Risk Management

Modifications by Prof. Dong Xuan and
Adam C. Champion

Learning Objectives

Upon completion of this material, you should be able to:

- Define risk management, risk identification, and risk control
- Understand how risk is identified, assessed and controlled

Terminology Review (1)

- **System:** Collection of hardware, software, data, procedures, networks, people, etc. that "belong together"
- **Vulnerability**, **exploit, threat**, **threat agent**
- **Victim impact (or cost):** What happens to victim as the result of a successful attack
  - Damaged reputation
  - Lost sales
  - Replacement cost
  - Recovery cost (e.g., reinstall OS and applications)
  - Not limited to $$

Terminology Review (2)

- **Attacker benefit:** What attacker gains from successful attack, e.g., $$, status in 1337 h4x0r underground, spreading political message by website defacement, etc.
- **Attacker cost:** What attacker "spends" to launch attack
  - Not limited to successful attacks
  - Not limited to $$ – could include special equipment, software, time, expertise, probability of getting caught and penalized
- **Risk:** Product of likelihood and magnitude of loss (when "bad things" happen)

Introduction

- **Risk management:** process of identifying and controlling risks facing an organization
  - **Risk identification:** process of examining an organization's current information technology security situation
  - **Risk control:** applying controls to reduce risks to an organization's data and information systems

An Overview of Risk Management

- "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." – Sun Tzu, *The Art of War*
- Know yourself: identify, examine, and understand the information and systems currently in place
- Know the enemy: identify, examine, and understand threats facing the organization

Risk Identification

- **Assets** are targets of various threats and threat agents
- Risk management involves identifying organization's assets and identifying threats/ vulnerabilities
- Risk identification begins with identifying organization's assets and assessing their value

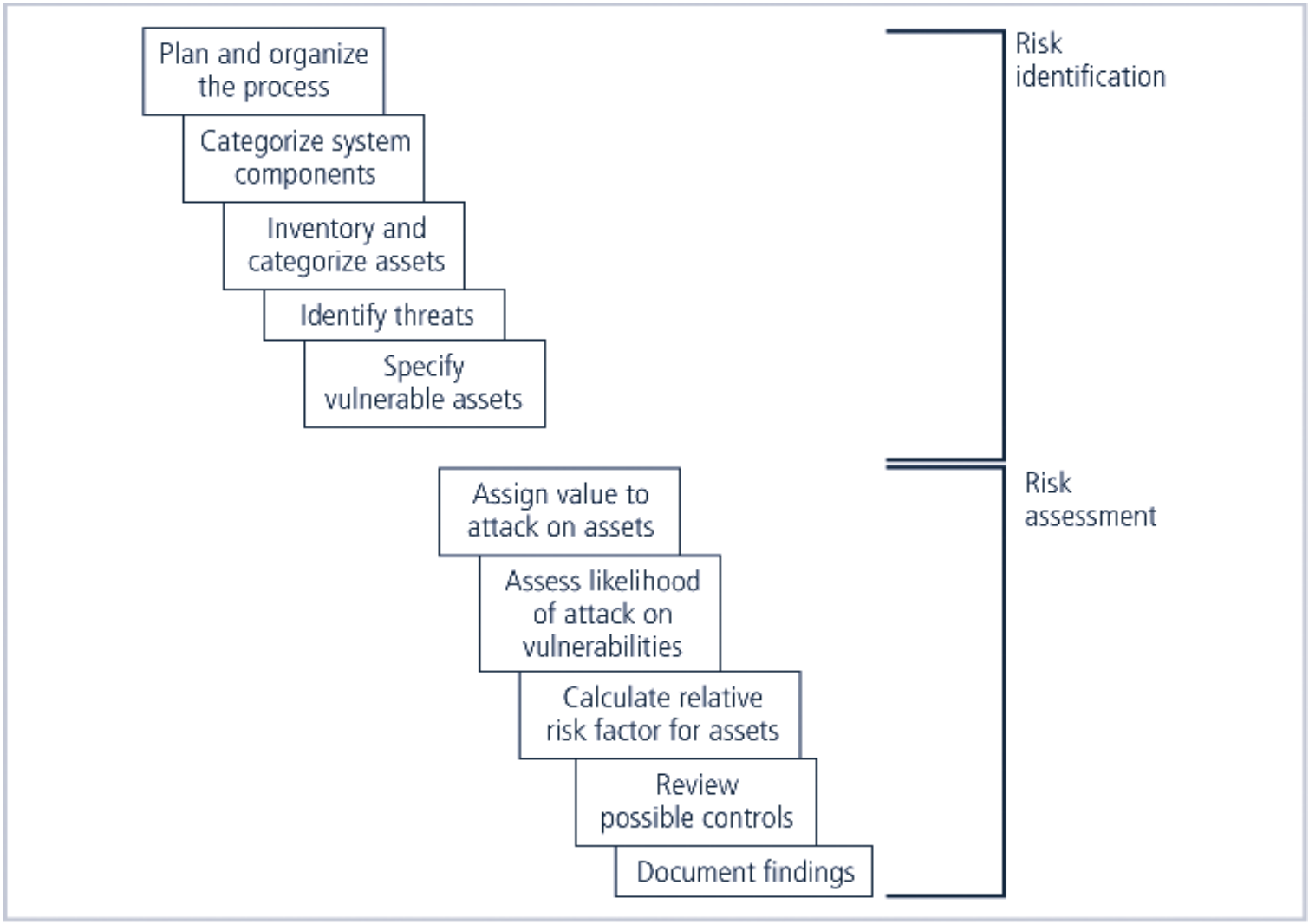

FIGURE 4-2 **Components of Risk Identification**

Asset Identification and Valuation

- Iterative process; begins with identification of assets, including all elements of an organization's system (people, procedures, data and information, software, hardware, networking)
- Assets are then classified and categorized

TABLE 4-1 Categorizing the Components of an Information System

Traditional system components	SecSDLC and risk management system components	
People	Employees	Trusted employees Other staff
	Nonemployees	People at trusted organizations Strangers
Procedures	Procedures	IT and business standard procedures IT and business sensitive procedures
Data	Information	Transmission Processing Storage
Software	Software	Applications Operating systems Security components
Hardware	System devices and peripherals	Systems and peripherals Security devices
	Networking components	Intranet components Internet or DMZ components

People, Procedures, and Data Asset Identification (1)

- Human resources, documentation, and data information assets are more difficult to identify
- People with knowledge, experience, and good judgment should be assigned this task
- These assets should be recorded using reliable data-handling process

People, Procedures, and Data Asset Identification (2)

- Asset attributes for people: position name/number/ID; supervisor; security clearance level; special skills
- Asset attributes for procedures: description; intended purpose; what elements is it tied to; storage location for reference; storage location for update
- Asset attributes for data: classification; owner/creator/ manager; data structure size; data structure used; online/ offline; location; backup procedures employed

Hardware, Software, and Network Asset Identification

- What information attributes to track depends on:
  - Needs of organization/risk management efforts
  - Management needs of information security/ information technology communities
- Asset attributes to be considered are: name; IP address; MAC address; element type; serial number; manufacturer name; model/part number; software version; physical or logical location; controlling entity

Information Asset Classification

- Many organizations have data classification schemes (e.g., confidential, internal, public data)
- Classification of components must be specific to allow determination of priority levels
- Categories must be comprehensive and mutually exclusive

Information Asset Valuation

- Questions help develop criteria for asset valuation: which information asset
  - is most critical to organization's success?
  - generates the most revenue/profitability?
  - would be most expensive to replace or protect?
  - would be the most embarrassing or cause greatest liability if revealed?

Data Classification and Management

- Variety of classification schemes used by corporate and military organizations
- Information owners responsible for classifying their information assets
- Information classifications must be reviewed periodically
- Most organizations do not need detailed level of classification used by military or federal agencies; however, organizations may need to classify data to provide protection

Threat Identification

- Realistic threats need investigation; unimportant threats are set aside
- Threat assessment:
  - Which threats present danger to assets?
  - Which threats represent the most danger to information?
  - How much would it cost to recover from attack?
  - Which threat requires greatest expenditure to prevent?

TABLE 4-3 Threats to Information Security

Threat	Example
Act of human error or failure	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of espionage or trespass	Unauthorized access and data collection
Deliberate acts of information extortion	Blackmail for information disclosure
Deliberate acts of sabotage or vandalism	Destruction of systems or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros, denial of service
Forces of nature	Fire, flood, earthquake, lightning
Quality of service deviations from service providers	Power and WAN quality of service issues
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

Vulnerability Identification

- Specific avenues threat agents can exploit to attack an information asset are called vulnerabilities
- Examine how each threat could be perpetrated and list organization's assets and vulnerabilities
- Process works best when people with diverse backgrounds within organization work iteratively in a series of brainstorming sessions
- At end of risk identification process, list of assets and their vulnerabilities is achieved

Risk Assessment

- Risk assessment evaluates the relative risk for each vulnerability
- Assigns a risk rating or score to each information asset

Documenting the Results of Risk Assessment

- Final summary comprised in ranked vulnerability risk worksheet
- Worksheet details asset, asset impact, vulnerability, vulnerability likelihood, and risk-rating factor
- Ranked vulnerability risk worksheet is initial working document for next step in risk management process: assessing and controlling risk

Risk Control

- Once ranked vulnerability risk worksheet complete, must choose one of four strategies to control each risk:
  - Apply safeguards (**avoidance**)
  - Transfer the risk (**transference**)
  - Reduce impact (**mitigation**)
  - Understand consequences and accept risk (**acceptance**)
- **Residual risk:** risk "left over" after identification and control

Avoidance

- Attempts to prevent exploitation of the vulnerability
- Preferred approach; accomplished through countering threats, removing asset vulnerabilities, limiting asset access, and adding protective safeguards
- Three common methods of risk avoidance:
  - Application of policy
  - Training and education
  - Applying technology

Transference

- Control approach that attempts to shift risk to other assets, processes, or organizations
- If lacking, organization should hire individuals/firms that provide security management and administration expertise
- Organization may then transfer risk associated with management of complex systems to another organization experienced in dealing with those risks

Mitigation (1)

- Attempts to reduce impact of vulnerability exploitation through planning and preparation
- Approach includes three types of plans:
  - Incident response plan (IRP)
  - Disaster recovery plan (DRP)
  - Business continuity plan (BCP)

Mitigation (2)

- DRP is most common mitigation procedure
- The actions to take while incident is in progress is defined in IRP
- BCP encompasses continuation of business activities if catastrophic event occurs

Acceptance

- Doing nothing to protect a vulnerability and accepting the outcome of its exploitation
- Valid only when the particular function, service, information, or asset does not justify cost of protection
- Risk appetite describes the degree to which organization is willing to accept risk as trade-off to the expense of applying controls

Selecting a Risk Control Strategy

- Level of threat and value of asset play major role in selection of strategy
- Rules of thumb on strategy selection can be applied:
  - When a vulnerability exists
  - When a vulnerability can be exploited
  - When attacker's cost is less than potential gain
  - When potential loss is substantial

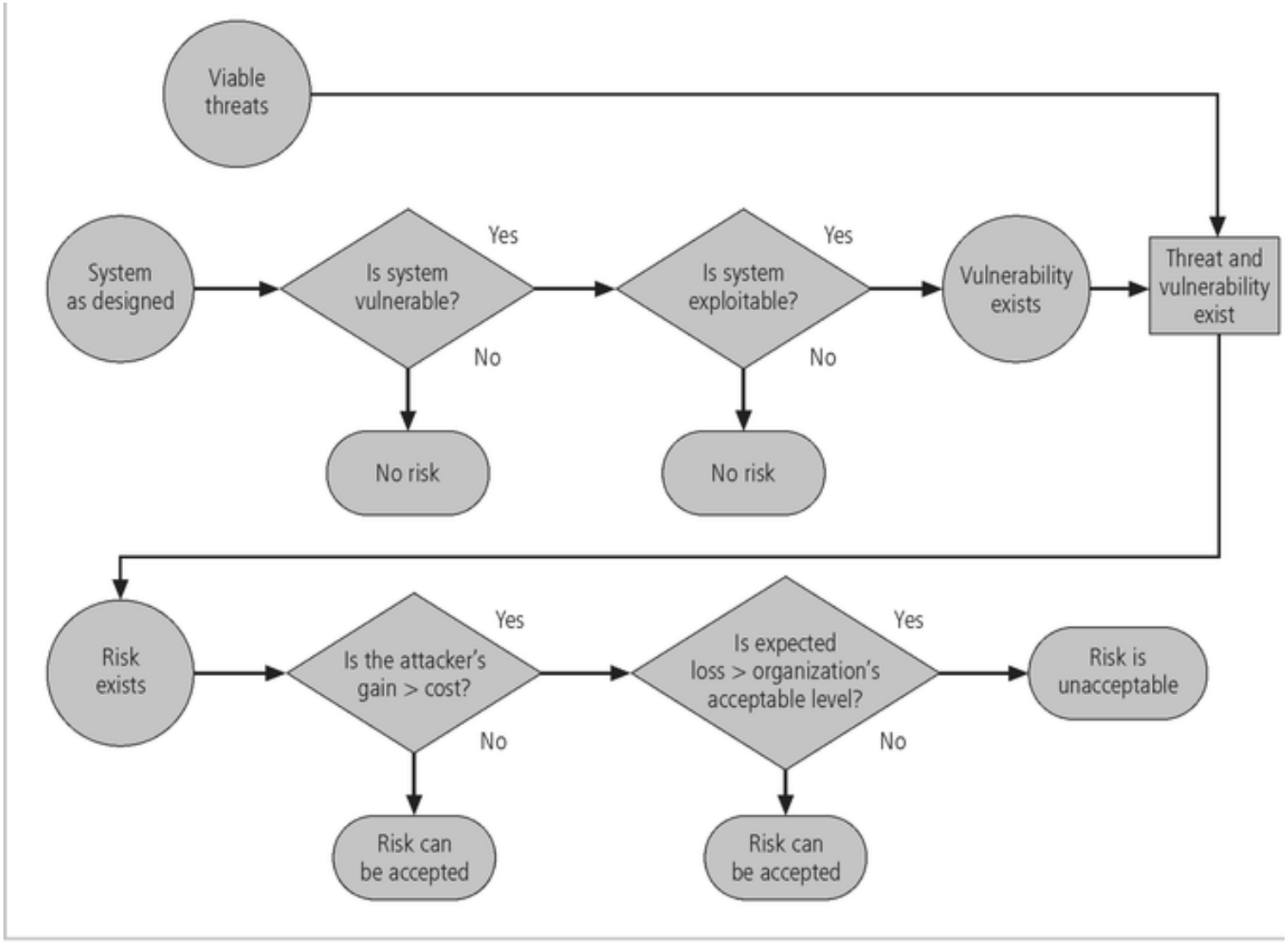

FIGURE 5-2 Risk Handling Decision Points[7]

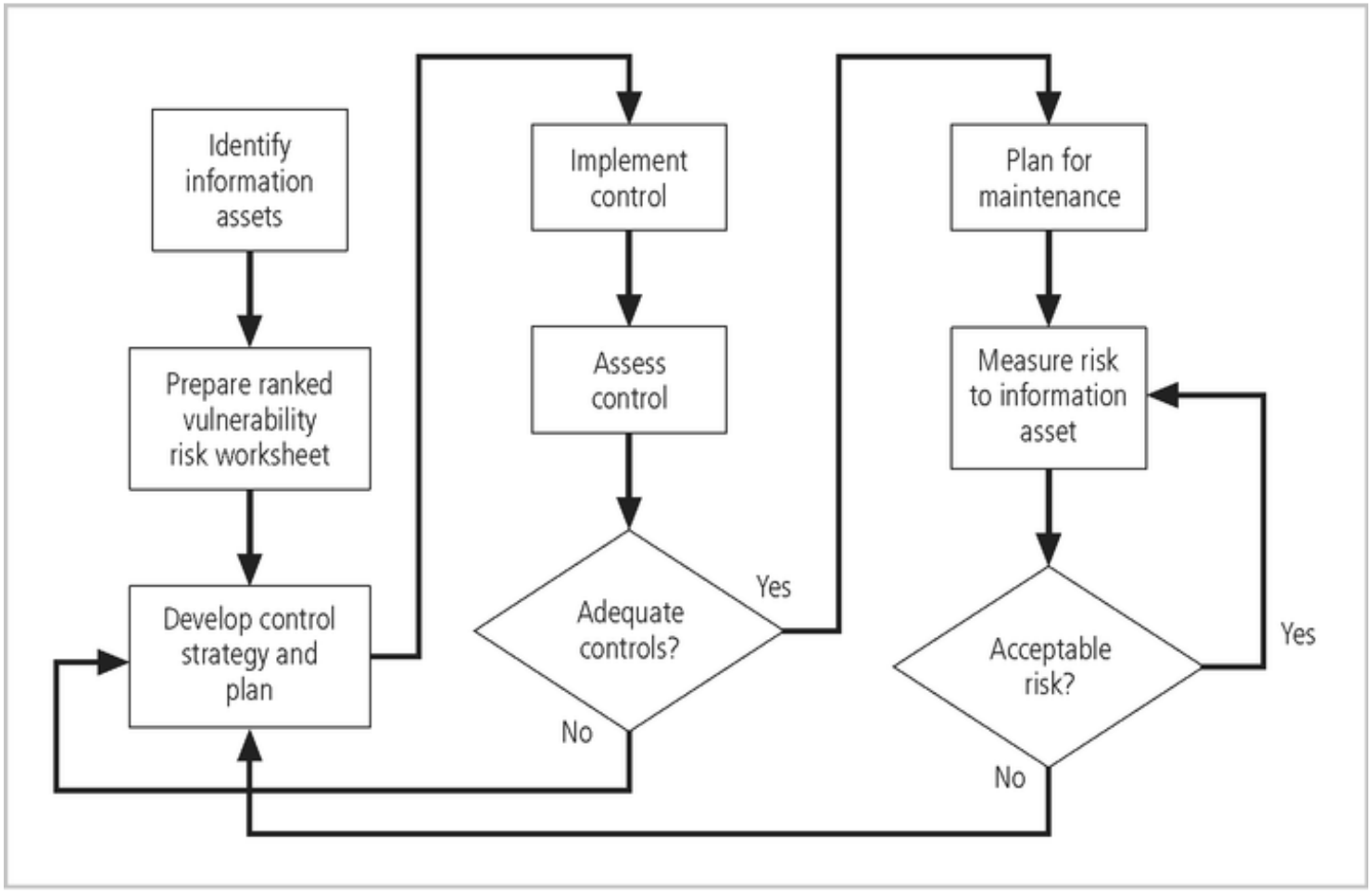

FIGURE 5-3 Risk Control Cycle[8]

Cost Benefit Analysis (CBA) (1)

- Most common approach for information security controls is economic feasibility of implementation
- CBA is begun by evaluating worth of assets to be protected and the loss in value if those assets are compromised
- The formal process to document this is called cost benefit analysis or economic feasibility study

Cost Benefit Analysis (CBA) (2)

- Items that impact cost of a control or safeguard include: cost of development; training fees; implementation cost; service costs; cost of maintenance
- Benefit is the value an organization realizes by using controls to prevent losses associated with a vulnerability
- Asset valuation is process of assigning financial value or worth to each information asset; there are many components to asset valuation

Cost Benefit Analysis (CBA) (3)

- SLE: Single Loss Expectancy ($$)
- ARO: Annualized Rate of Occurrence (# times/yr.)
- ALE: Annualized Loss Expectancy = SLE × ARO ($$/yr)
- ACS: Annualized Cost of Safeguard ($$/year)
- CBA = $ALE_{prior} - ALE_{post} - ACS$ ($$/year)
  - If CBA is positive, that's good
  - If CBA is negative, spend more for protection than expected loss
  - Higher CBA is more efficient
- Problems:
  - "Garbage in garbage out" statistics
  - We don't know how often some events occur (or the unknown)
  - *Silo effect:* we focus on specific systems and miss common controls across systems

Benchmarking (1)

- An alternative approach to risk management
- Benchmarking is process of seeking out and studying practices in other organizations that one's own organization desires to duplicate
- One of two measures typically used to compare practices:
  - Metrics-based measures
  - Process-based measures

Benchmarking (2)

- Standard of due care: when adopting levels of security for a legal defense, organization shows it has done what any prudent organization would do in similar circumstances
- Due diligence: demonstration that organization is diligent in ensuring that implemented standards continue to provide required level of protection
- Failure to support standard of due care or due diligence can leave organization open to legal liability

Benchmarking (3)

- Best business practices: security efforts that provide a superior level protection of information
- When considering best practices for adoption in an organization, consider:
  - Does organization resemble identified target with best practice?
  - Are resources at hand similar?
  - Is organization in a similar threat environment?

Problems with Applying Benchmarking and Best Practices

- Organizations don't talk to each other (biggest problem)
- No two organizations are identical
- Best practices are a moving target
- Knowing what was going on in information security industry in recent years through benchmarking doesn't necessarily prepare for what's next

Summary

- Risk identification: formal process of examining and documenting risk present in information systems
- Risk control: process of taking carefully reasoned steps to ensure the confidentiality, integrity, and availability of components in organization's information system
- Risk identification
  - A risk management strategy enables identification, classification, and prioritization of organization's information assets
  - Residual risk: risk that remains to the information asset even after the existing control is applied

Summary

- Risk control: four strategies are used to control risks that result from vulnerabilities:
  - Apply safeguards (avoidance)
  - Transfer the risk (transference)
  - Reduce impact (mitigation)
  - Understand consequences and accept risk (acceptance)