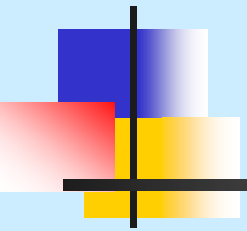
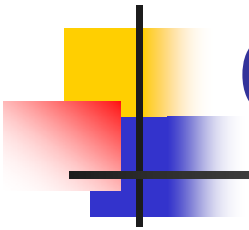


Chapter 8 : Policies and Procedures



Objectives

- Define the security policy cycle
- Explain risk identification
- Design a security policy
- Define types of security policies
- Define compliance monitoring and evaluation

Understand Why Policy Is Important

- Policy provides the rules that govern how systems should be configured and how employees of an organization should act in normal circumstances and react during unusual circumstances.

Understand Why Policy Is Important (cont.)

- Thus the policy performs two primary functions:
  - Policy defines what security should be within an organization
    - Policy defines the proper configurations on computer systems and networks as well as physical security measures.
    - Policy also defines how employees should perform certain security-related duties such as the administration of users.
    - Policy also defines how employees are expected to behave when using computer systems that belong to the organization.
  - Policy puts everyone on the same page so everyone understands what is expected
    - It provides the framework for the employees to work together
    - It defines the goals and objectives of the security program
    - And provides the basis for security teamwork

Information Policy

- The information policy defines what sensitive information is within the organization and how that information should be protected.
- Information can be in the form of paper records or electronic files. The policy should take both into account.

Information Policy (cont.)

- Classifications – two or three levels are usually sufficient for most organization :
  - Public classification – can be provided to the public
  - Company confidential – releasable to employees but not to public
  - Restricted or protected – restricted to a limited number of employees

Information Security Policy

- Marking and storing sensitive information
  - Paper – locked in cabinets
  - Electronic – access control on files
- Transmission of sensitive information
  - Paper – perhaps use certified mail
  - Electronic – encryption of email messages
- Destruction of sensitive information
  - Paper – cross-cut shredding
  - Electronic – wipe information using PGP desktop and BCWipe

Understanding the Security Policy Cycle

- First part of the cycle is risk identification
- Risk identification seeks to determine the risks that an organization faces against its information assets
- That information becomes the basis of developing a security policy
- A security policy is a document or series of documents that clearly defines the defense mechanisms an organization will employ to keep information secure

Understanding the Security Policy Cycle (continued)

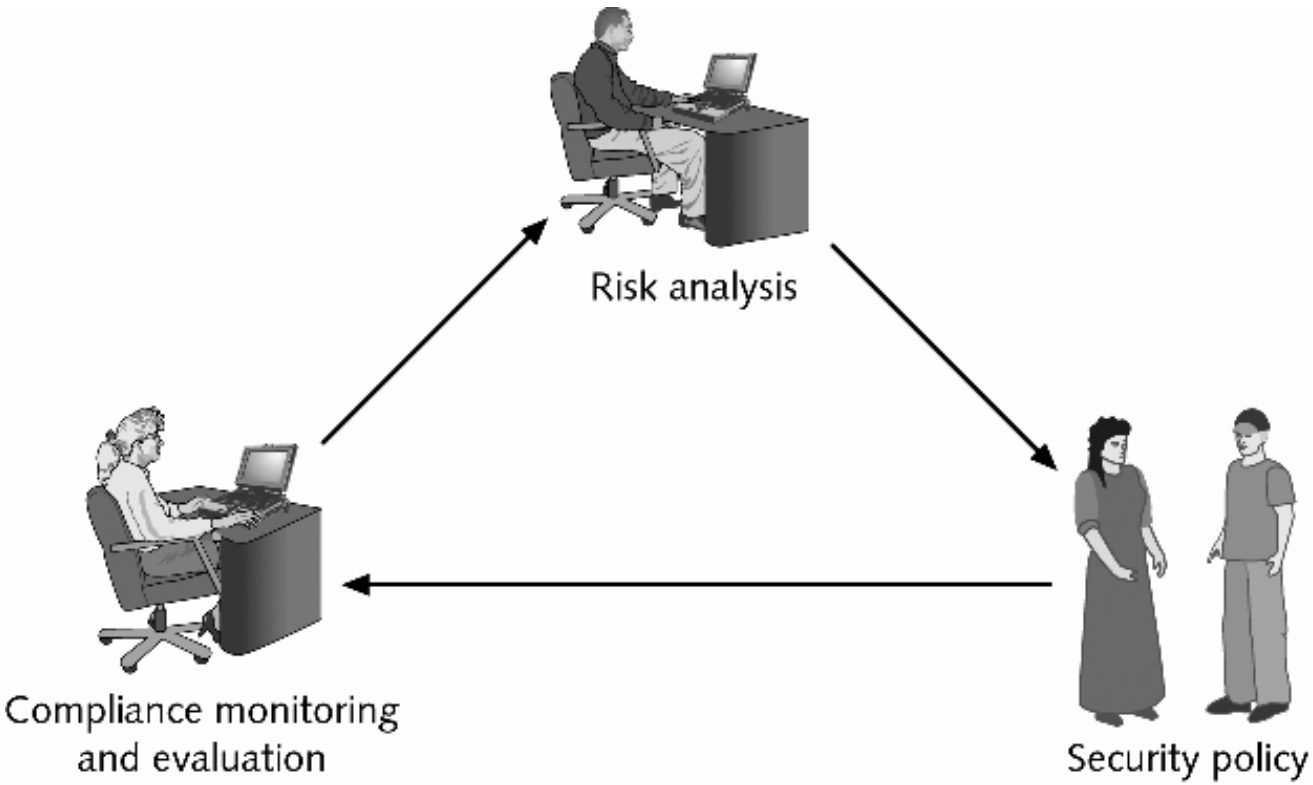


Figure 1 Security policy cycle

Reviewing Risk Identification

- First step in security policy cycle is to identify risks
- Involves the four steps:
  - Inventory the assets
  - Determine what threats exist against the assets and by which threat agents
  - Investigate whether vulnerabilities exist that can be exploited
  - Decide what to do about the risks

Reviewing Risk Identification (continued)

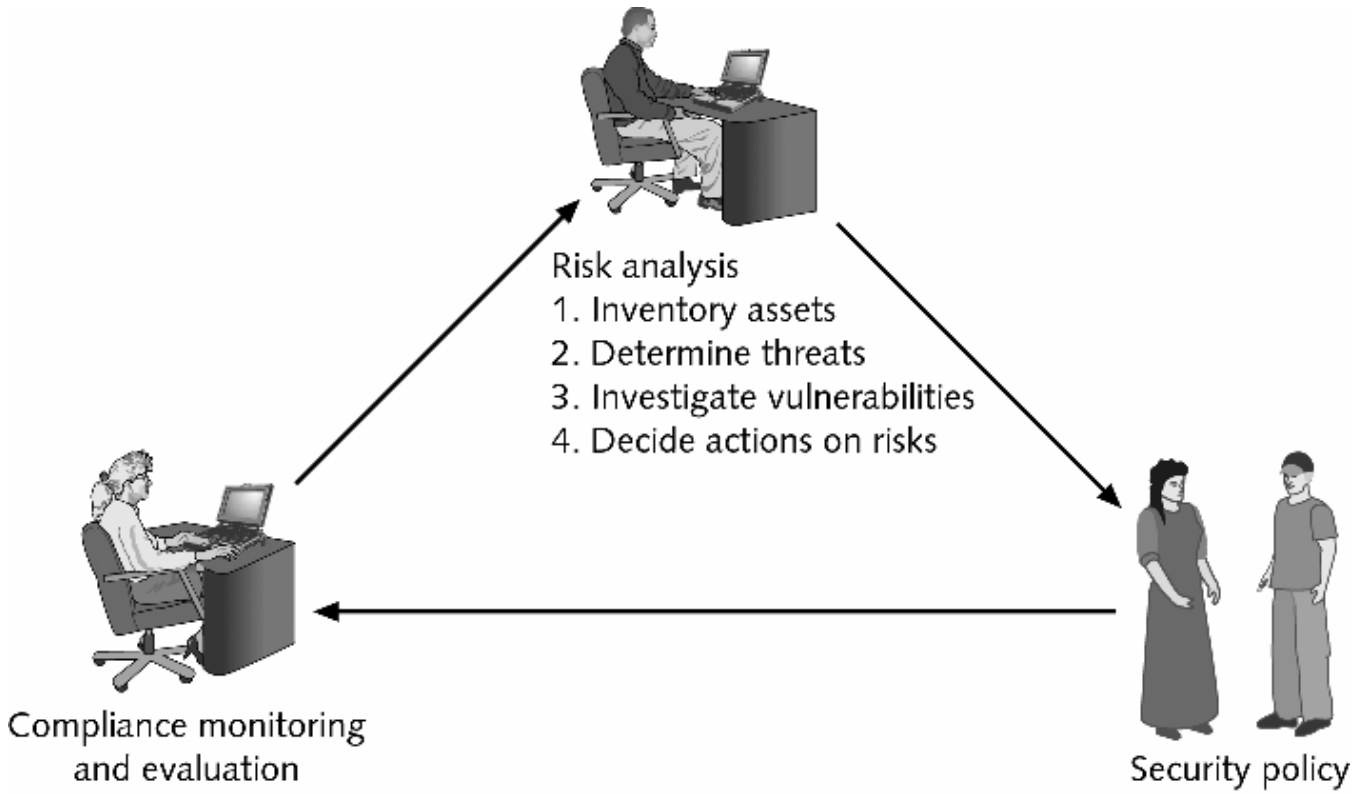


Figure 2 Risk identification elements

Asset Identification

- An asset is any item with a positive economic value
- Many types of assets, classified as follows:
  - Physical assets
  - Data
  - Software
  - Hardware
  - Personnel
- Along with the assets, **attributes of the assets** need to be compiled

Asset Identification (cont.)

- After an inventory of assets has been created and their attributes identified, the next step is to determine each item's relative value
- Factors to be considered in determining the relative value are listed on the following slides :

Asset Identification (cont.)

- An organization has many types of assets which can be classified as follows:
  - Physical assets – buildings , automobiles, etc..
  - Data – employee databases and inventory records
  - Software – application programs, OS and security s/w
  - Hardware – computers and networking equipment
  - Personnel – employees, customers, partners, and vendors

Threat Identification

- A threat is not limited to those from attackers, but also includes acts of God, such as fire or severe weather
- Threat modeling constructs scenarios of the types of threats that assets can face
- The goal of threat modeling is to better understand who the attackers are, why they attack, and what types of attacks may occur

Threats To Information Security

Category of threat	Example
Human error	Employee reformats hard drive
Compromise of intellectual property	S/w piracy
Espionage	Spy steals production schedule
Extortion	Mail clerk blackmailed into intercepting letters
Sabotage or vandalism	Attacker implants worm that erases files
Theft	Laptop is stolen from airport
Software attacks	Virus, worm, DoS
Acts of God	Fire, flood, earthquake
Utility interruption	Electrical power is cut off
Hardware failure or errors	Firewall blocks all packets
Software errors	Bug prevents program from properly loading

Threat Identification (cont.)

- A valuable tool used in threat modeling is the construction of an attack tree
- An attack tree provides a visual image of the attacks that may occur against an asset

Threat Identification (cont.)

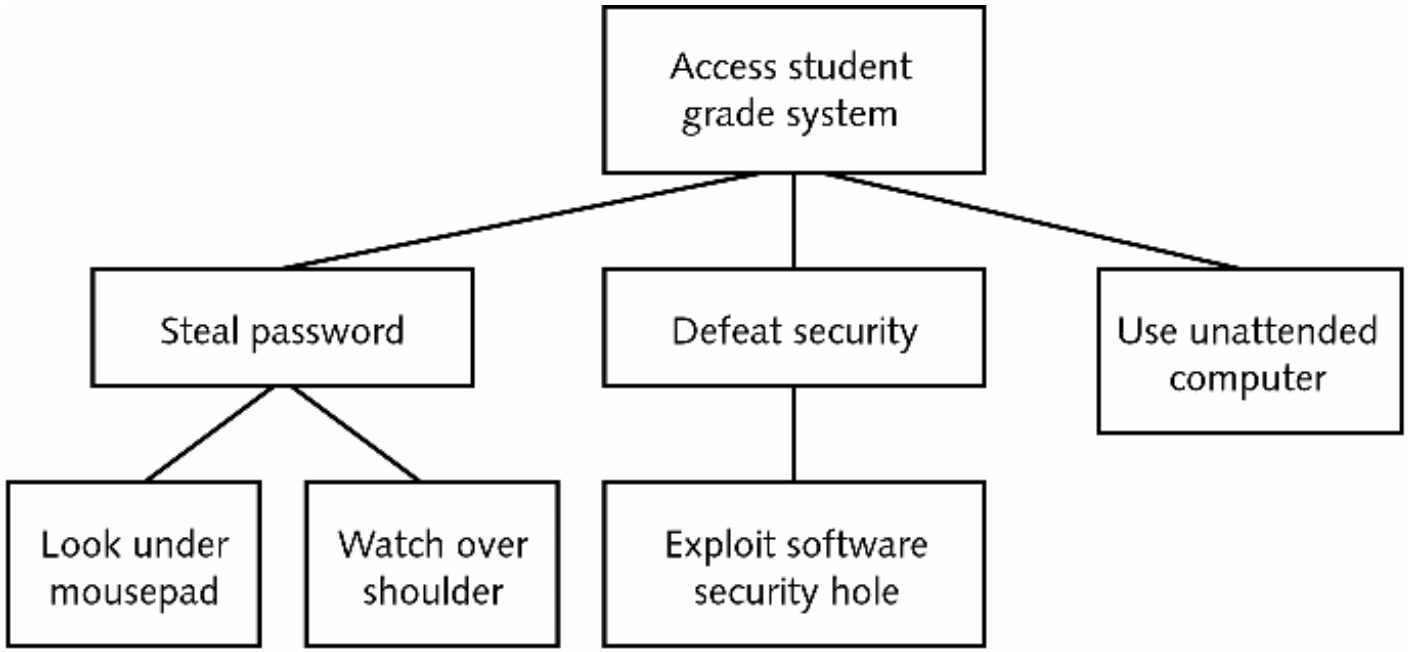


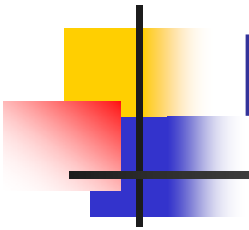
Figure 3 Attack tree for accessing student grade system

Vulnerability Appraisal

- After assets have been inventoried and prioritized and the threats have been explored, the next question becomes, what current security weaknesses may expose the assets to these threats?
- Vulnerability appraisal takes a current snapshot of the security of the organization as it now stands

Vulnerability Appraisal (cont.)

- To assist with determining vulnerabilities of hardware and software assets, use vulnerability scanners
- These tools, available as free Internet downloads and as commercial products, compare the asset against a database of known vulnerabilities and produce a discovery report that exposes the vulnerability and assesses its severity



Risk Assessment

- Final step in identifying risks is to perform a risk assessment
- Risk assessment involves determining the likelihood that the vulnerability is a risk to the organization
- Each vulnerability can be ranked by the scale
- Sometimes calculating anticipated losses can be helpful in determining the impact of a vulnerability

Risk Assessment (cont.)

- Formulas commonly used to calculate expected losses are:
  - Single Loss Expectancy
  - Annualized Loss Expectancy
- An organization has three options when confronted with a risk:
  - Accept the risk
  - Diminish the risk
  - Transfer the risk

Risk Assessment (cont.)

Table 1 Risk identification steps

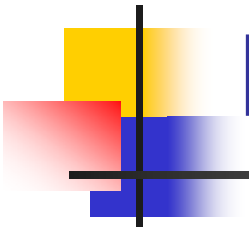
Risk Identification Action	Steps
A. Asset identification	1. Inventory the assets.
	2. Record asset attributes.
	3. Determine the asset's relative value.
B. Threat identification	1. Classify threats by category.
	2. Design attack tree.
C. Vulnerability appraisal	1. Determine current weaknesses in assets.
	2. Use vulnerability scanners on hardware and software.
D. Risk assessment	1. Estimate impact of vulnerability on organization.
	2. Calculate loss expectancy.
	3. Estimate probability the vulnerability will occur.
	4. Decide what to do with the risk.

Designing the Security Policy

- Designing a security policy is the logical next step in the security policy cycle
- After risks are clearly identified, a policy is needed to mitigate what the organization decides are the most important risks

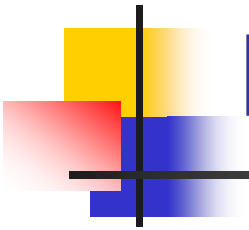
What Is a Security Policy?

- A policy is a document that outlines specific requirements or rules that must be met
  - Has the following characteristics
    - Defines what appropriate behavior for users is
    - What tools and procedures are needed
    - HR action in response to inappropriate behavior
  - Correct vehicle for an organization to use when establishing information security
- A standard is a collection of requirements specific to the system or procedure that must be met by everyone
- A guideline is a collection of suggestions that should be implemented



Balancing Control and Trust

- To create an effective security policy, two elements must be carefully balanced: trust and control
- Three models of trust:
  - Trust everyone all of the time
  - Trust no one at any time
  - Trust some people some of the time



Designing a Policy

- When designing a security policy, you can consider a standard set of principles
- These can be divided into what a policy must do and what a policy should do

Designing a Policy (cont.)

Table 2 Policy must and should statements

Security Policy Must	Security Policy Should
Be able to implement and enforce it.	State reasons why the policy is necessary.
Be concise and easy to understand.	Describe what is covered by the policy.
Balance protection with productivity.	Outline how violations will be handled.

Designing a Policy (cont.)

- Security policy design should be the work of a team and not one or two technicians
- The team should have these representatives:
  - Senior level administrator
  - Member of management who can enforce the policy
  - Member of the legal staff
  - Representative from the user community

Elements of a Security Policy

- Because security policies are formal documents that outline acceptable and unacceptable employee behavior, legal elements are often included in these documents
- The three most common elements:
  - Due care
  - Separation of duties
  - Need to know

Elements of a Security Policy (cont.)

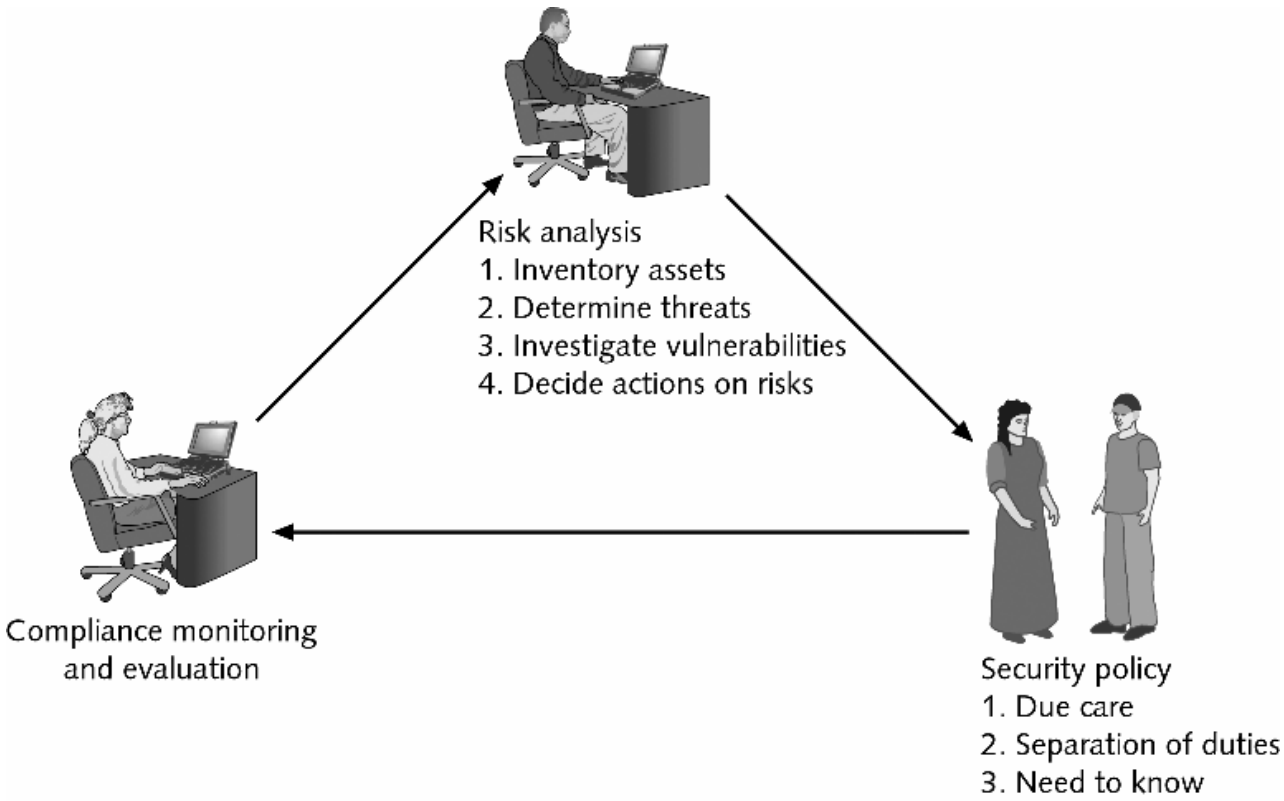
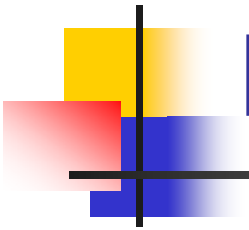


Figure 4 Security policy elements



Due Care

- Term used frequently in legal and business settings
- Defined as obligations that are imposed on owners and operators of assets to exercise reasonable care of the assets and take necessary precautions to protect them

Separation of Duties

- Key element in internal controls
- Means that one person's work serves as a complementary check on another person's
- No one person should have complete control over any action from initialization to completion

Need to Know

- One of the best methods to keep information confidential is to restrict who has access to that information
- Only that employee whose job function depends on knowing the information is provided access

Types of Security Policies

- Umbrella term for all of the subpolicies included within it
- In this section, you examine some common security policies:
  - Acceptable use policy
  - Human resource policy
  - Password management policy
  - Privacy policy
  - Disposal and destruction policy
  - Service-level agreement

Types of Security Policies (continued)

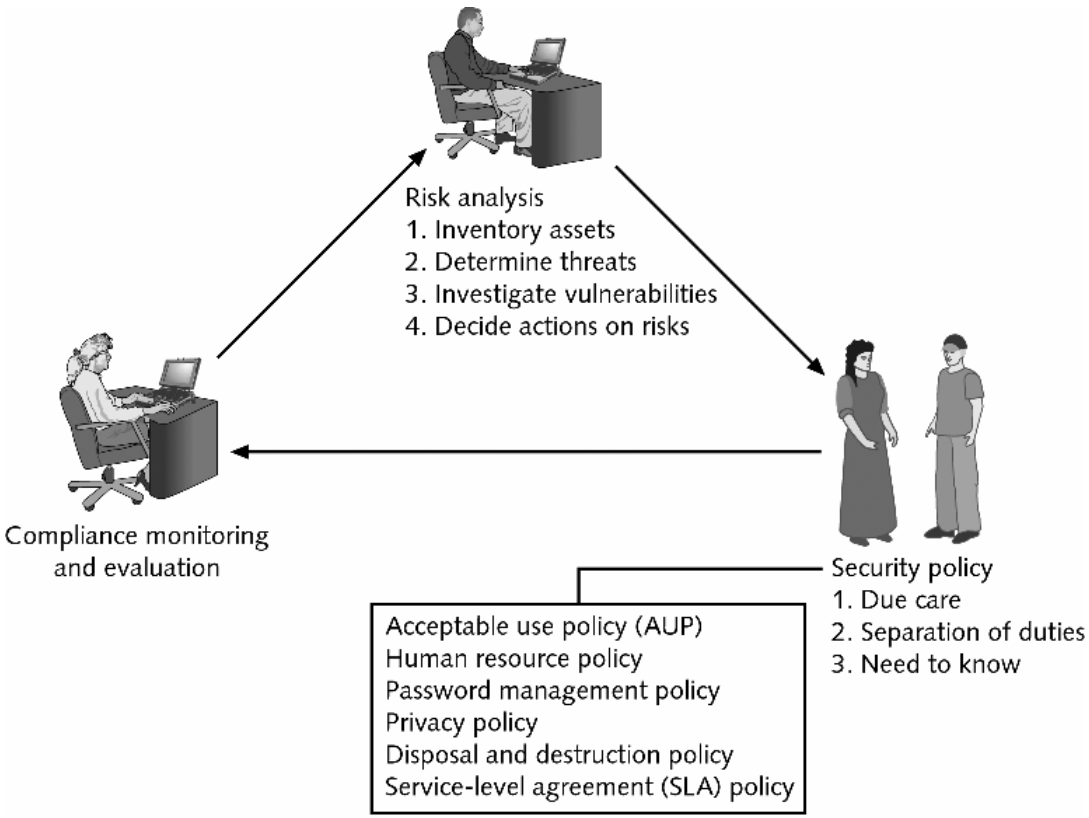


Figure 5 Types of security policies

Types of Security Policies (continued)

Table 3 Examples of security policies

Name of Security Policy	Description
Acceptable encryption policy	Defines requirements for using cryptography
Analog line policy	Defines standards for use of analog dial-up lines for sending and receiving faxes and for connection to computers
Antivirus policy	Establishes guidelines for effectively reducing the threat of computer viruses on the organization's network and computers
Audit vulnerability scanning policy	Outlines the requirements and provides the authority for an information security team to conduct audits and risk assessments and investigate incidents to ensure conformance to security policies or to monitor user activity
Automatically forwarded e-mail policy	Prescribes that no e-mail will be automatically forwarded to an external destination without prior approval from the appropriate manager or director
Database credentials coding policy	Defines requirements for storing and retrieving database usernames and passwords
Dial-in access policy	Outlines appropriate dial-in access and its use by authorized personnel

Types of Security Policies (continued)

Table 4 Examples of security policies (continued)

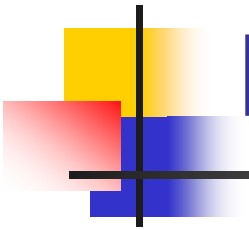
Name of Security Policy	Description
Demilitarized zone (DMZ) security policy	Defines standards for all networks and equipment located in the DMZ
E-mail policy	Creates standards for using corporate e-mail
E-mail retention policy	Helps employees determine what information sent or received by e-mail should be retained and for how long
Extranet policy	Defines the requirements for third-party organizations to access the organization's networks
Information sensitivity policy	Establishes criteria for classifying and securing the organization's information in a manner appropriate to its level of security
Router security policy	Outlines standards for minimal security configuration for routers and switches
Server security policy	Creates standards for minimal security configuration for servers
Virtual private network (VPN) security policy	Establishes requirements for Remote Access IP security (IPSec) or Layer 2 Tunneling Protocol (L2TP) VPN connections to the organization's network
Wireless communication policy	Defines standards for wireless systems used to connect to the organization's networks

Acceptable Use Policy (AUP)

- Defines what actions users of a system may perform while using computing and networking equipment
- Should have an overview regarding what is covered by this policy
- Unacceptable use should also be outlined

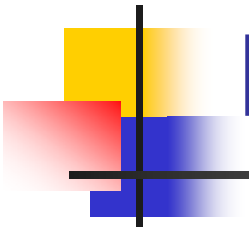
Human Resource Policy

- Policies of the organization that address human resources
- Should include statements regarding how an employee's information technology resources will be addressed



Password Management Policy

- Although passwords often form the weakest link in information security, they are still the most widely used
- A password management policy should clearly address how passwords are managed
- In addition to controls that can be implemented through technology, users should be reminded of how to select and use passwords



Privacy Policy

- Privacy is of growing concern among today's consumers
- Organizations should have a privacy policy that outlines how the organization uses information it collects

Disposal and Destruction Policy

- A disposal and destruction policy that addresses the disposing of resources is considered essential
- The policy should cover how long records and data will be retained
- It should also cover how to dispose of them

Service-Level Agreement (SLA) Policy

- Contract between a vendor and an organization for services
- Typically contains the items listed on the following slides :

SLA Policy Contents

- Scope of worked to be performed
- Performance, reporting and tracking
- Resolving problems
- Compensation
- Customer duties and responsibilities
- Vendor duties and responsibilities
- Exclusions and exceptions

Understanding Compliance Monitoring and Evaluation

- The final process in the security policy cycle is compliance monitoring and evaluation
- Some of the most valuable analysis occurs when an attack penetrates the security defenses
- A team must respond to the initial attack and reexamine security policies that address the vulnerability to determine what changes need to be made to prevent its reoccurrence

Incidence Response Policy

- Outlines actions to be performed when a security breach occurs
- Most policies outline composition of an incidence response team (IRT)
- Should be composed of individuals from:
  - Senior management
  - IT personnel
  - Corporate counsel
  - Human resources
  - Public relations

Incidence Response Policy (cont.)

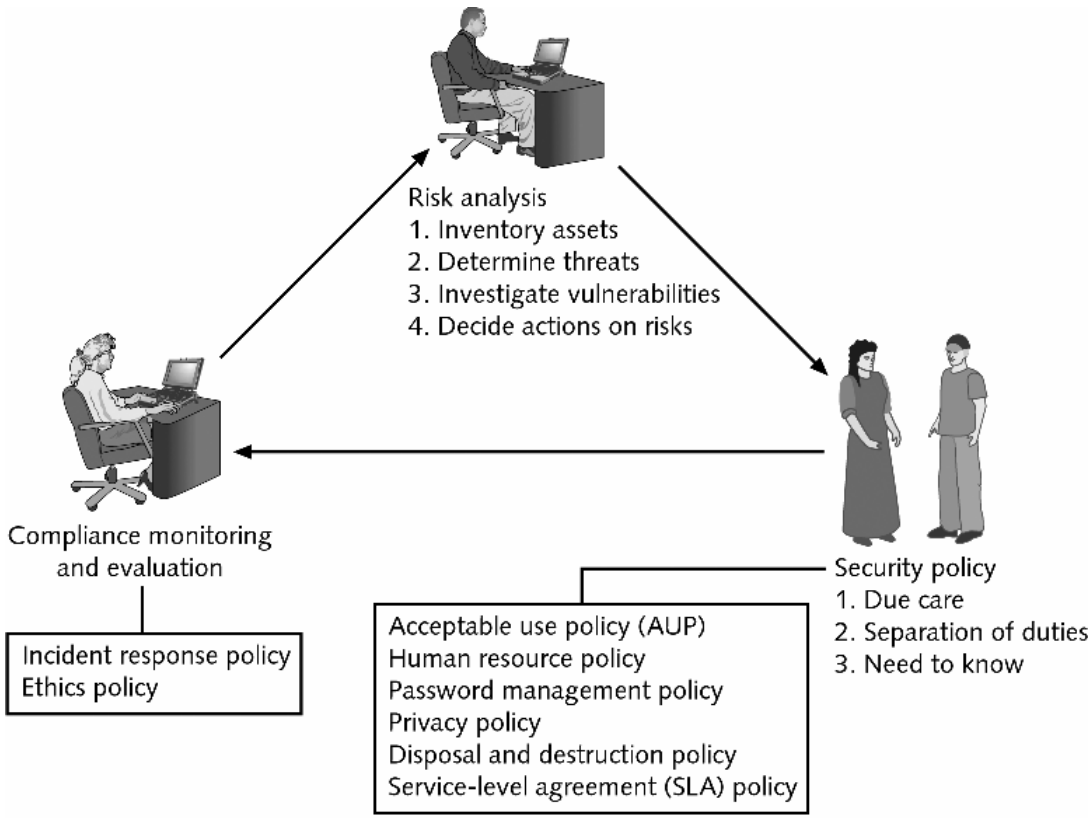


Figure 5 Compliance monitoring and evaluation

Ethics Policy

- Codes of ethics by external agencies have encouraged its membership to adhere to strict ethical behavior within their profession
- Codes of ethics for IT professionals are available from the Institute for Electrical and Electronic Engineers (IEEE) and the Association for Computing Machinery (ACM), among others
- Main purpose of an ethics policy is to state the values, principles, and ideals each member of an organization must agree to