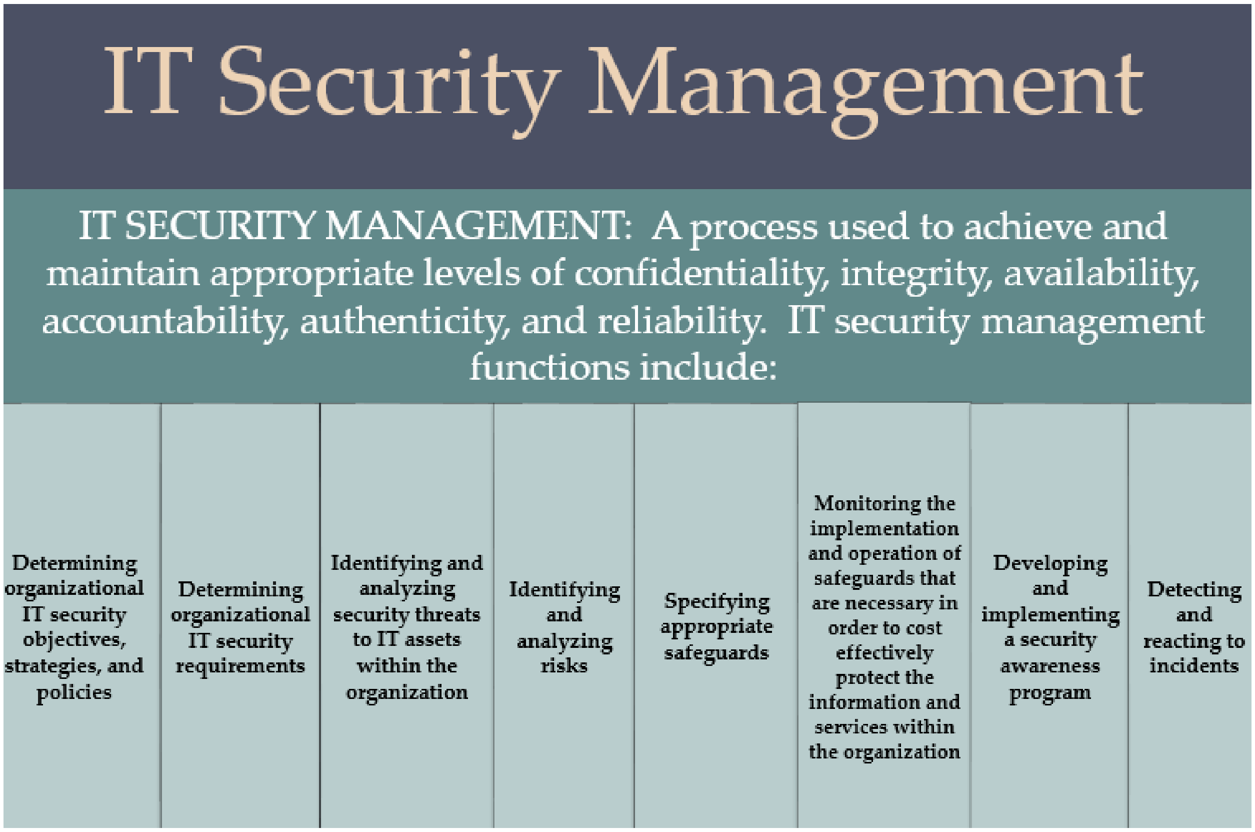
Chapter 14(14.1, 14.2, 14.3)



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

Plan: Establish security policy, objectives, processes, and procedures; perform risk assessment; develop risk treatment plan with appropriate selection of controls or acceptance of risk.

Do: Implement the risk treatment plan.

Check: Monitor and maintain the risk treatment plan.

Act: Maintain and improve the information security risk management process in response to incidents, review, or identified changes.

This process is illustrated in Figure 14.2, which can be aligned with Figure 14.1.

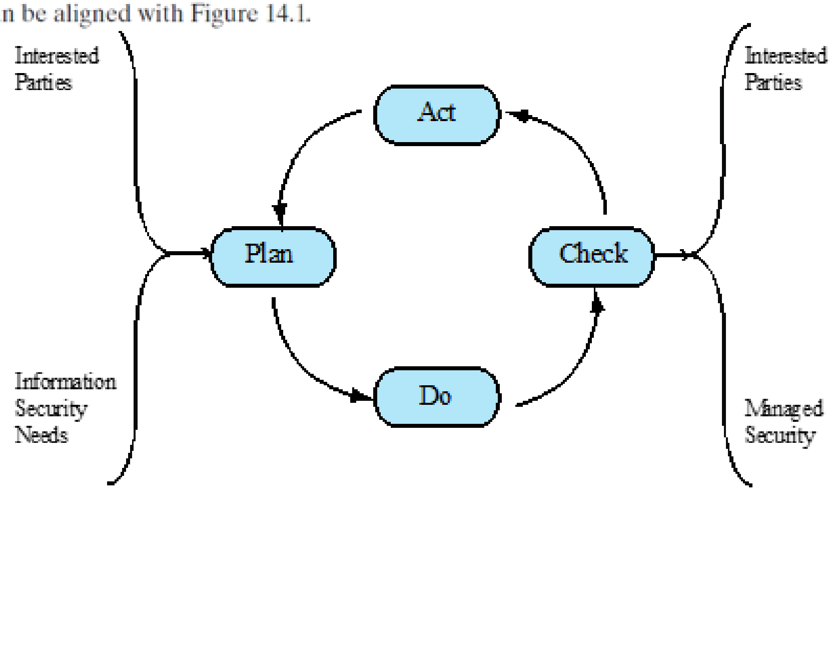
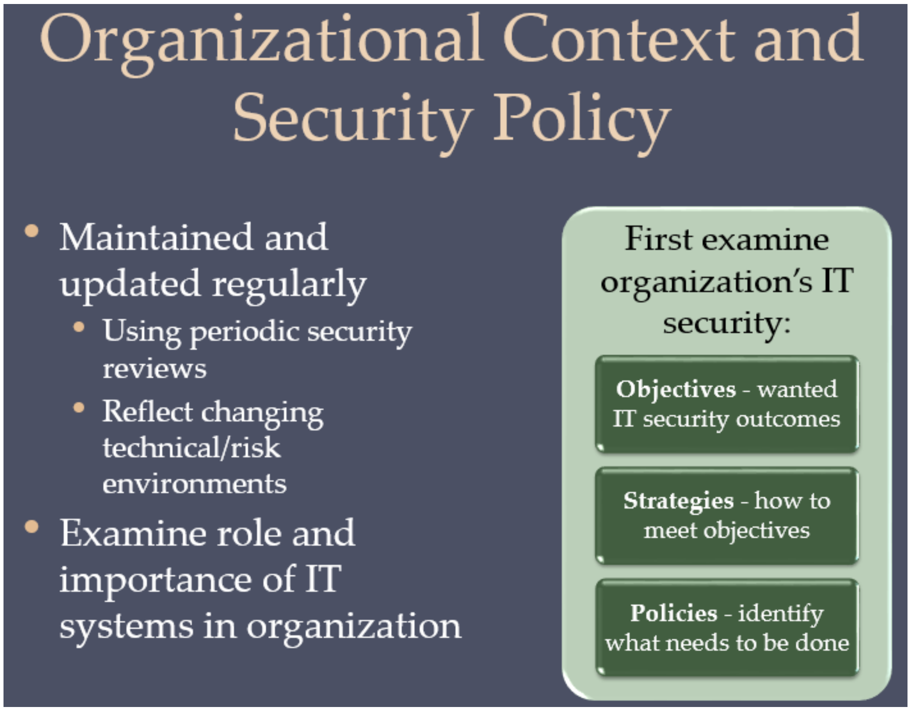


Figure 14.2 The Plan - Do - Check - Act Process Model



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:

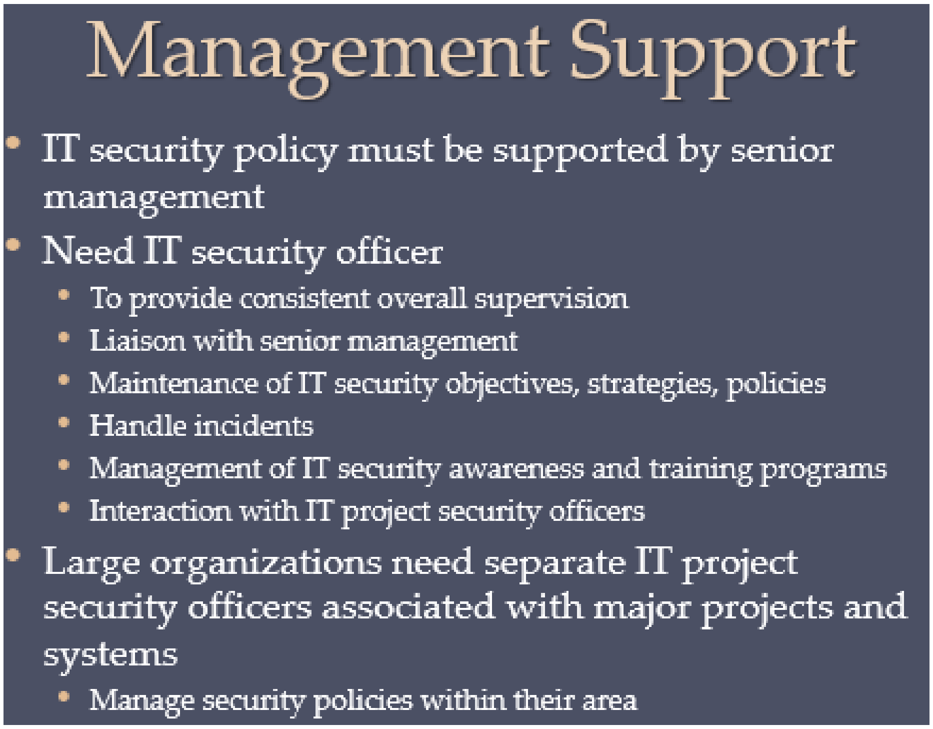
Objectives - wanted IT security outcomes

Strategies - how to meet objectives

Policies - identify what needs to be done

An **organizational security policy** is developed that describes what the objectives and strategies are and the process used to achieve them. This policy typically needs to address at least the following topics:

- The scope and purpose of the policy
- Integration of security into systems development and procurement
- Definition of the information classification scheme used across the organization
- Contingency and business continuity planning
- Incident detection and handling processes
- How and when this policy should be reviewed
- The method for controlling changes to this policy
- The risk management approach adopted by the organization
- How security awareness and training is to be handled



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:

It is a critical component of the process. Ideally every single organizational asset is examined, and every conceivable risk to it is evaluated. In practice this is clearly impossible. The time and effort required, even for large, well-resourced organizations, is clearly neither achievable nor cost effective.

Specifying the acceptable level of risk is simply wise management and means that resources used up are reasonable in the context of the organization's available budget, time, and personnel resources.

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

1. Baseline Approach:

The baseline approach to risk assessment aims to implement a basic general level of security controls on systems using baseline documents, codes of practice, and **industry best practice.** The goal of the baseline approach is to implement generally agreed controls to provide protection against the most common threats.

The **advantages** of this approach are that it doesn't require the expenditure of additional resources in conducting a more formal risk assessment and that the same measures can be replicated over a range of systems

The major **disadvantage** is that no special consideration is given to variations in the organization's risk exposure based on who they are and how their systems are used. Also, there is a chance that the baseline level may be set either too high, leading to expensive or restrictive security measures that may not be warranted, or set too low, resulting in insufficient security and leaving the organization vulnerable.

The use of the baseline approach alone would generally be recommended only for small organizations without the resources to implement more structured approaches.

2. Informal Approach:

The informal approach involves conducting some form of informal, practical risk analysis for the organization's IT systems. This analysis exploits the knowledge and expertise of the individuals performing this analysis. It may involve reviewing of existing policies and procedures, and observation of day-to-day operations.

A major **advantage** of this approach is that the individuals performing the analysis require **no additional skills**. Hence, an informal risk assessment can be performed relatively **quickly and cheaply**. In addition, because the organization's systems are being examined, judgments can be made about **specific vulnerabilities and risks** to systems for the organization that the baseline approach would not address. Thus more accurate and targeted controls may be used than would be the case with the baseline approach

There are a number of **disadvantages**. Because a formal process is not used, there is a chance that **some risks may not be considered appropriately**, potentially leaving the organization vulnerable. Besides, because the approach is informal, the **results may be skewed** by the views of the individuals performing the analysis. Lastly, there may be **inconsistent results over time** as a result of differing expertise in those conducting the analysis. The use of the informal approach would generally be recommended for small to medium-sized organizations where the IT systems are not necessarily essential

3. Detailed Risk (not in slides)

4. Combined (not in slides)