COURSE TECHNOLOGY
CENGAGE Learning™

Principals of Information Security, Fourth Edition

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

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

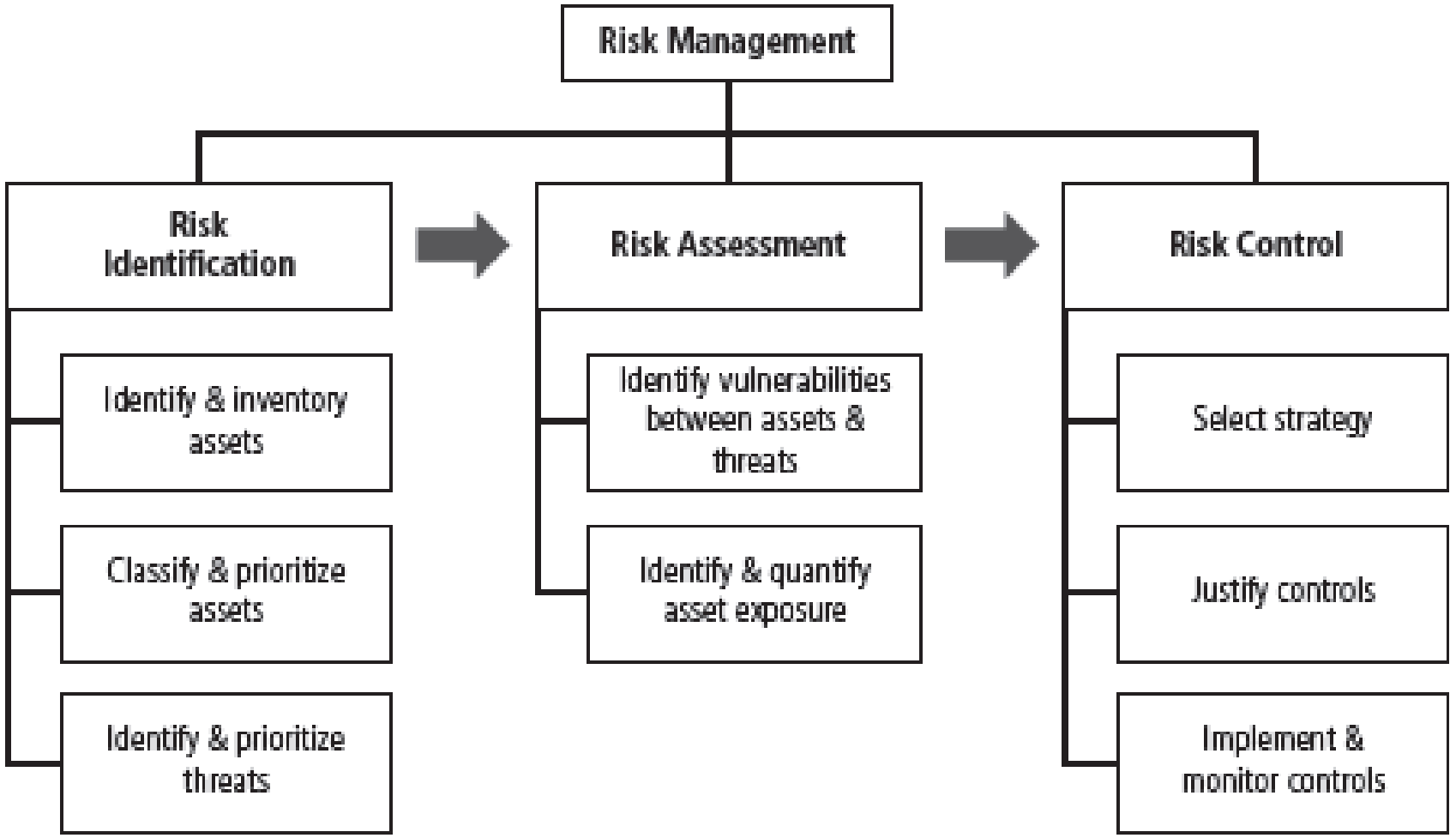

Figure 4-1 Components of Risk Management

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 Identification

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

1. 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
  - Reviews
  - Presentations to management
- Tasks laid out, assignments made and timetables discussed

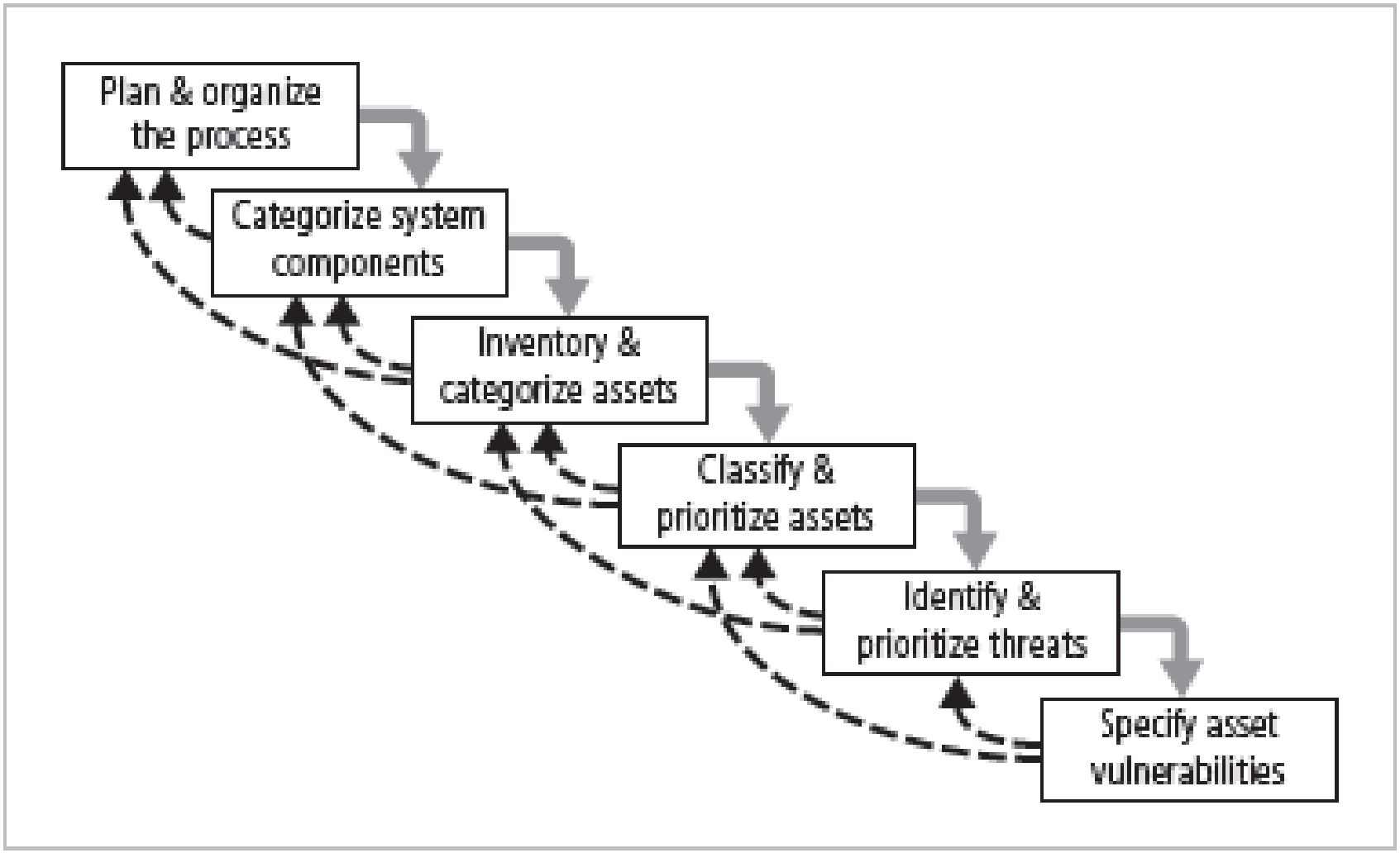

Figure 4-2 Components of Risk Identification

2. Categorize System components

- 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

3. Inventory & categorize assets

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

3. Inventory & categorize assets

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

4. 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

4. Classifying and Prioritizing Information Assets

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?

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

- 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

5. 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 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]

Risk Assessment

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

1. Identify vulnerabilities (asset – threat)

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

2. Identify Asset Exposure

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

Risk Control

1. Select Strategy

- 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 continuation of business activities if catastrophic 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

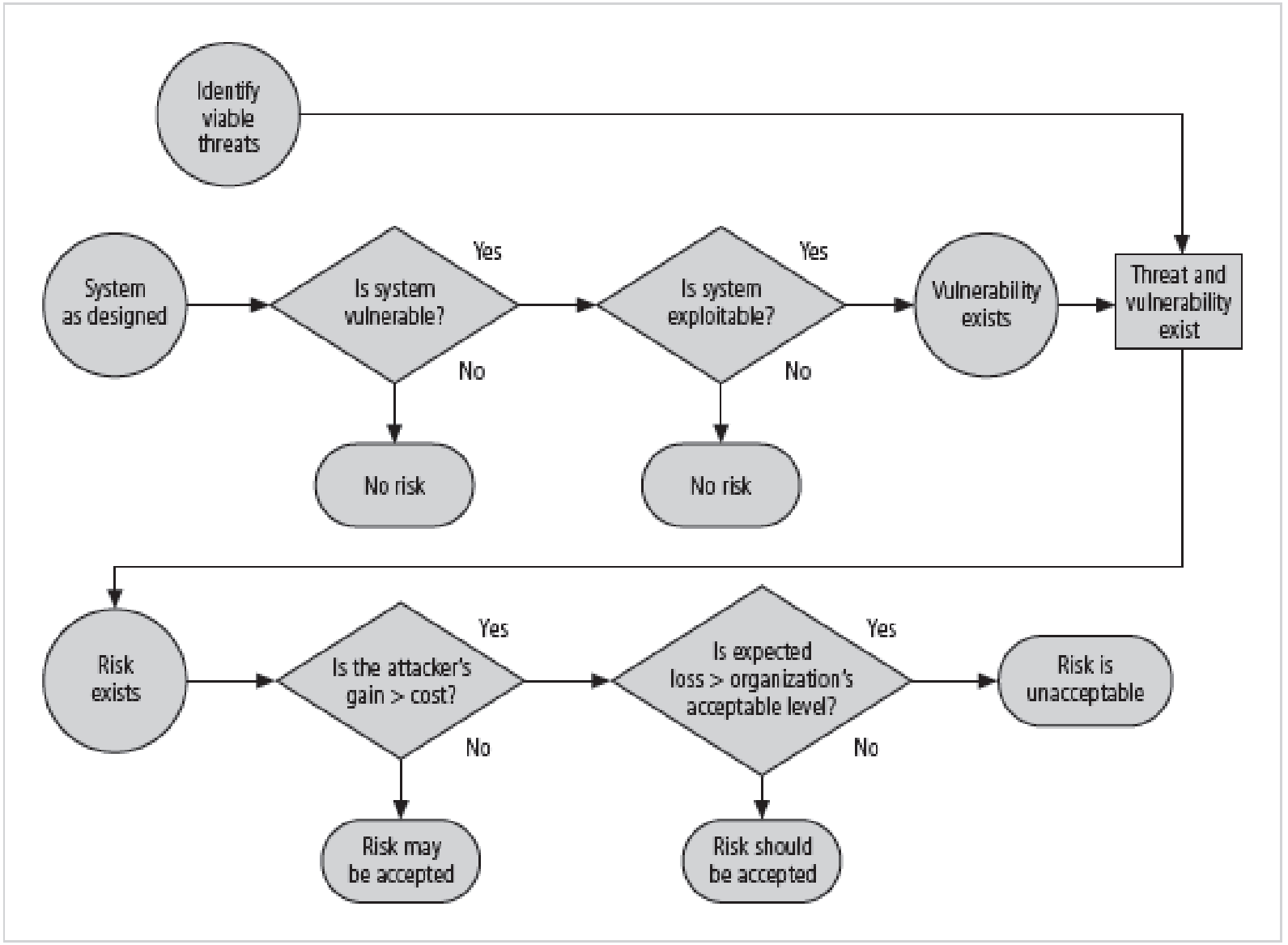

Figure 4-8 Risk Handling Decision Points

2. Justify Controls

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

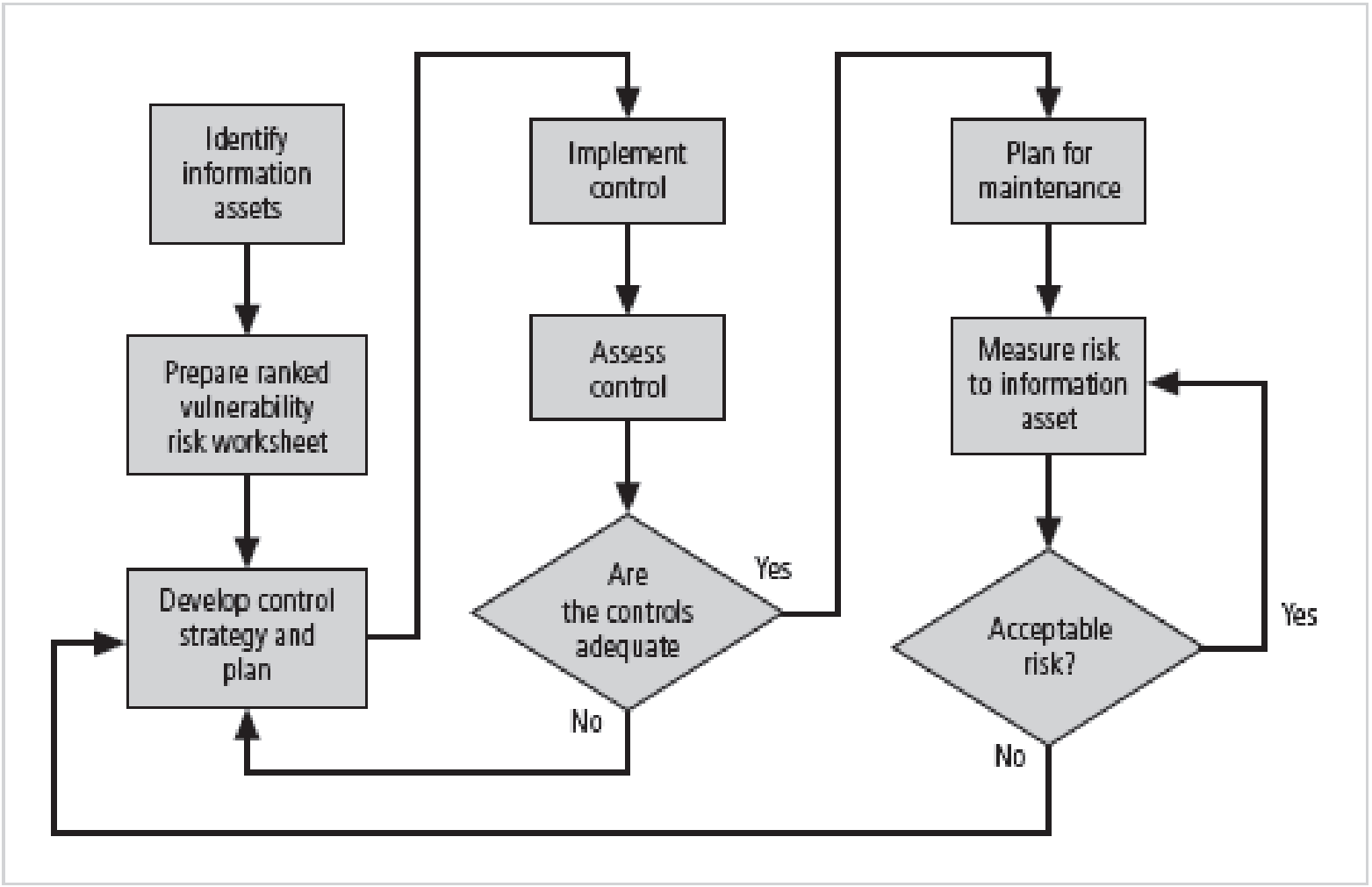

Figure 4-9 Risk Control Cycle

Summary (continued)

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