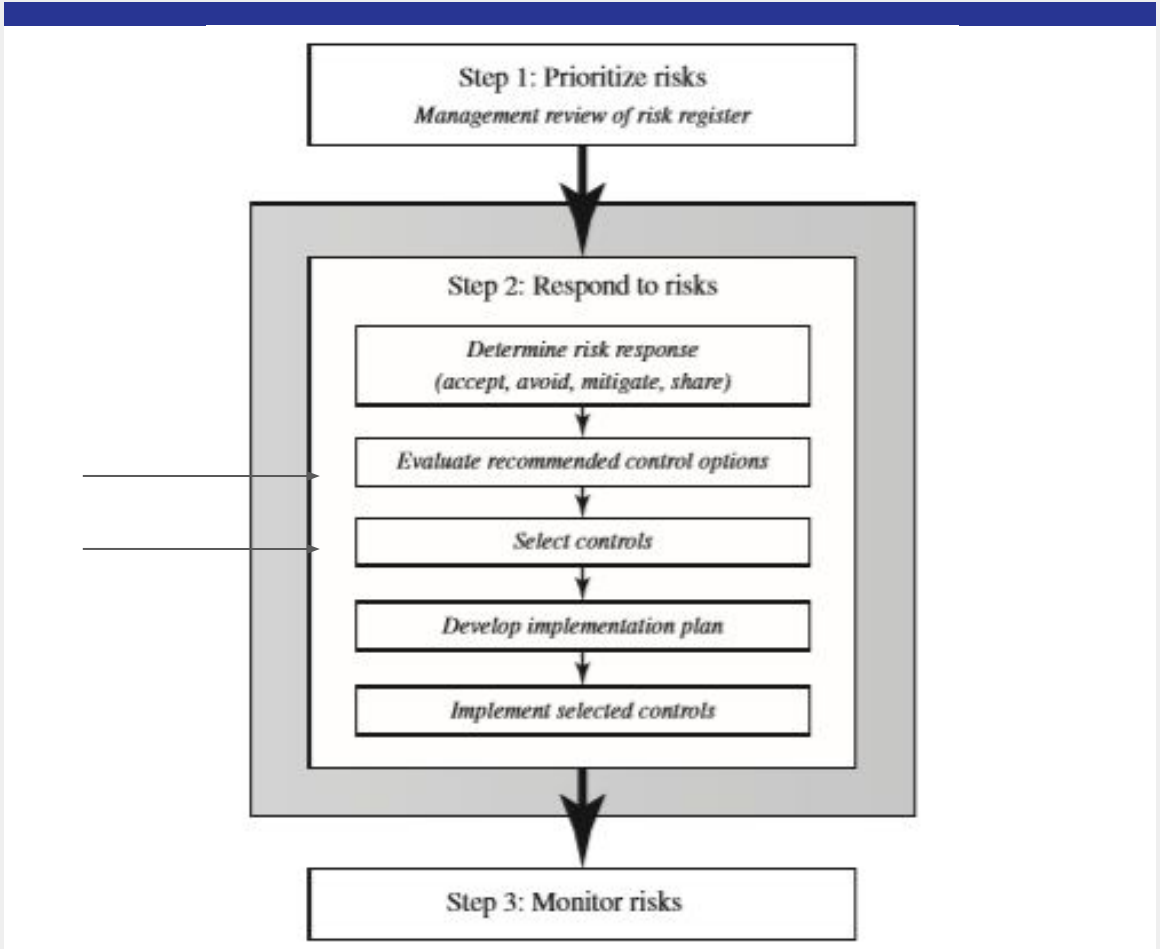
What is IT security control?

- If a risk assessment identifies areas that need “treatment”, then the security controls are used as part of the “treatment”.

- Control = safeguard = countermeasure help in reducing the risk by:
  - Preventing or eliminating a security violation
  - By minimizing the harm it can cause
  - By discovering and reporting it to enable corrective actions

IT Security Management
Controls and Implementation

Fig 15.1



Control classes

Management controls -> issues that management needs to address

Operational controls -> address the correct implementation of security policies and standards;

- Mechanisms and procedures that are primary implemented by people rather than systems.

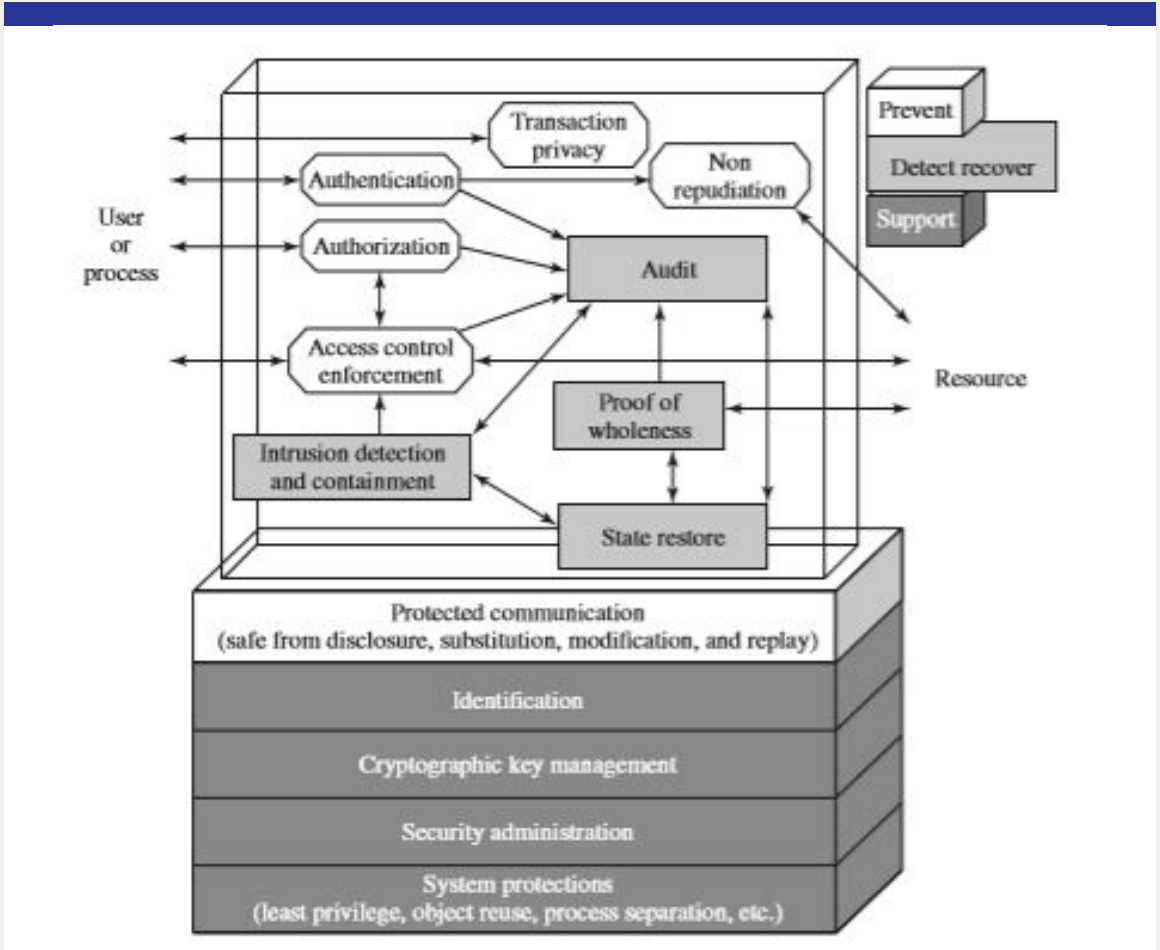
Technical controls -> correct use of hardware & software security capabilities is systems.

Control categories

1. Supportive controls
    a. Pervasive, generic, underlying technical IT security capabilities that are interrelated with, and used by, many other controls.
2. Preventive controls
    a. Focus on preventing security breaches from occurring
3. Detection & recovery controls
    a. Focus on the response to security breach
    b. Providing means to restore lost resources

Technical security control measures

Fig 15.2.



Different lists of controls

- Different national & international standards:
  - For information security management - ISO 27002
  - Management of information and communications technology security - FIPS 200
  - Recommended Security Controls for Federal Information Systems - SP 800-53
  - *Master list of controls*: ***ISO 27002*** (table 15.2, page 515).
- All these standards have overlapping categories of control
- Recommended:
  - Selecting the control categories needed for the organization & implemented across all IT systems for the organization.
  - Making adjustments for some of the systems

Recommended areas for adjustments

1. **Technology**
   - Some controls are applicable to certain technology
     i. Wireless network & use of cryptography
     ii. Readers for access token
   - Controls that cannot be implemented are substituted with alternating controls in other areas
     i. Administrative procedures
     ii. Physical access control
2. **Common controls**
   - Manage centrally
   - Keep consistency also when changing the controls
3. **Public access systems**
   - Organization’s web public server - access by general public
4. **Infrastructure controls**
   - Physical access or environmental controls - only relevant to areas that host the relevant equipment
5. **Scalability issues**
   - Controls vary in size based on company size and security needed
6. **Risk assessments**
   - Adjusting control based on certain risks that were assessed

Reduction of risk

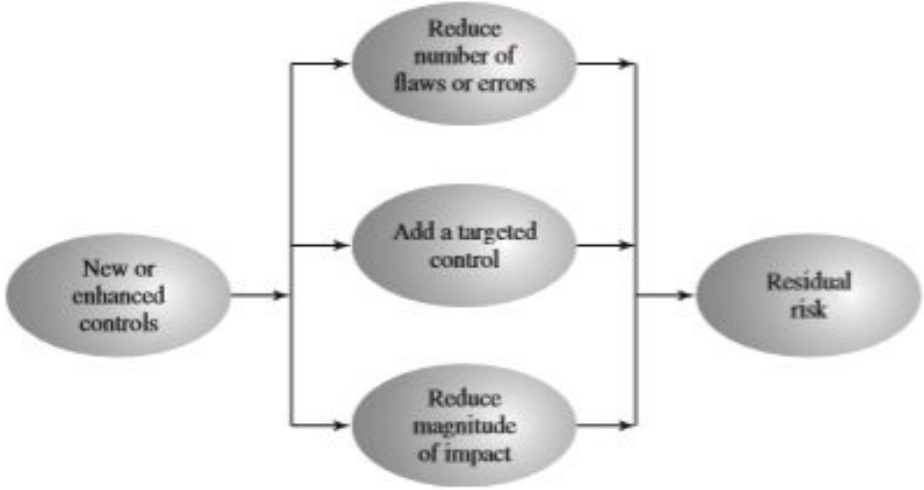


Figure 15.3 **Residual Risk**

Other important points:

1. Risk vs Cost of implementing the needed control
2. Usually the cost of the needed control is less than just not eliminating the assessed risk