Information Security (CS3002)

Instructor: Dr. Muhammad Usama

Email: usama.khanzada@nu.edu.pk

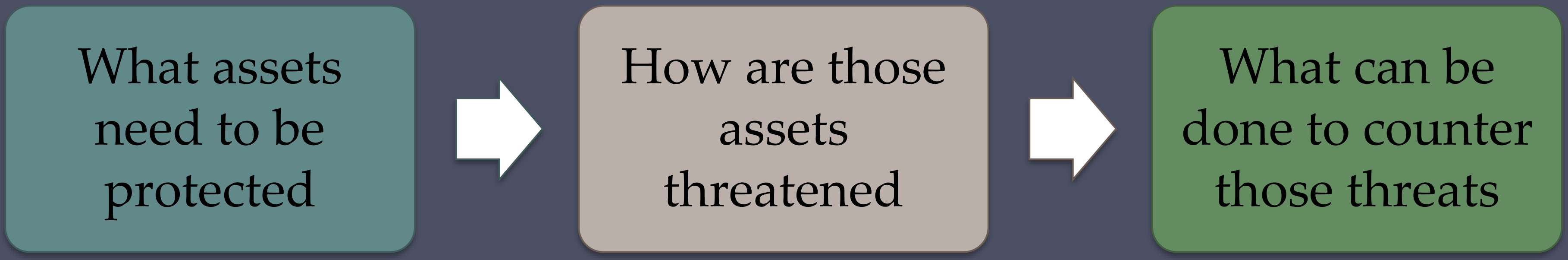
Book: Computer Security - Principles and Practice (Chapter 14)

IT Security Management

- and Risk Assessment

IT Security Management Overview

Is the formal process of answering the questions:



What assets need to be protected

How are those assets threatened

What can be done to counter those threats

- Ensures that critical assets are sufficiently protected in a cost-effective manner
- Security risk assessment is needed for each asset in the organization that requires protection
- Provides the information necessary to decide what management, operational, and technical controls are needed to reduce the risks identified

Table 14.1
ISO/IEC 27000 Series of Standards on IT Security Techniques

27000:2016	“Information security management systems - Overview and vocabulary” provides an overview of information security management systems, and defines the vocabulary and definitions used in the 27000 family of standards.
27001:2013	“Information security management systems – Requirements” specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System.
27002:2013	“Code of practice for information security management” provides guidelines for information security management in an organization and contains a list of best-practice security controls. It was formerly known as ISO17799.
27003:2010	“Information security management system implementation guidance” details the process from inception to the production of implementation plans of an Information Security Management System specification and design.
27004:2009	“Information security management – Measurement” provides guidance to help organizations measure and report on the effectiveness of their information security management system processes and controls.
27005:2011	“Information security risk management” provides guidelines on the information security risk management process. It supersedes ISO13335-3/4.
27006:2015	“Requirements for bodies providing audit and certification of information security management systems” specifies requirements and provides guidance for these bodies.

IT Security Management

IT SECURITY MANAGEMENT: A process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity, and reliability. IT security management functions include:

- **Determining organizational IT security objectives, strategies, and policies**
- **Determining organizational IT security requirements**
- **Identifying and analyzing security threats to IT assets within the organization**
- **Identifying and analyzing risks**
- **Specifying appropriate safeguards**
- **Monitoring the implementation and operation of safeguards that are necessary in order to cost effectively protect the information and services within the organization**
- **Developing and implementing a security awareness program**
- **Detecting and reacting to incidents**

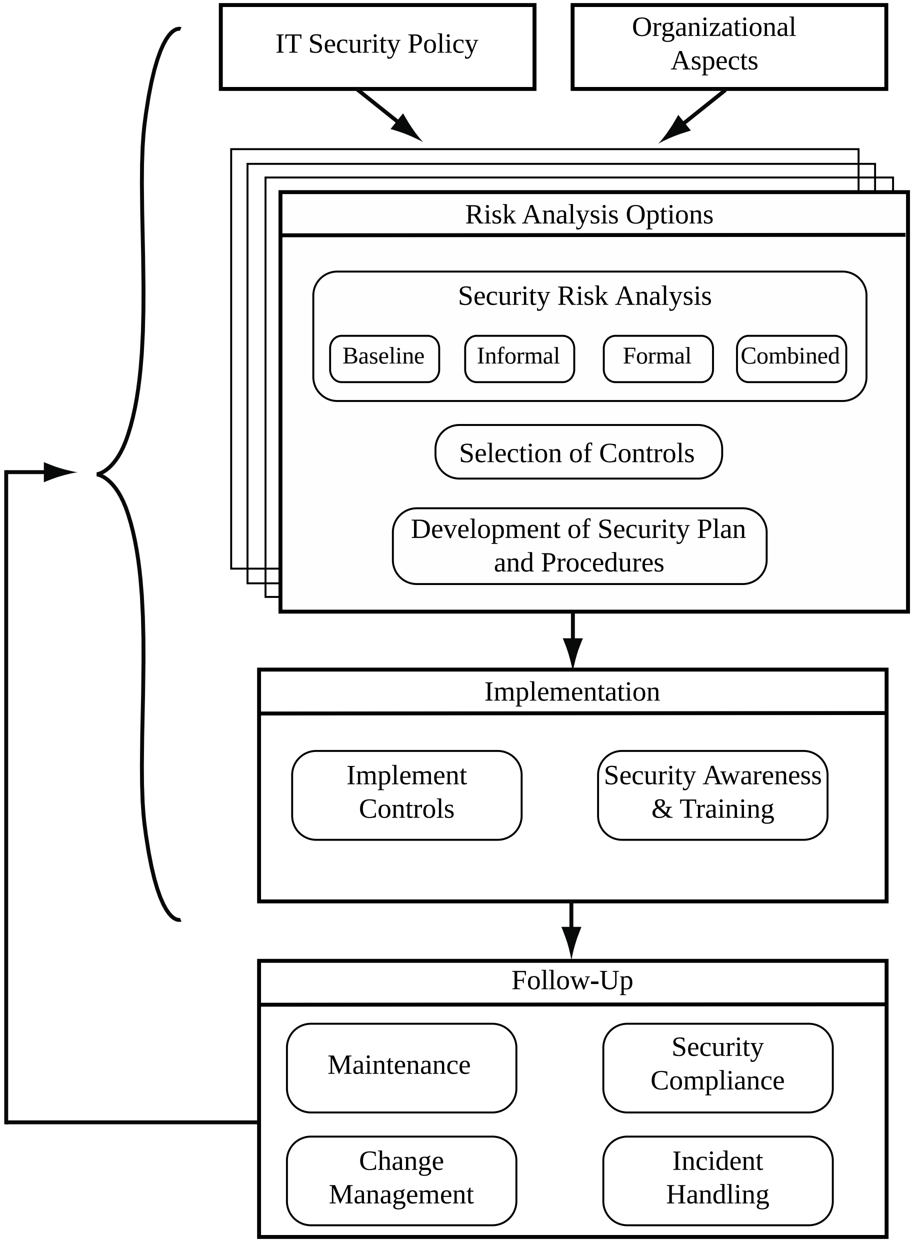


Figure 14.1 Overview of IT Security Management

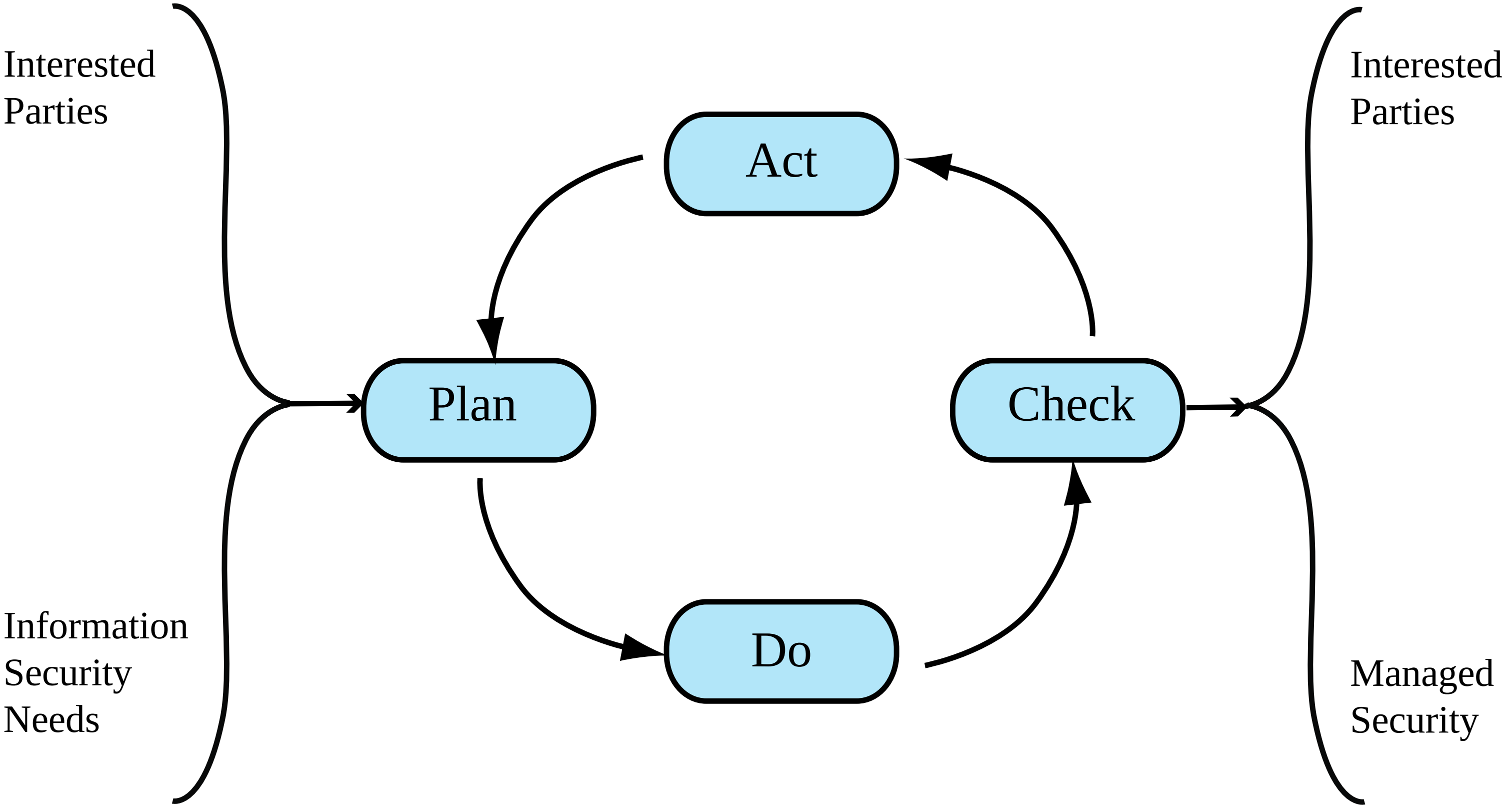
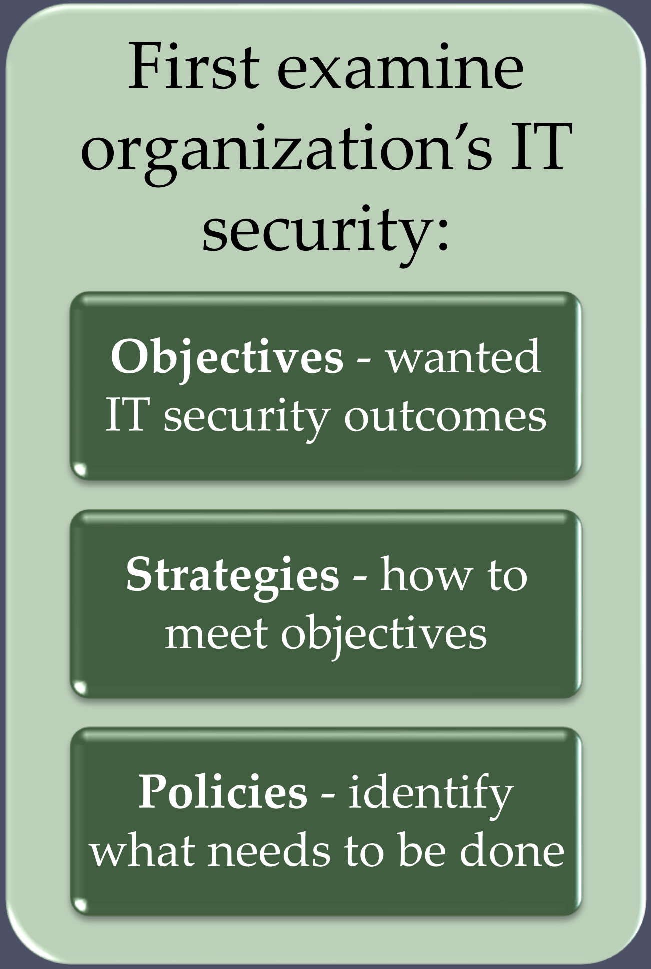


Figure 14.2 The Plan - Do - Check - Act Process Model

Organizational Context and Security Policy

- Maintained and updated regularly
  - Using periodic security reviews
  - Reflect changing technical/risk environments
- Examine role and importance of IT systems in organization



First examine organization's IT security:

Objectives - wanted IT security outcomes

Strategies - how to meet objectives

Policies - identify what needs to be done

Security Policy

Needs to address:

- Scope and purpose including relation of objectives to business, legal, regulatory requirements
- IT security requirements
- Assignment of responsibilities
- Risk management approach
- Security awareness and training
- General personnel issues and any legal sanctions
- Integration of security into systems development
- Information classification scheme
- Contingency and business continuity planning
- Incident detection and handling processes
- How and when policy reviewed, and change control to it

Management Support

- IT security policy must be supported by senior management
- Need IT security officer
  - To provide consistent overall supervision
  - Liaison with senior management
  - Maintenance of IT security objectives, strategies, policies
  - Handle incidents
  - Management of IT security awareness and training programs
  - Interaction with IT project security officers
- Large organizations need separate IT project security officers associated with major projects and systems
  - Manage security policies within their area

Security Risk Assessment

Critical component of process

Ideally examine every organizational asset

- Not feasible in practice

Approaches to identifying and mitigating risks to an organization's IT infrastructure:

- Baseline
- Informal
- Detailed risk
- Combined

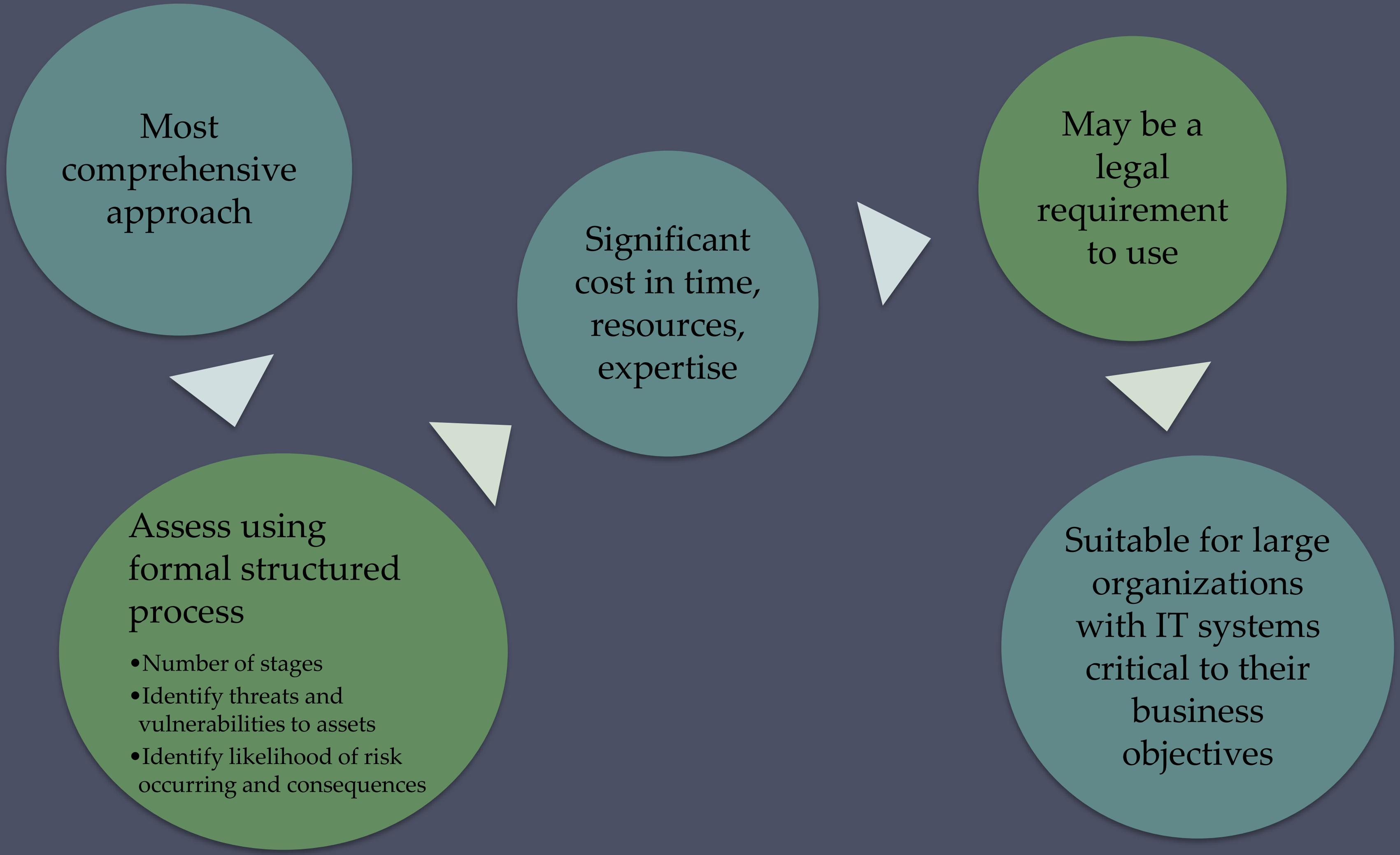
Baseline Approach

- Goal is to implement agreed controls to provide protection against the most common threats
- Forms a good base for further security measures
- Use “industry best practice”
  - Easy, cheap, can be replicated
  - Gives no special consideration to variations in risk exposure
  - May give too much or too little security
- Generally recommended only for small organizations without the resources to implement more structured approaches

Informal Approach

- Involves conducting an informal, pragmatic risk analysis on organization's IT systems
- Exploits knowledge and expertise of analyst
- Fairly quick and cheap
- Judgments can be made about vulnerabilities and risks that baseline approach would not address
- Some risks may be incorrectly assessed
- Skewed by analyst's views, varies over time
- Suitable for small to medium sized organizations where IT systems are not necessarily essential

Detailed Risk Analysis



Most comprehensive approach

Assess using formal structured process

- Number of stages
- Identify threats and vulnerabilities to assets
- Identify likelihood of risk occurring and consequences

Significant cost in time, resources, expertise

May be a legal requirement to use

Suitable for large organizations with IT systems critical to their business objectives

Combined Approach

- Combines elements of the baseline, informal, and detailed risk analysis approaches
- Aim is to provide reasonable levels of protection as quickly as possible then to examine and adjust the protection controls deployed on key systems over time
- Approach starts with the implementation of suitable baseline security recommendations on all systems
- Next, systems either exposed to high risk levels or critical to the organization's business objectives are identified in the high-level risk assessment
- A decision can then be made to possibly conduct an immediate informal risk assessment on key systems, with the aim of relatively quickly tailoring controls to more accurately reflect their requirements
- Lastly, an ordered process of performing detailed risk analyses of these systems can be instituted
- Over time, this can result in the most appropriate and cost-effective security controls being selected and implemented on these systems

Summary

- IT security management
- Organizational context and security policy
- Security risk assessment
    - Baseline approach
    - Informal approach
    - Detailed risk analysis
    - Combined approach