Principles of Information Security

Chapter 4

Risk Management

Once we know our weaknesses, they cease to do us any harm.

G.C. (GEORG CHRISTOPH) LICHTENBERG (1742–1799)
GERMAN PHYSICIST, PHILOSOPHER

Learning Objectives

- Upon completion of this material, you should be able to:
  - Define risk management, risk identification, and risk control
  - Describe how risk is identified and assessed/evaluated
  - Assess risk based on probability of occurrence and likely impact
  - Explain the fundamental aspects of documenting risk via the process of risk assessment

Learning Objectives (cont'd.)

- Describe the various risk mitigation strategy options
- Identify the categories that can be used to classify controls
- Recognize the conceptual frameworks for evaluating risk controls and formulate a cost benefit analysis
- Describe how to maintain risk controls

Introduction

- Organizations must design and create safe environments in which business processes and procedures can function
- 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

- Know yourself: identify, examine, and understand the information and systems currently in place
- Know the enemy: identify, examine, and understand threats facing the organization
- Responsibility of each community of interest within an organization to manage risks that are encountered

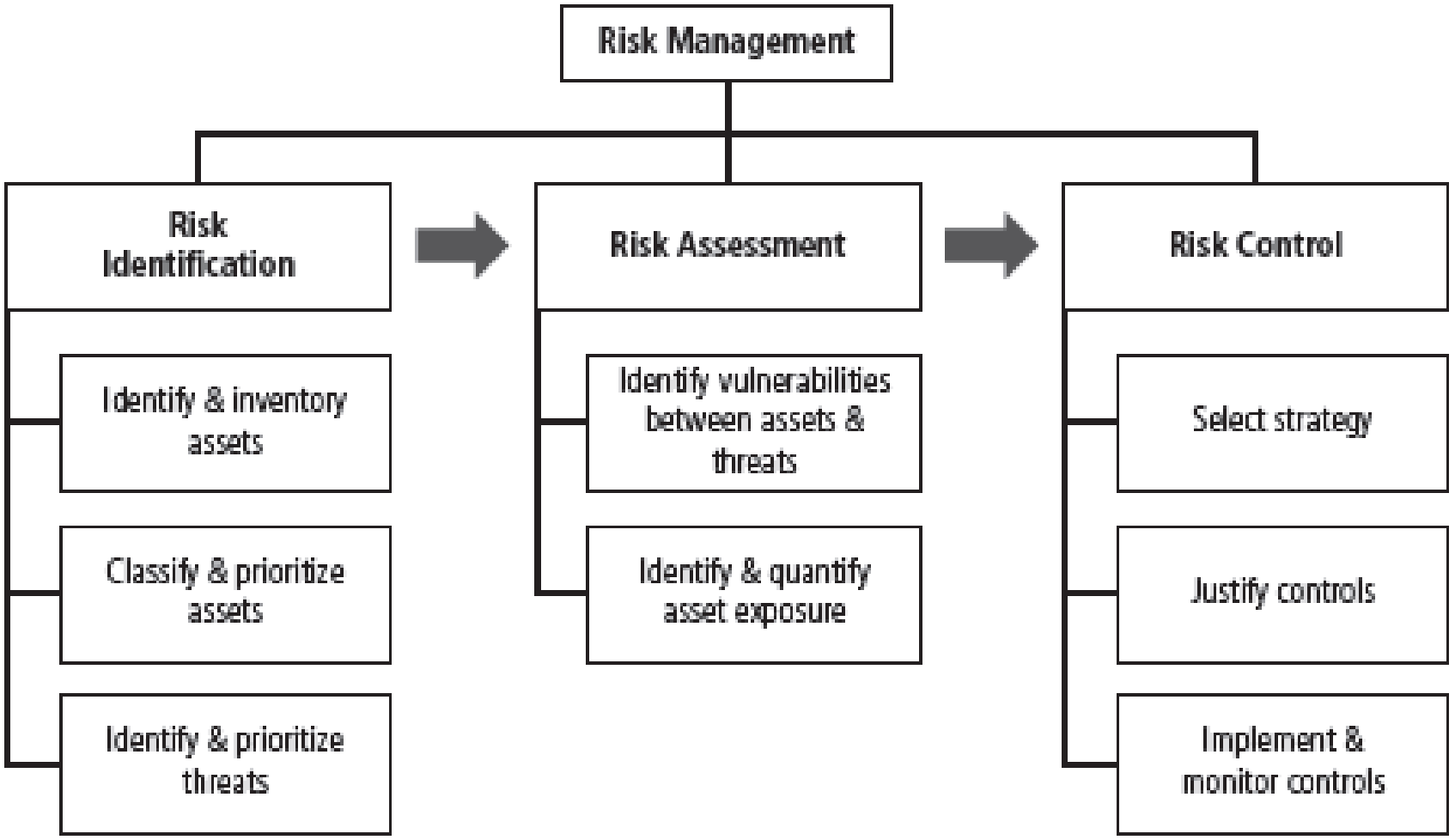

Figure 4-1 Components of Risk Management

The Roles of the Communities of Interest

- Information security, management and users, and information technology all must work together
- Communities of interest are responsible for:
  - Evaluating the risk controls
  - Determining which control options are cost effective for the organization
  - Acquiring or installing the needed controls
  - Ensuring that the controls remain effective

Risk Identification

- Risk management involves identifying, classifying, and prioritizing an organization's assets
- A threat assessment process identifies and quantifies/measures the risks facing each asset
- Components of risk identification
  - People
  - Procedures
  - Data
  - Software
  - Hardware

Plan and Organize the Process

- First step in the Risk Identification process is to follow your project management principles
- Begin by organizing a team with representation across all affected groups
- The process must then be planned out
  - Periodic deliverables/releases
  - Reviews
  - Presentations to management
- Tasks laid out, assignments made and timetables/schedules discussed

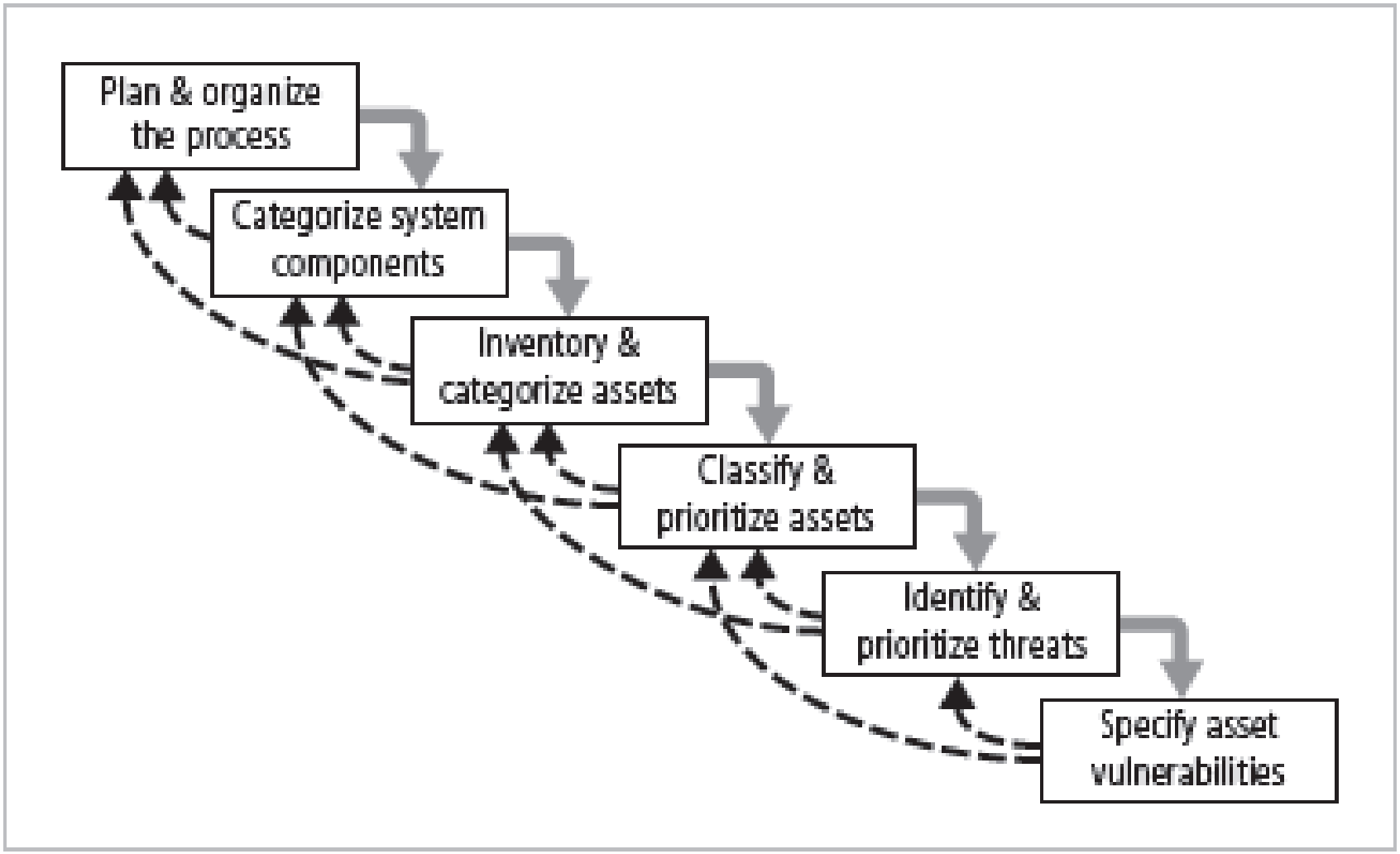

Figure 4-2 Components of Risk Identification

Asset Identification and Inventory

- 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

Traditional System Components	SesSDLC Components	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

Table 4-1 Categorizing the Components of an Information System

People, Procedures, and Data Asset Identification

- Human resources, documentation, and data information assets are more difficult to identify
- Important asset attributes:
  - People: position name/number/ID; supervisor; security clearance level; special skills
  - Procedures: description; intended purpose; what elements it is tied to; storage location for reference; storage location for update
  - 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
  - Preferences/needs of the security and 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
- Automated tools can identify system elements for hardware, software, and network components

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

Classifying and Prioritizing Information Assets

- 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/standard 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?

System Name: SLS E-Commerce
Date Evaluated: February 2006
Evaluated By: D. Jones

Information assets	Data classification	Impact to profitability
Information Transmitted:		
EDI Document Set 1—Logistics BOL to outsourcer (outbound)	Confidential	High
EDI Document Set 2—Supplier orders (outbound)	Confidential	High
EDI Document Set 2—Supplier fulfillment advice (inbound)	Confidential	Medium
Customer order via SSL (inbound)	Confidential	Critical
Customer service Request via e-mail (inbound)	Private	Medium
DMZ Assets:		
Edge Router	Public	Critical
Web server #1—home page and core site	Public	Critical
Web server #2—Application server	Private	Critical

Notes: BOL: Bill of Lading:
DMZ: Demilitarized Zone
EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

Figure 4-5 Sample Inventory Worksheet

Information Asset Valuation (cont'd.)

- Information asset prioritization
  - Create weighting for each category based on the answers to questions
  - Calculate relative importance of each asset using weighted factor analysis
  - List the assets in order of importance using a weighted factor analysis worksheet

Information Asset	Criteria 1: Impact to Revenue	Criteria 2: Impact to Profitability	Criteria 3: Impact to Public Image	Weighted Score
Criterion Weight (1-100) Must total 100	30	40	30	
EDI Document Set 1—Logistics BOL to outsourcer (outbound)	0.8	0.9	0.5	75
EDI Document Set 2—Supplier orders (outbound)	0.8	0.9	0.6	78
EDI Document Set 2—Supplier fulfillment advice (inbound)	0.4	0.5	0.3	41
Customer order via SSL (inbound)	1.0	1.0	1.0	100
Customer service request via e-mail (inbound)	0.4	0.4	0.9	55

Table 4-2 Example of a Weighted Factor Analysis Worksheet
Notes: EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

Identifying and Prioritizing Threats

- 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 (spend money) to prevent?

Threat	Example
Compromises to intellectual property	Piracy, copyright infringement
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, flood, earthquake, lightning
Human error or failure	Accidents, employee mistakes, failure to follow policy
Information extortion	Blackmail of information disclosure
Missing, inadequate, or incomplete controls	Software controls, physical security
Missing, inadequate, or incomplete organizational policy or planning	Training issues, privacy, lack of effective policy
Quality of service deviations from service providers	Power and WAN quality of service issues
Sabotage or vandalism	Destruction of systems or information
Software attacks	Viruses, worms, macros, denial of service
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of property

Table 4-3 Threats to Information Security[5]

Vulnerability Identification

- Specific avenues/ways threat agents can exploit to attack an information asset are called vulnerabilities
- Examine how each threat could be perpetrated (carried out) 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
- The goal at this point: create a method for evaluating the relative risk of each listed vulnerability

Likelihood

- The probability that a specific vulnerability will be the object of a successful attack
- Assign numeric value: number between 0.1 (low) and 1.0 (high), or a number between 1 and 100
- Zero not used since vulnerabilities with zero likelihood are removed from asset/vulnerability list
- Use selected rating model consistently
- Use external references for values that have been reviewed/adjusted for your circumstances

Risk Determination

- For the purpose of relative risk assessment:
  - Risk EQUALS
  - Likelihood of vulnerability occurrence
  - TIMES value (or impact)
  - MINUS percentage risk already controlled
  - PLUS an element of uncertainty

Identify Possible Controls

- For each threat and associated vulnerabilities that have residual risk, create preliminary list of control ideas
- Residual risk is risk that remains to information asset even after existing control has been applied
- There are three general categories of controls:
  - Policies
  - Programs
  - Technologies

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

Asset	Asset Impact or Relative Value	Vulnerability	Vulnerability Likelihood	Risk-Rating Factor
Customer service request via e-mail (inbound)	55	E-mail disruption due to hardware failure	0.2	11
Customer order via SSL (inbound)	100	Lost orders due to web server hardware failure	0.1	10
Customer order via SSL (inbound)	100	Lost orders due to Web server or ISP service failure	0.1	10
Customer service request via e-mail (inbound)	55	E-mail disruption due to SMTP mail relay attack	0.1	5.5
Customer service request via e-mail (inbound)	55	E-mail disruption due to ISP service failure	0.1	5.5
Customer order via SSL (inbound)	100	Lost orders due to Web server denial-of-service attack	0.025	2.5
Customer order via SSL (inbound)	100	Lost orders due to Web server software failure	0.01	1

Table 4-9 Ranked Vulnerability Risk Worksheet

Deliverable	Purpose
Information asset classification worksheet	Assembles information about information assets and their impact
Weighted criteria analysis worksheet	Assigns ranked value or impact weight to each information asset
Ranked vulnerability risk worksheet	Assigns ranked value of risk rating for each uncontrolled asset-vulnerability pair

Table 4-10 Risk Identification and Assessment Deliverables/Releases

Risk Control Strategies

- Once ranked vulnerability risk worksheet complete, must choose one of five strategies to control each risk:
  - Defend
  - Transfer
  - Mitigate
  - Accept
  - Terminate

Defend

- 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

Transfer

- 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

Mitigate

- Attempts to reduce impact of vulnerability exploitation through planning and preparation
- Approach includes three types of plans
  - Incident **response** plan (IRP): define the actions to take while incident is in progress
  - Disaster **recovery** plan (DRP): most common mitigation procedure
  - Business **continuity** plan (BCP): encompasses/enclose continuation of business activities if catastrophic /disaster event occurs

Accept

- 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

Terminate

- Directs the organization to avoid those business activities that introduce uncontrollable risks
- May seek an alternate mechanism to meet customer needs

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/actual

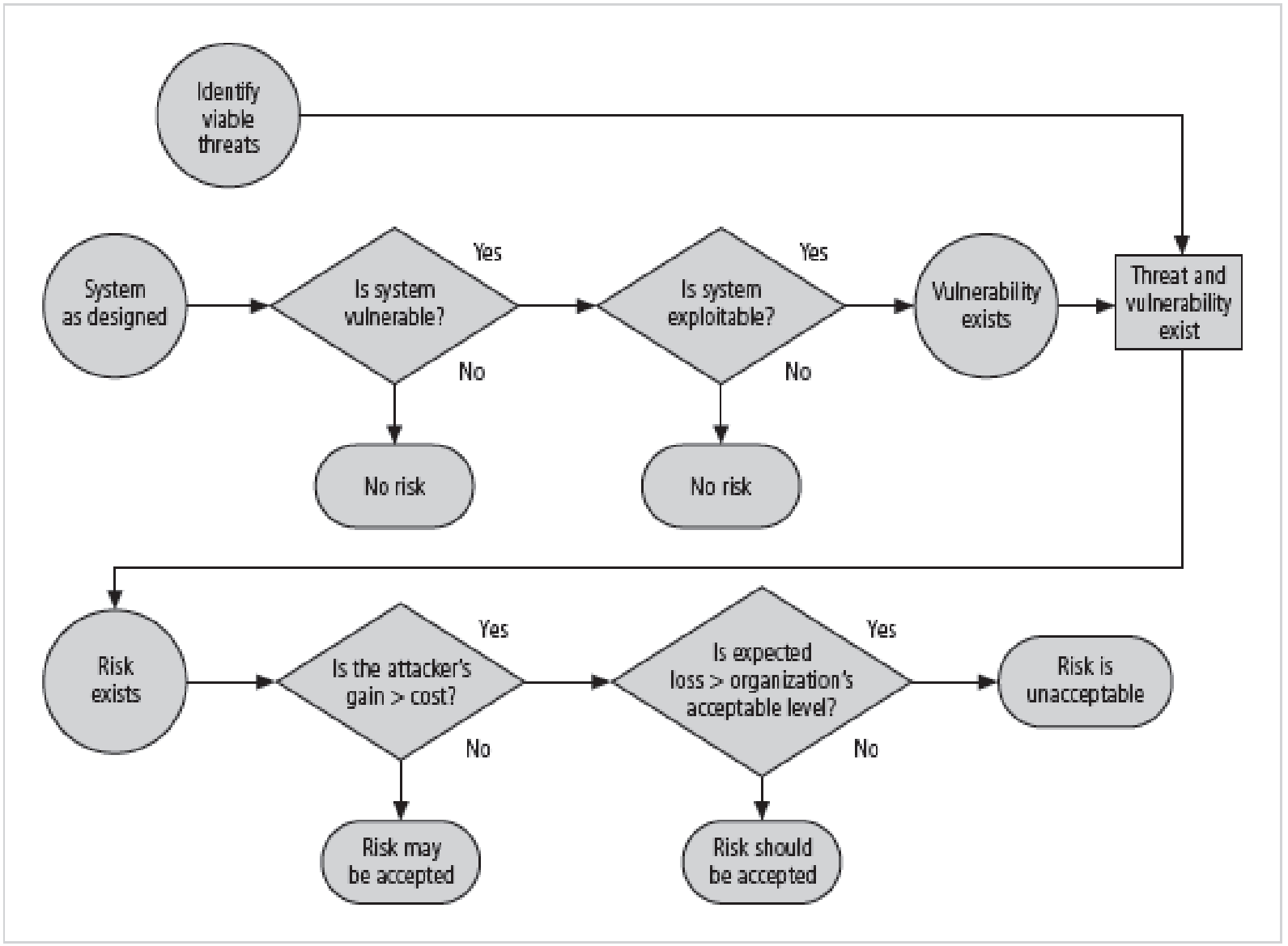

Figure 4-8 Risk Handling Decision Points

Feasibility Studies

- Before deciding on strategy, all information about economic/noneconomic consequences of vulnerability of information asset must be explored
- A number of ways exist to determine advantage of a specific control

Cost Benefit Analysis (CBA)

- Begun by evaluating worth of assets to be protected and the loss in value if they are compromised
- The formal process to document this is called cost benefit analysis or economic feasibility study
- Items that affect cost of a control or safeguard include: cost of development; training fees; implementation cost; service costs; cost of maintenance
- Benefit: value an organization realizes using controls to prevent losses from a vulnerability

Cost Benefit Analysis (CBA) (cont'd.)

- Asset valuation: process of assigning financial value or worth to each information asset
- Process result is estimate of potential loss per risk
- Expected loss per risk stated in the following equation:
  - Annualized loss expectancy (ALE) = single loss expectancy (SLE) × annualized rate of occurrence (ARO)
- SLE = asset value × exposure factor (EF)

The Cost Benefit Analysis (CBA) Formula

- CBA determines if alternative being evaluated is worth cost incurred to control vulnerability
  - CBA most easily calculated using ALE from earlier assessments, before implementation of proposed control:
    - CBA = ALE(prior) – ALE(post) – ACS
  - ALE(prior) is annualized loss expectancy of risk before implementation of control
  - ALE(post) is estimated ALE based on control being in place for a period of time
  - ACS is the annualized cost of the safeguard/protection

Evaluation, Assessment, and Maintenance of Risk Controls

- Selection and implementation of control strategy is not end of process
- Strategy and accompanying controls must be monitored/reevaluated on ongoing basis to determine effectiveness and to calculate more accurately the estimated residual risk
- Process continues as long as organization continues to function

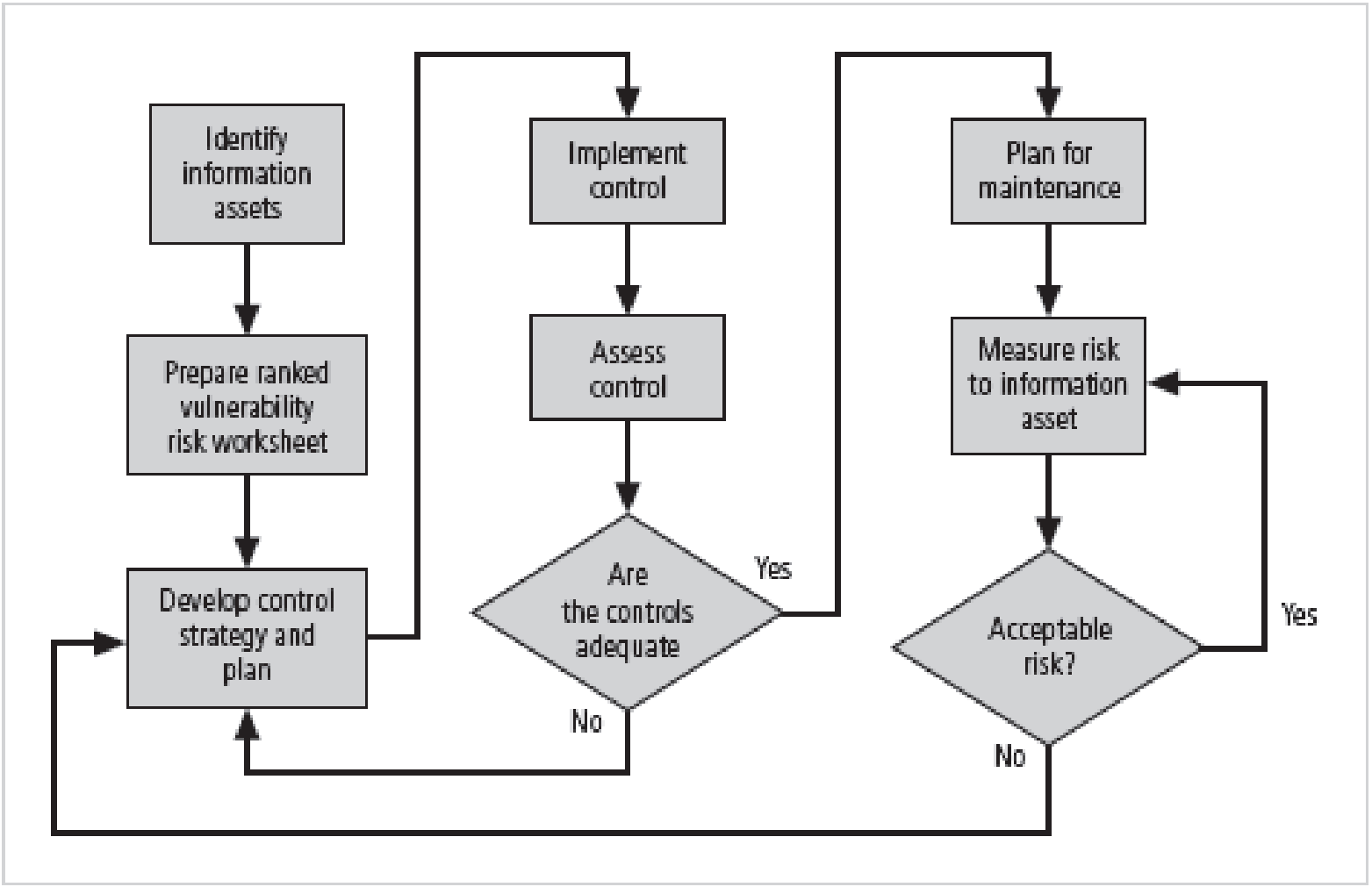

Figure 4-9 Risk Control Cycle

Benchmarking and Best Practices

- An alternative approach to risk management
- Benchmarking: 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 and Best Practices (cont'd.)

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

Benchmarking and Best Practices (cont'd.)

- Problems with the application of 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

Benchmarking and Best Practices (cont'd.)

- Baselining
  - Analysis of measures against established standards
  - In information security, baselining is comparison of security activities and events against an organization's future performance
  - Useful during baselining to have a guide to the overall process

Risk Management Discussion Points

- Organization must define level of risk it can live with
- Risk appetite: defines quantity and nature/type of risk that organizations are willing to accept as trade-offs between perfect security and unlimited accessibility
- Residual risk: risk that has not been completely removed, shifted, or planned for

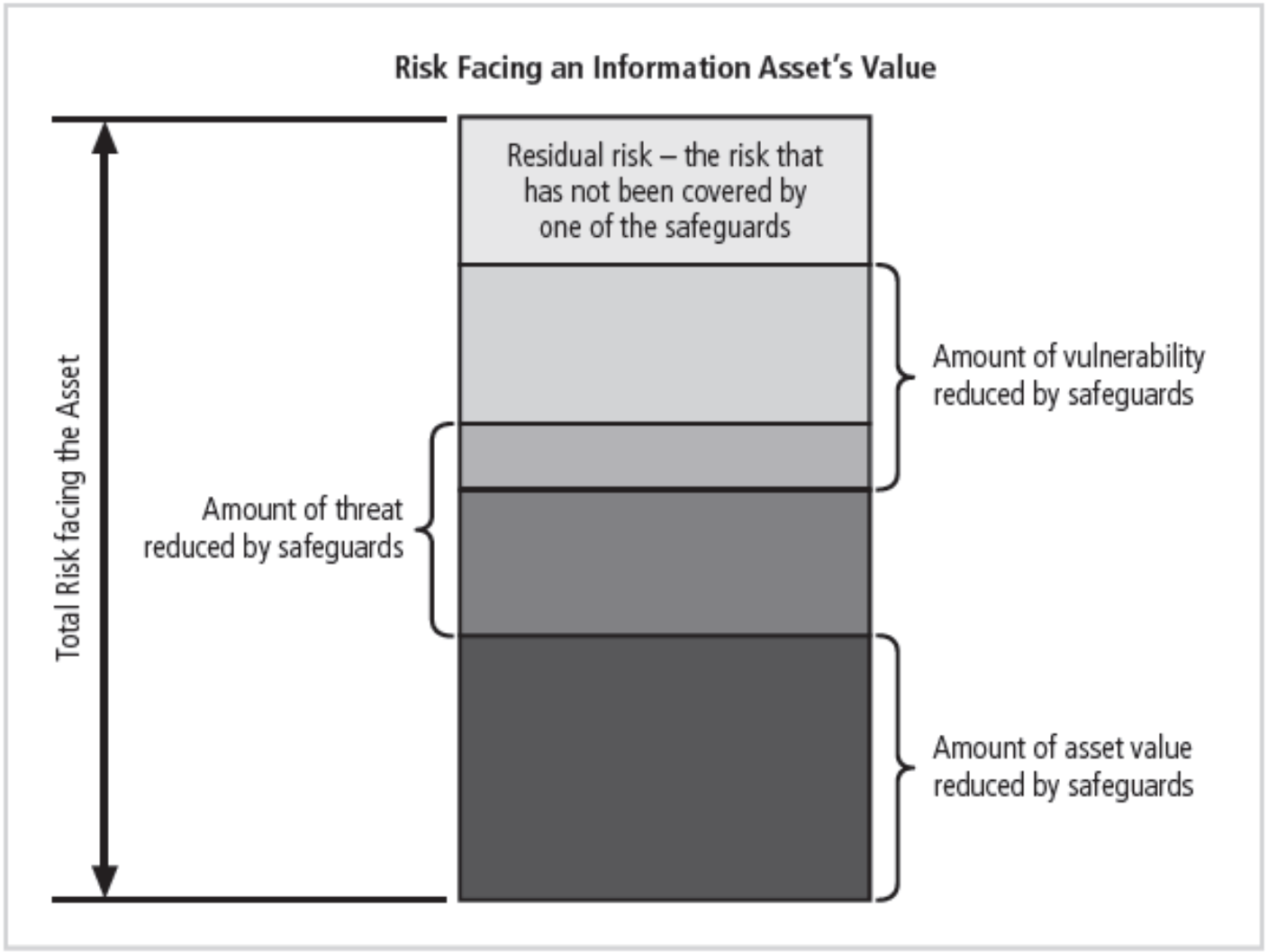

Figure 4-10 Residual risk

Documenting Results

- At minimum, each information asset-threat pair should have documented control strategy clearly identifying any remaining residual risk
- Another option: document outcome of control strategy for each information asset-vulnerability pair as an action plan
- Risk assessment may be documented in a topic-specific report

Recommended Risk Control Practices

- Convince budget authorities to spend up to value of asset to protect from identified threat
- Final control choice may be balance of controls providing greatest value to as many asset-threat pairs as possible
- Organizations looking to implement controls that don't involve such complex, inexact, and dynamic calculations

Summary

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

Summary (continued)

- Risk control: five strategies are used to control risks that result from vulnerabilities:
  - Defend
  - Transfer
  - Mitigate
  - Accept
  - Terminate

Summary (continued)

- Selecting a risk control strategy
  - Cost Benefit Analysis
- Risk Control
  - Best Practices and Benchmarks