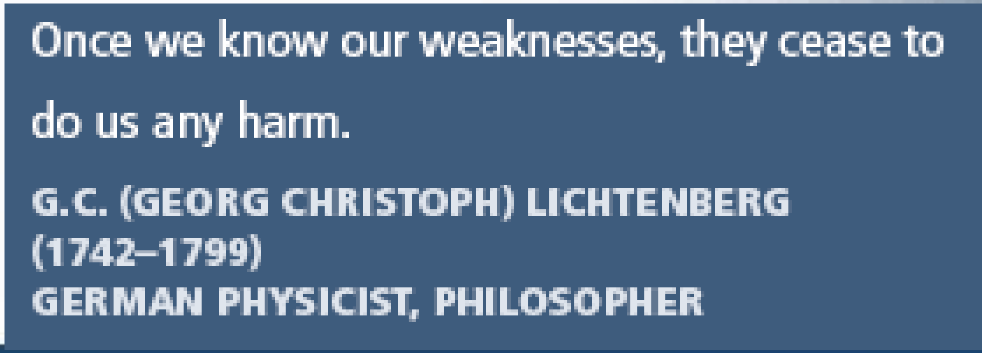
COURSE TECHNOLOGY
CENGAGE Learning™

Principles of Information Security, Fifth Edition

Chapter 5

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
  - 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)

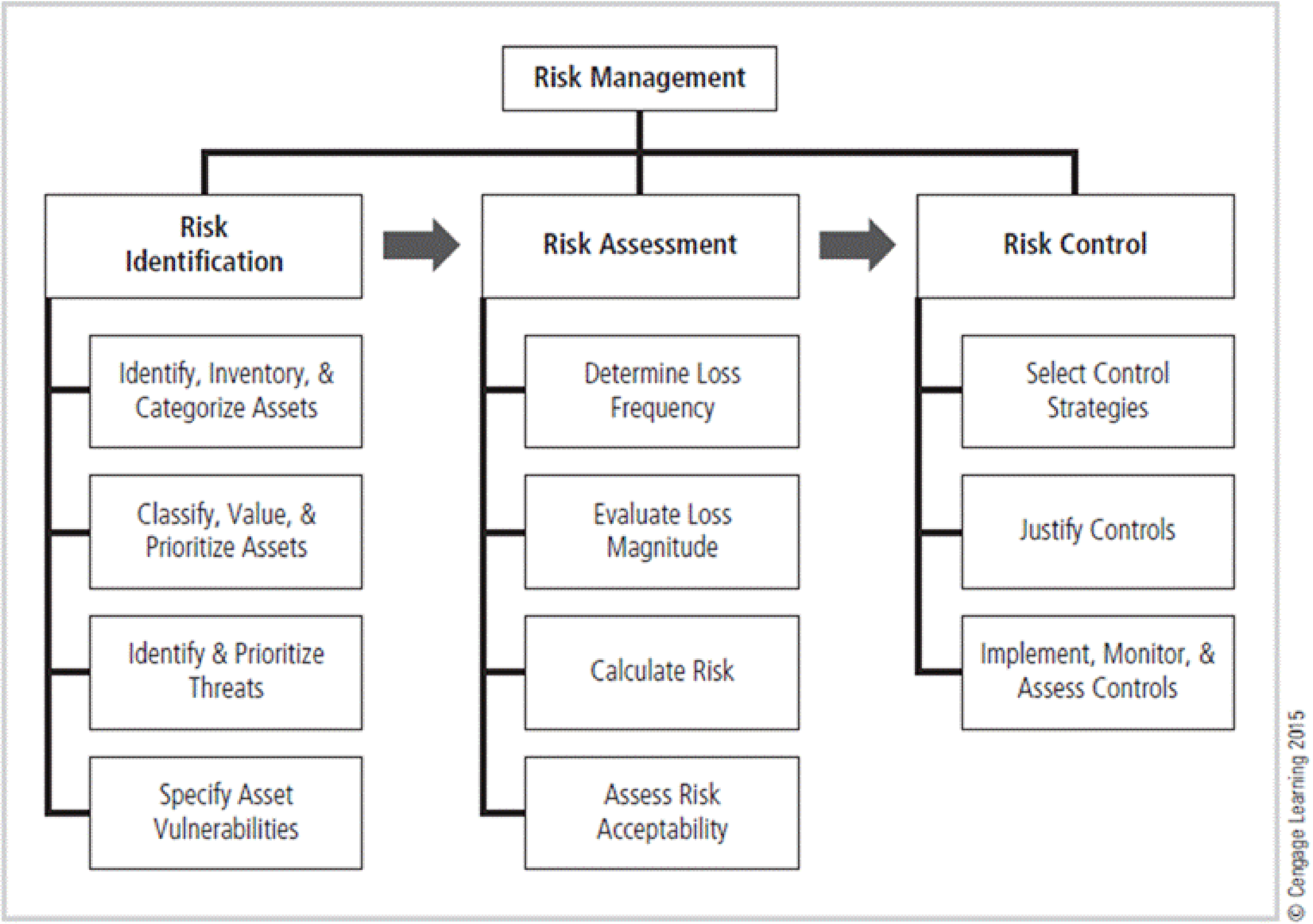
- Describe the various risk mitigation strategy options
- Identify the categories that can be used to classify controls
- Discuss conceptual frameworks for evaluating risk controls and formulate a cost-benefit analysis

Introduction

- Organizations must design and create safe environments in which business processes and procedures can function.
- Risk management: the process of identifying, assessing, and reducing risks facing an organization
- Risk identification: the enumeration and documentation of risks to an organization’s information assets
- Risk control: the application of controls that reduce the risks to an organization’s assets to an acceptable level

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 the threats facing the organization
- Responsibility of each community of interest within an organization to manage the risks that are encountered


Risk Management
Risk Identification
Risk Assessment
Risk Control
Identify, Inventory, & Categorize Assets
Classify, Value, & Prioritize Assets
Identify & Prioritize Threats
Specify Asset Vulnerabilities
Determine Loss Frequency
Evaluate Loss Magnitude
Calculate Risk
Assess Risk Acceptability
Select Control Strategies
Justify Controls
Implement, Monitor, & Assess Controls

© Cengage Learning 2015

Figure 5-1 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 Appetite and Residual Risk

- Risk appetite: It defines the quantity and nature of risk that organizations are willing to accept as trade-offs between perfect security and unlimited accessibility.
  - Reasoned approach is one that balances the expense of controlling vulnerabilities against possible losses if the vulnerabilities are exploited.
- Residual risk: risk that has not been completely removed, shifted, or planned for
  - The goal of information security is to bring residual risk into line with risk appetite.

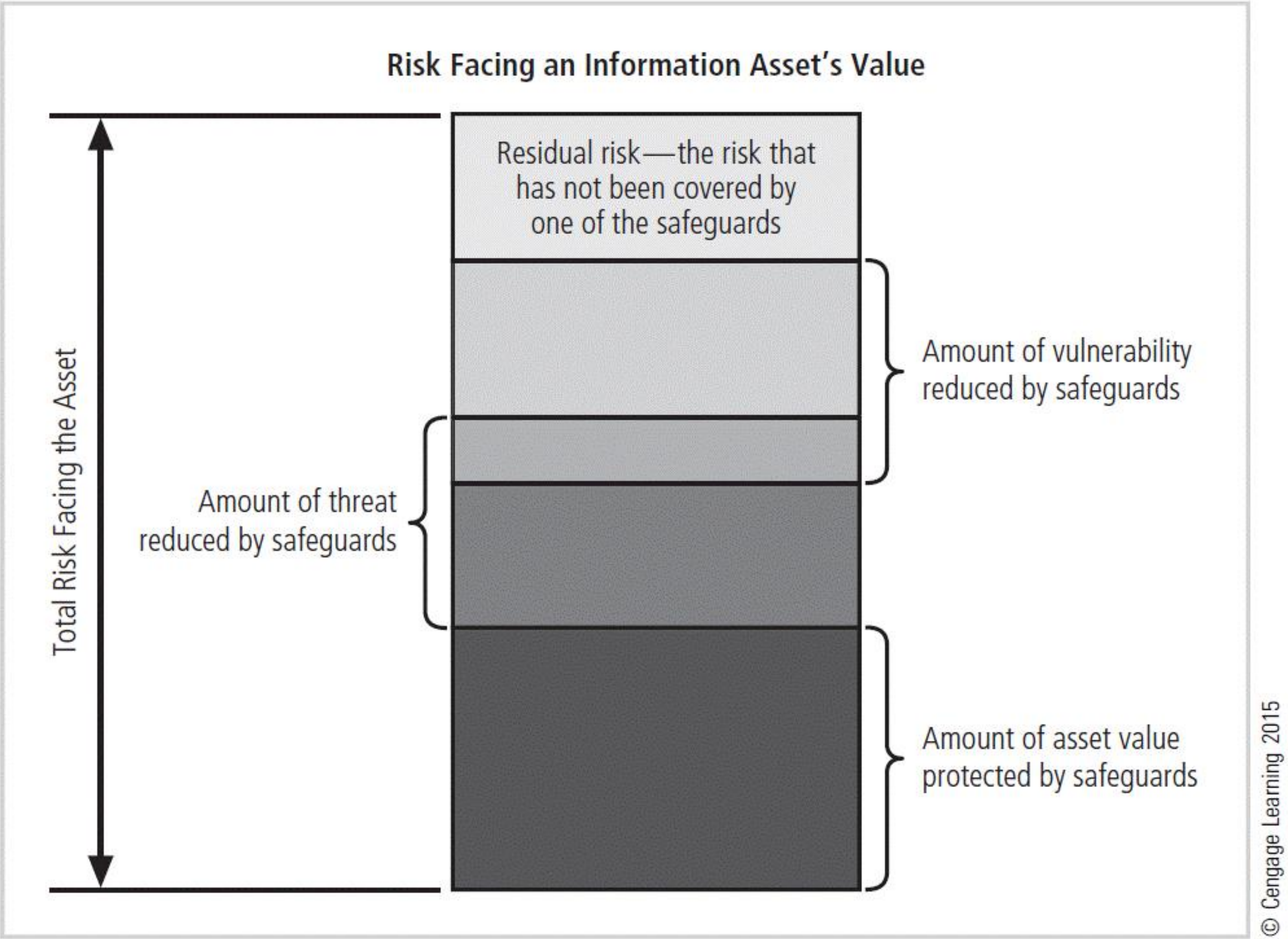

Risk Facing an Information Asset's Value
Total Risk Facing the Asset
Residual risk—the risk that has not been covered by one of the safeguards
Amount of vulnerability reduced by safeguards
Amount of threat reduced by safeguards
Amount of asset value protected by safeguards
© Cengage Learning 2015

Figure 5-3 Residual risk

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.

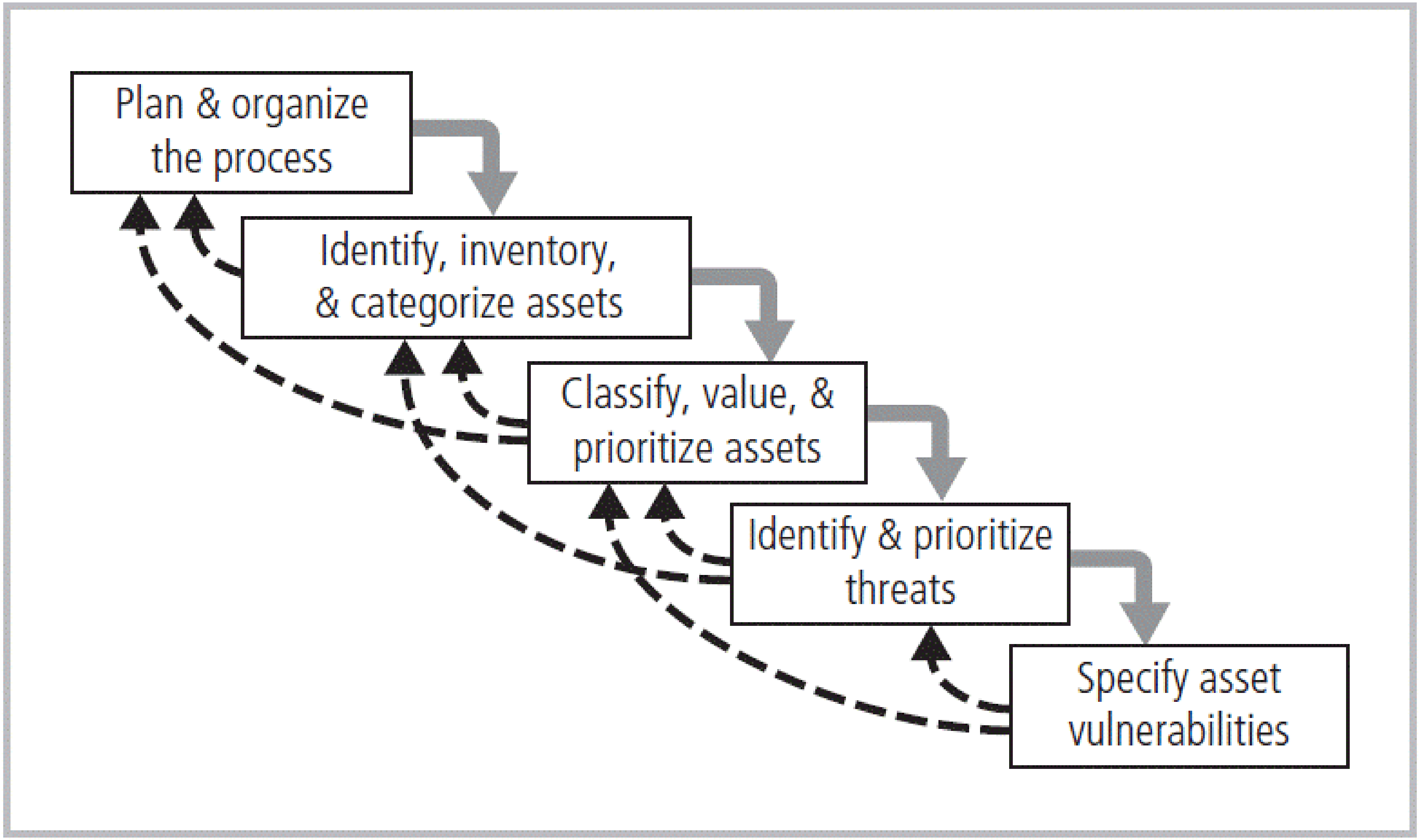

Plan & organize the process
Identify, inventory, & categorize assets
Classify, value, & prioritize assets
Identify & prioritize threats
Specify asset vulnerabilities

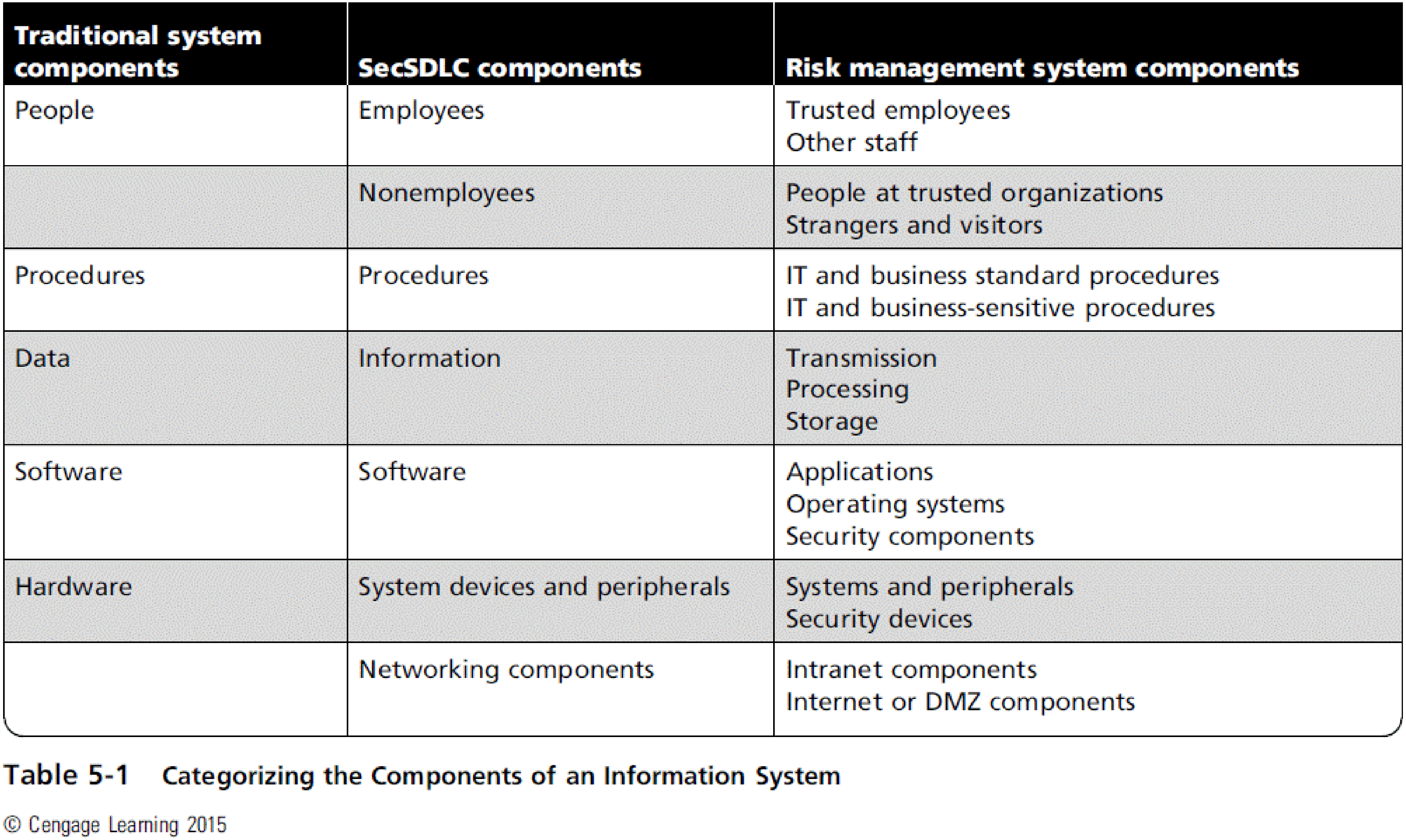
Figure 5-4 Components of risk identification

Plan and Organize the Process

- The 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

Identifying, Inventorying, and Categorizing Assets

- Iterative process: Begins with the identification and inventory of assets, including all elements of an organization’s system (people, procedures, data and information, software, hardware, networking)
- Assets are then categorized.



Traditional system components	SecSDLC components	Risk management system components
People	Employees	Trusted employees Other staff
	Nonemployees	People at trusted organizations Strangers and visitors
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 5-1 **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; relation to software/hardware/networking elements; 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, and controlling entity.

Asset Inventory

- Unless information assets are identified and inventoried, they cannot be effectively protected.
- Inventory process involves formalizing the identification process in some form of organizational tool.
- Automated tools can sometimes identify the system elements that make up hardware, software, and network components.

Asset Categorization

- People comprise employees and nonemployees.
- Procedures either do not expose knowledge useful to a potential attacker or are sensitive and could allow adversary to gain advantage.
- Data components account for the management of information in transmission, processing, and storage.
- Software components are applications, operating systems, or security components.
- Hardware: either the usual system devices and peripherals or part of information security control systems

Classifying, Valuing, and Prioritizing Information Assets

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

Data Classification and Management

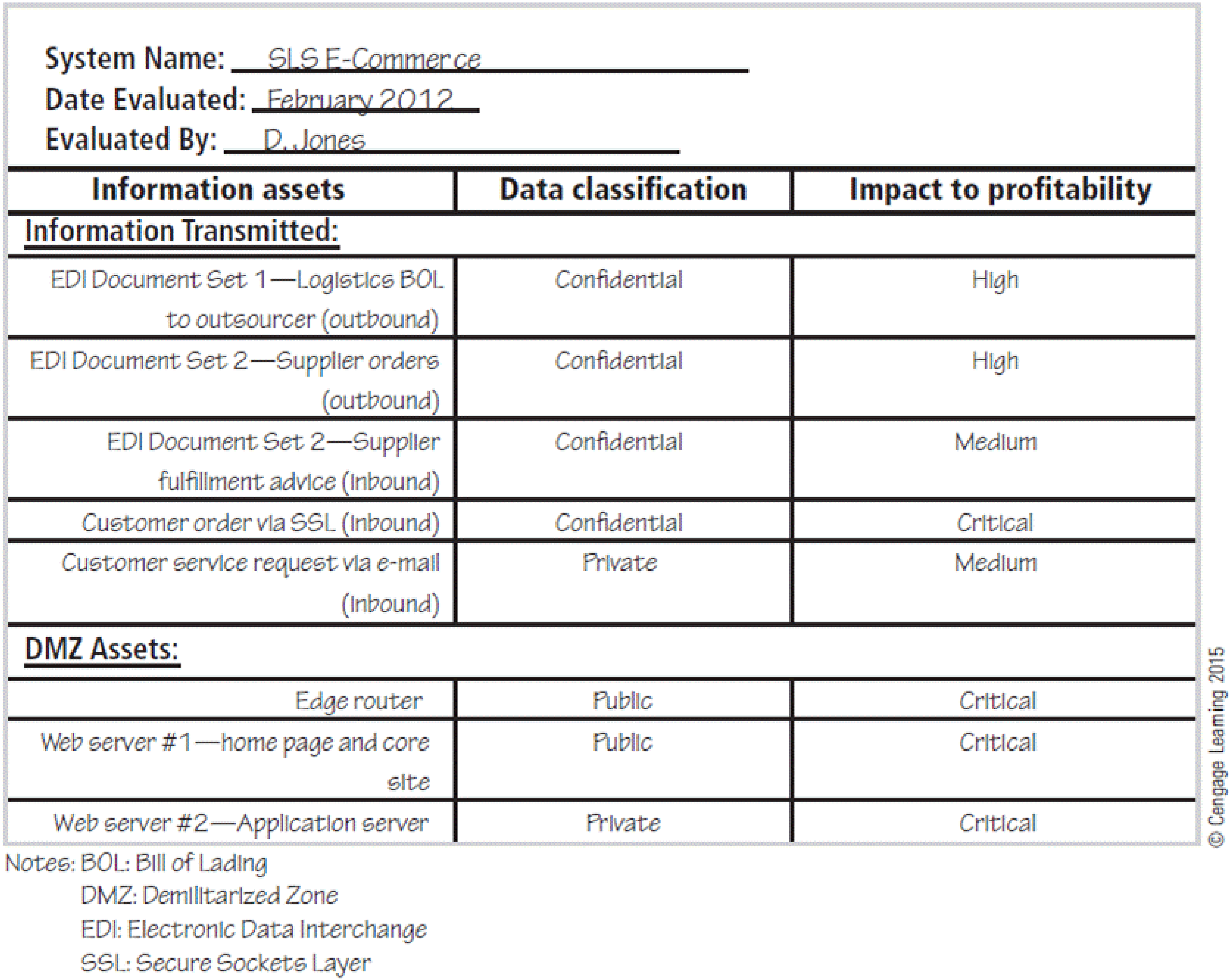
- Variety of classification schemes are used by corporate and military organizations.
- Information owners are responsible for classifying their information assets.
- Information classifications must be reviewed periodically.
- Classifications include confidential, internal, and external.

Data Classification and Management (cont'd)

- Security clearances
  - Each data user must be assigned authorization level indicating classification level.
  - Before accessing specific set of data, the employee must meet the need-to-know requirement.
- Management of classified data includes storage, distribution, transportation, and destruction.
- Clean desk policy
- Dumpster diving

Information Asset Valuation

- Questions help develop criteria for asset valuation.
- Which information asset:
  - Is most critical to the organization’s success?
  - Generates the most revenue/profitability?
  - Plays the biggest role in generating revenue or delivering services?
  - Would be the 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 2012

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

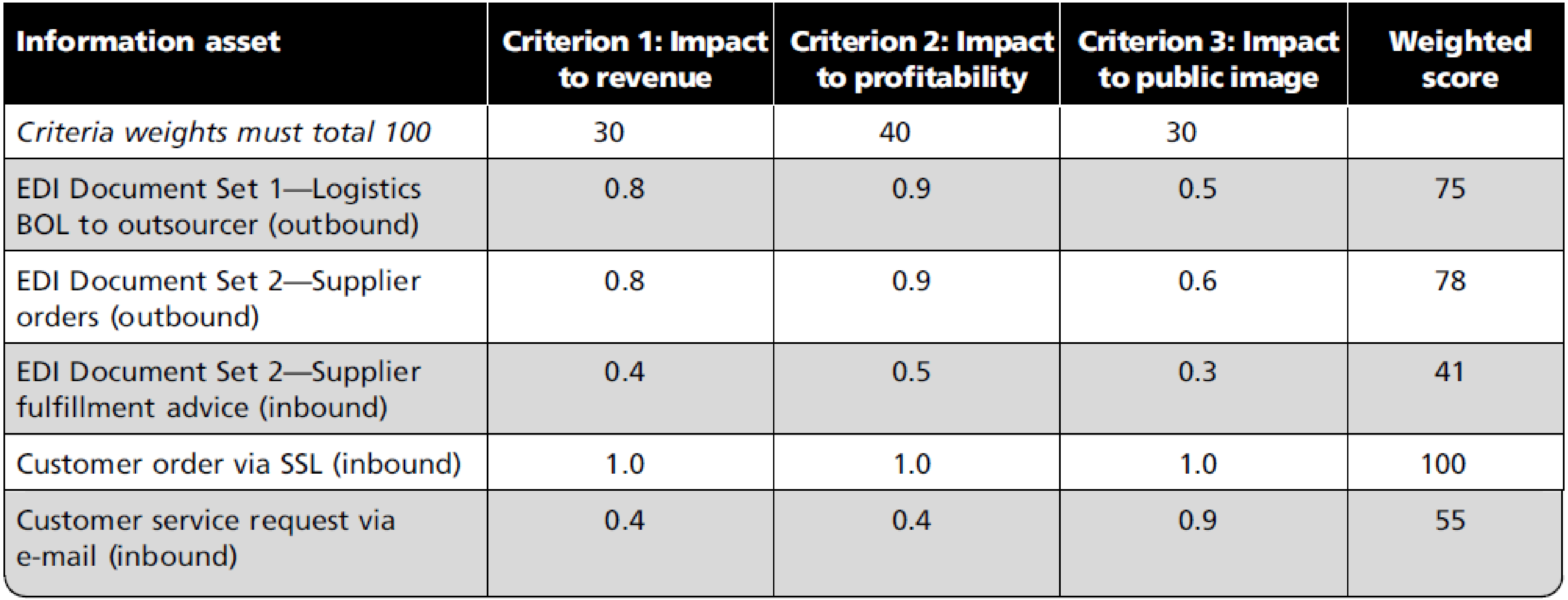
Notes: BOL: Bill of Lading
DMZ: Demilitarized Zone
EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

© Cengage Learning 2015

Figure 5-7 Sample inventory worksheet

Information Asset Valuation (cont’d)

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



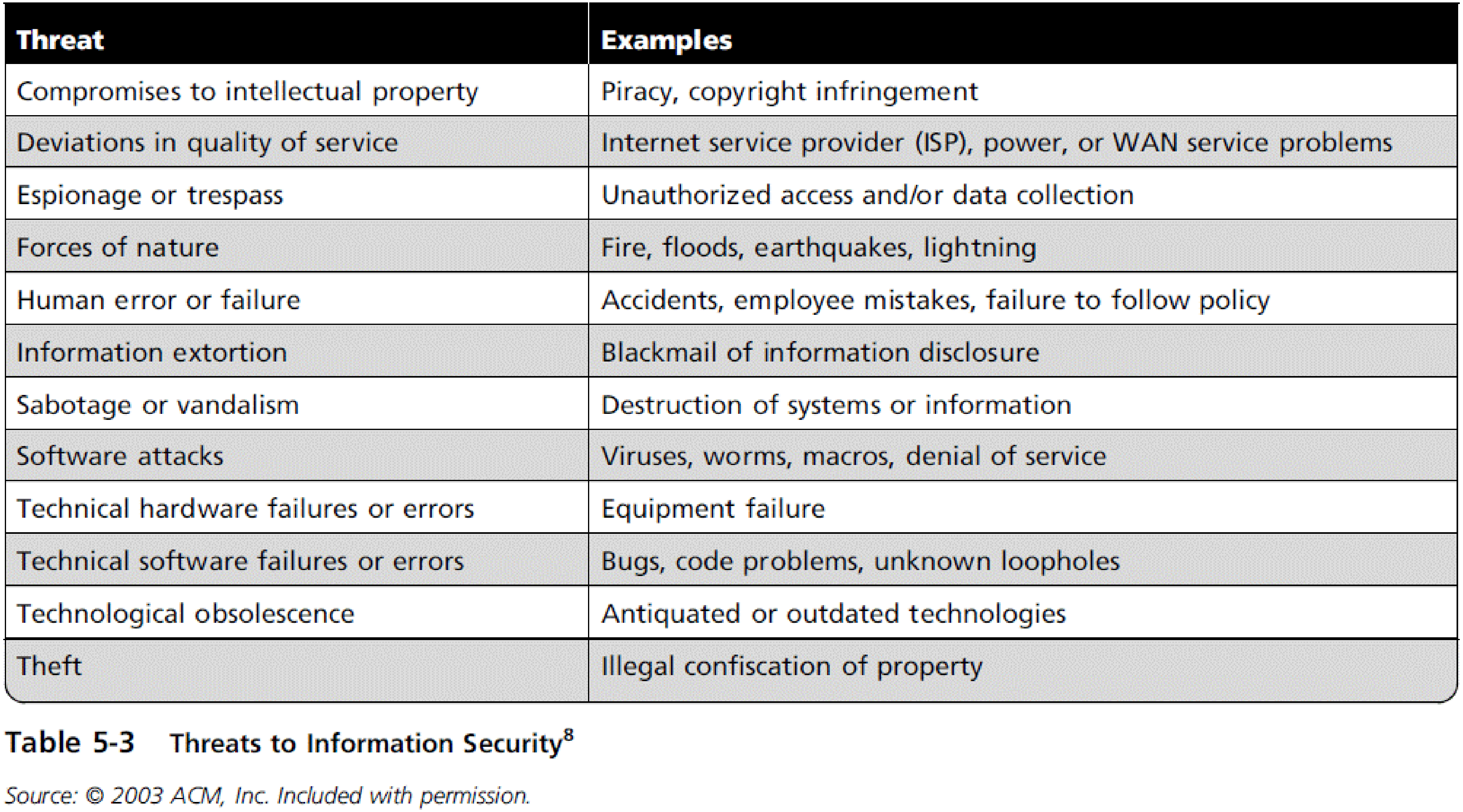
Information asset	Criterion 1: Impact to revenue	Criterion 2: Impact to profitability	Criterion 3: Impact to public image	Weighted score
Criteria weights must total 100	30	40	30	
EDI Document Set 1—Logistics BOL to outsourcer (outbound)	0.8	0.9	0.5	75
EDI Document Set 2—Supplier orders (outbound)	0.8	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 5-2 **Example of a Weighted Factor Analysis Worksheet**

Note: In the table, EDI stands for *electronic data interchange,* BOL stands for *bill of lading*, and SSL is 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 a successful attack?
  - Which threat requires greatest expenditure to prevent?



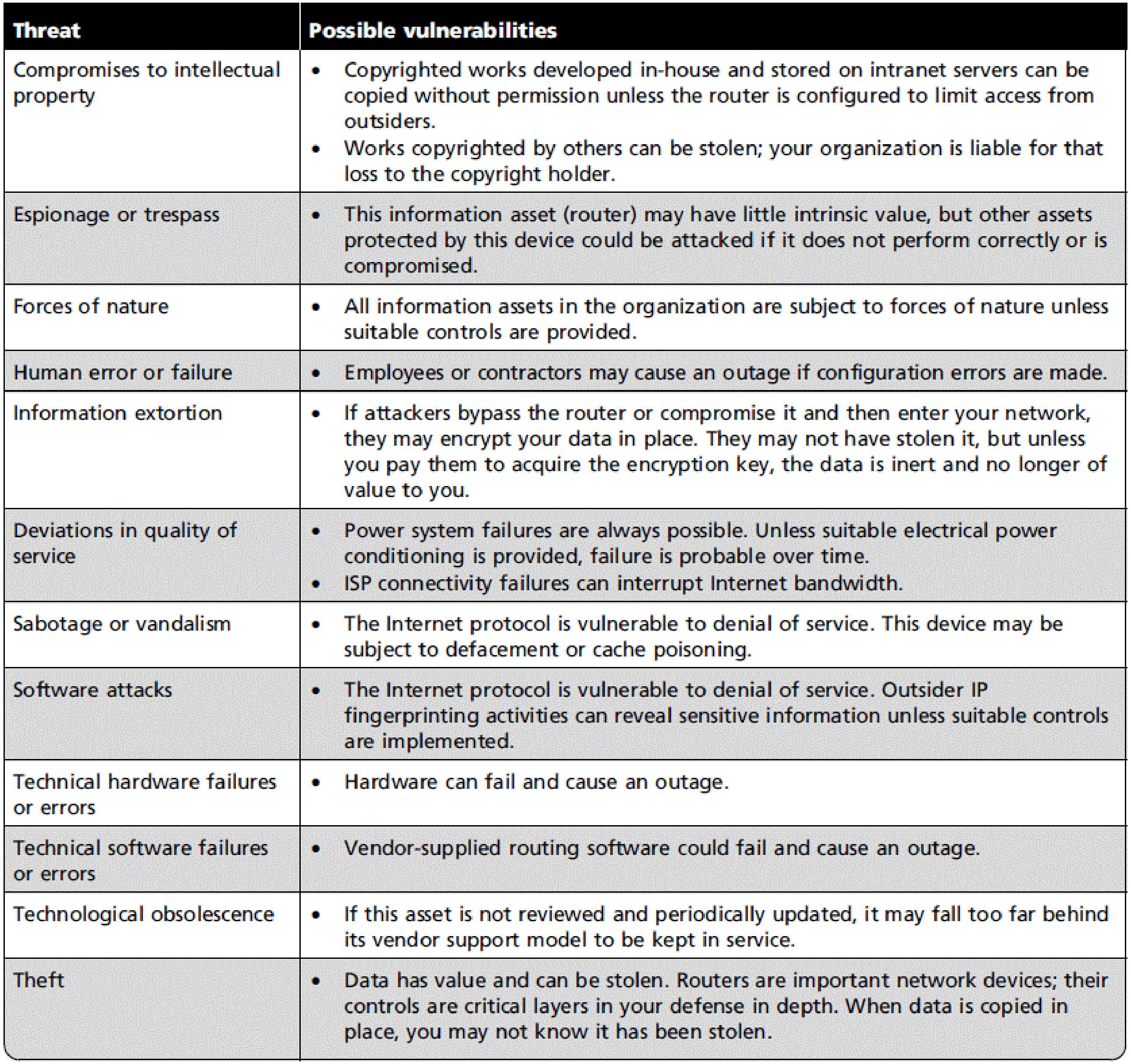
Threat	Examples
Compromises to intellectual property	Piracy, copyright infringement
Deviations in quality of service	Internet service provider (ISP), power, or WAN service problems
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, floods, earthquakes, lightning
Human error or failure	Accidents, employee mistakes, failure to follow policy
Information extortion	Blackmail of information disclosure
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 5-3 **Threats to Information Security**[8]

Source: © 2003 ACM, Inc. Included with permission.

Specifying Asset Vulnerabilities

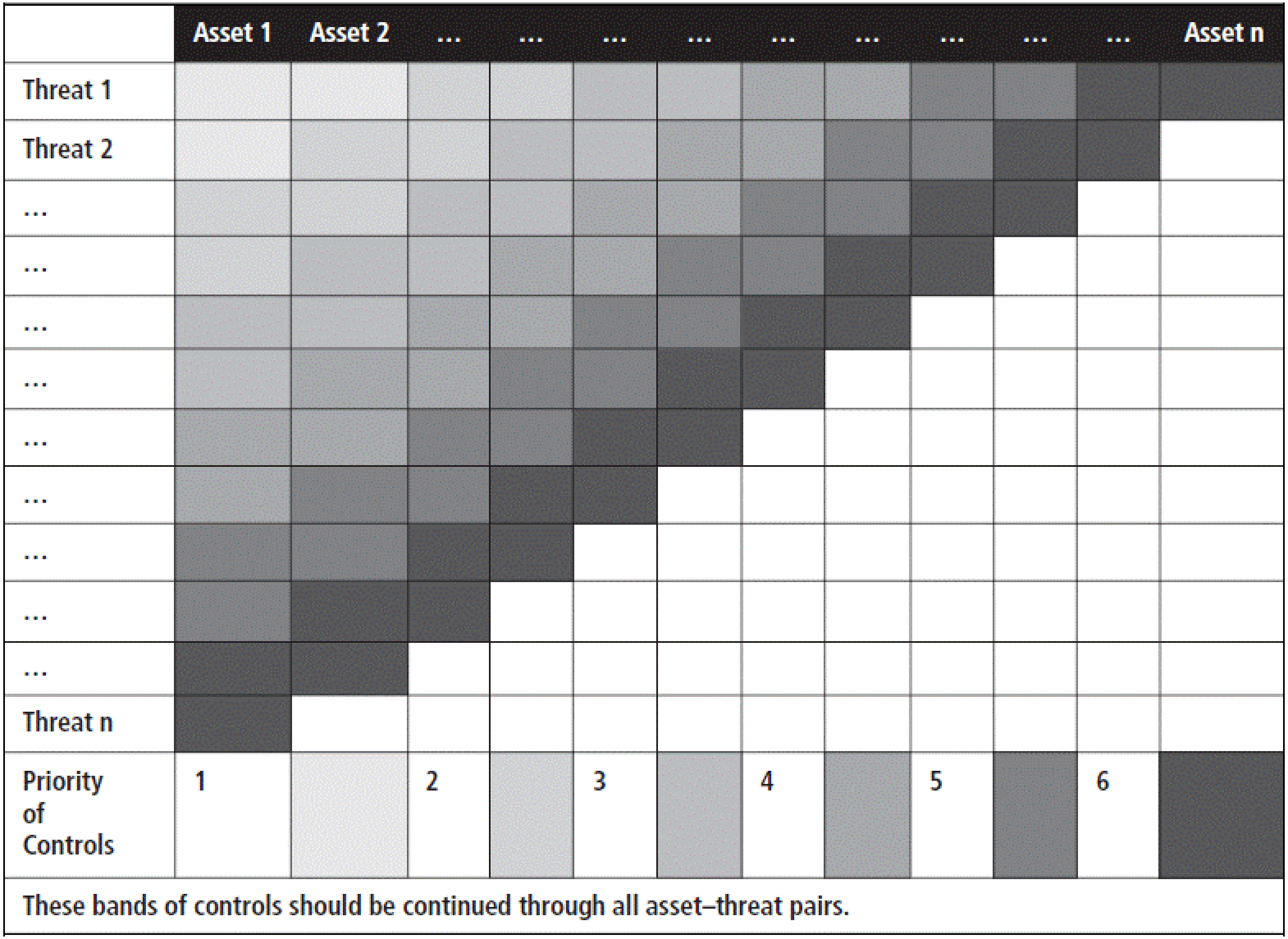
- Specific avenues threat agents can exploit to attack an information asset are called vulnerabilities.
- Examine how each threat could be perpetrated and list the organization’s assets and vulnerabilities.
- Process works best when people with diverse backgrounds within organization work iteratively in a series of brainstorming sessions.
- At the end of the risk identification process, prioritized list of assets with their vulnerabilities is achieved.
  - Can be combined with weighted list of threats to form threats-vulnerabilities-assets (TVA) worksheet



Threat	Possible vulnerabilities
Compromises to intellectual property	• Copyrighted works developed in-house and stored on intranet servers can be copied without permission unless the router is configured to limit access from outsiders. • Works copyrighted by others can be stolen; your organization is liable for that loss to the copyright holder.
Espionage or trespass	• This information asset (router) may have little intrinsic value, but other assets protected by this device could be attacked if it does not perform correctly or is compromised.
Forces of nature	• All information assets in the organization are subject to forces of nature unless suitable controls are provided.
Human error or failure	• Employees or contractors may cause an outage if configuration errors are made.
Information extortion	• If attackers bypass the router or compromise it and then enter your network, they may encrypt your data in place. They may not have stolen it, but unless you pay them to acquire the encryption key, the data is inert and no longer of value to you.
Deviations in quality of service	• Power system failures are always possible. Unless suitable electrical power conditioning is provided, failure is probable over time. • ISP connectivity failures can interrupt Internet bandwidth.
Sabotage or vandalism	• The Internet protocol is vulnerable to denial of service. This device may be subject to defacement or cache poisoning.
Software attacks	• The Internet protocol is vulnerable to denial of service. Outsider IP fingerprinting activities can reveal sensitive information unless suitable controls are implemented.
Technical hardware failures or errors	• Hardware can fail and cause an outage.
Technical software failures or errors	• Vendor-supplied routing software could fail and cause an outage.
Technological obsolescence	• If this asset is not reviewed and periodically updated, it may fall too far behind its vendor support model to be kept in service.
Theft	• Data has value and can be stolen. Routers are important network devices; their controls are critical layers in your defense in depth. When data is copied in place, you may not know it has been stolen.

Table 5-7 **Vulnerability Assessment of a Hypothetical DMZ Router**

© Cengage Learning 2015



	Asset 1	Asset 2	…	…	…	…	…	…	…	…	…	Asset n
Threat 1	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
Threat 2	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	
…	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨		
…	▨	▨	▨	▨	▨	▨	▨	▨	▨			
…	▨	▨	▨	▨	▨	▨	▨	▨				
…	▨	▨	▨	▨	▨	▨	▨					
…	▨	▨	▨	▨	▨	▨						
…	▨	▨	▨	▨	▨							
…	▨	▨	▨	▨								
…	▨	▨	▨									
…	▨	▨										
Threat n	▨											
Priority of Controls	1	▨	2	▨	3	▨	4	▨	5	▨	6	▨
These bands of controls should be continued through all asset–threat pairs.												

Table 5-8 Sample TVA Spreadsheet

© Cengage Learning 2015

Risk Assessment

- Risk assessment evaluates the relative risk for each vulnerability.
- It assigns a risk rating or score to each information asset.
- Planning and organizing risk assessment
  - The goal at this point is to create a method for evaluating the relative risk of each listed vulnerability.

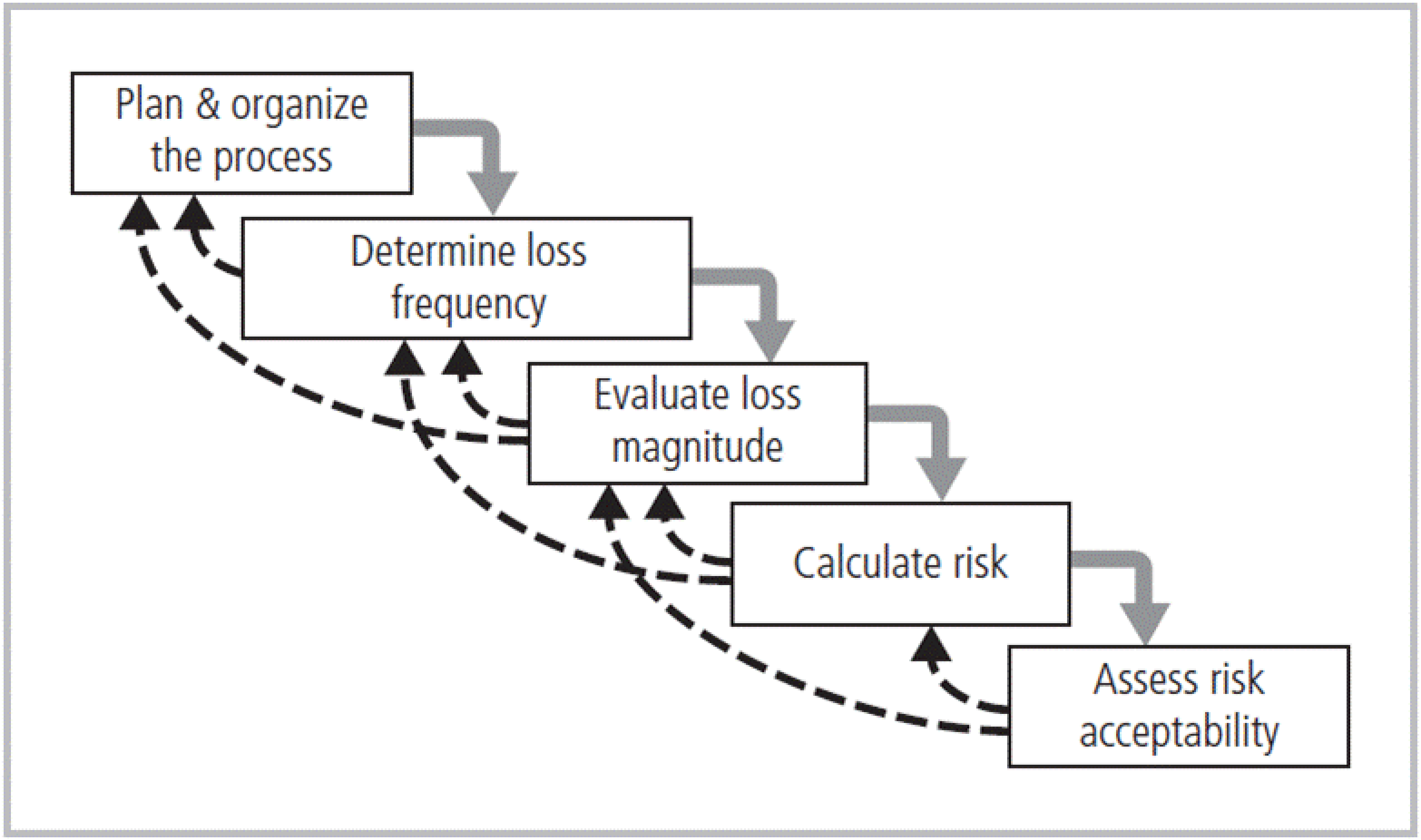


Figure 5-8 Major stages of risk assessment

Determining the Loss Frequency

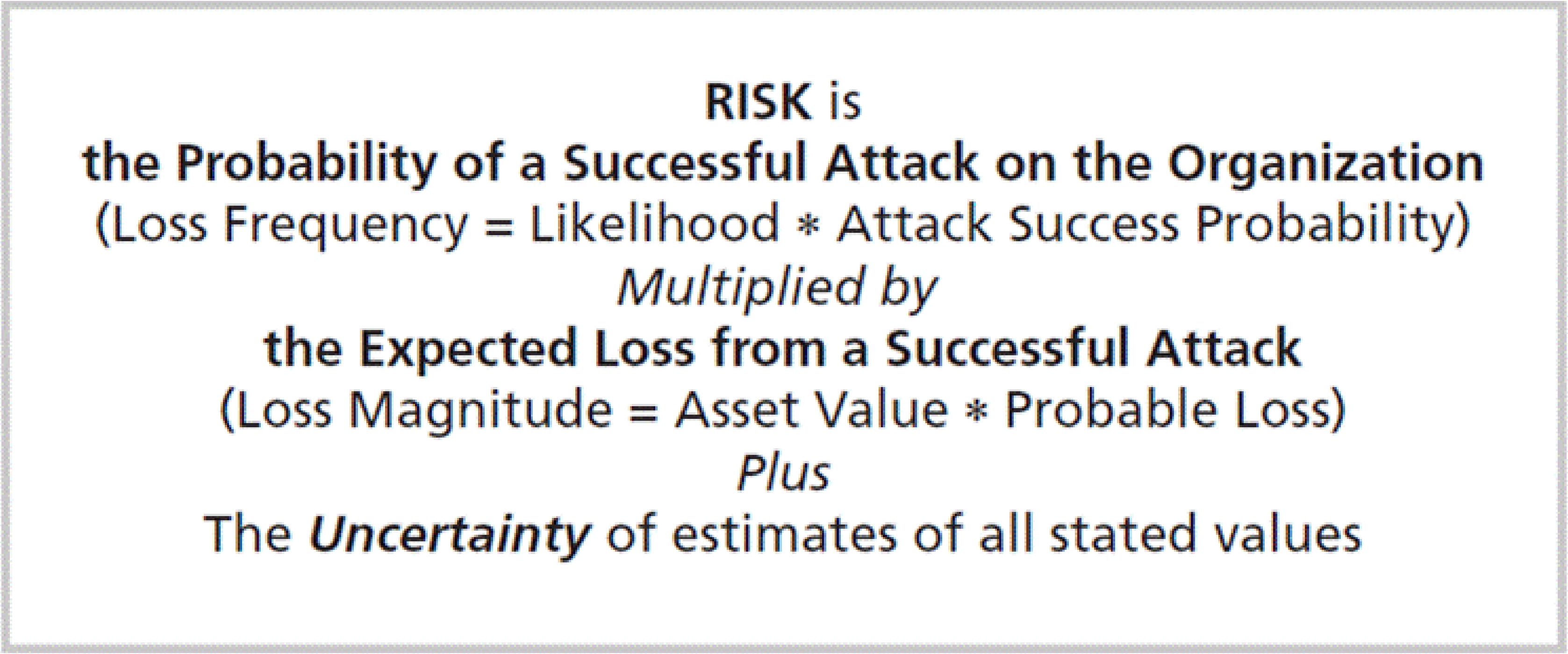
- Describes an assessment of the likelihood of an attack combined with expected probability of success
- Use external references for values that have been reviewed/adjusted for your circumstances.
- Assign numeric value to likelihood, typically annual value.
  - Targeted by hackers once every five years: 1/5, 20 percent
- Determining an attack's success probability by estimating quantitative value (e.g., 10 percent) for the likelihood of a successful attack; value subject to uncertainty

Evaluating Loss Magnitude

- The next step is to determine how much of an information asset could be lost in a successful attack.
  - Also known as loss magnitude or asset exposure
- Combines the value of information asset with the percentage of asset lost in event of a successful attack
- Difficulties involve:
  - Valuating an information asset
  - Estimating percentage of information asset lost during best-case, worst-case, and most likely scenarios

Calculating Risk

- For the purpose of relative risk assessment, risk equals:
  - Loss frequency TIMES loss magnitude
  - MINUS the percentage of risk mitigated by current controls
  - PLUS an element of uncertainty



RISK is

the Probability of a Successful Attack on the Organization

(Loss Frequency = Likelihood * Attack Success Probability)

Multiplied by

the Expected Loss from a Successful Attack

(Loss Magnitude = Asset Value * Probable Loss)

Plus

The ***Uncertainty*** of estimates of all stated values

© Cengage Learning 2015

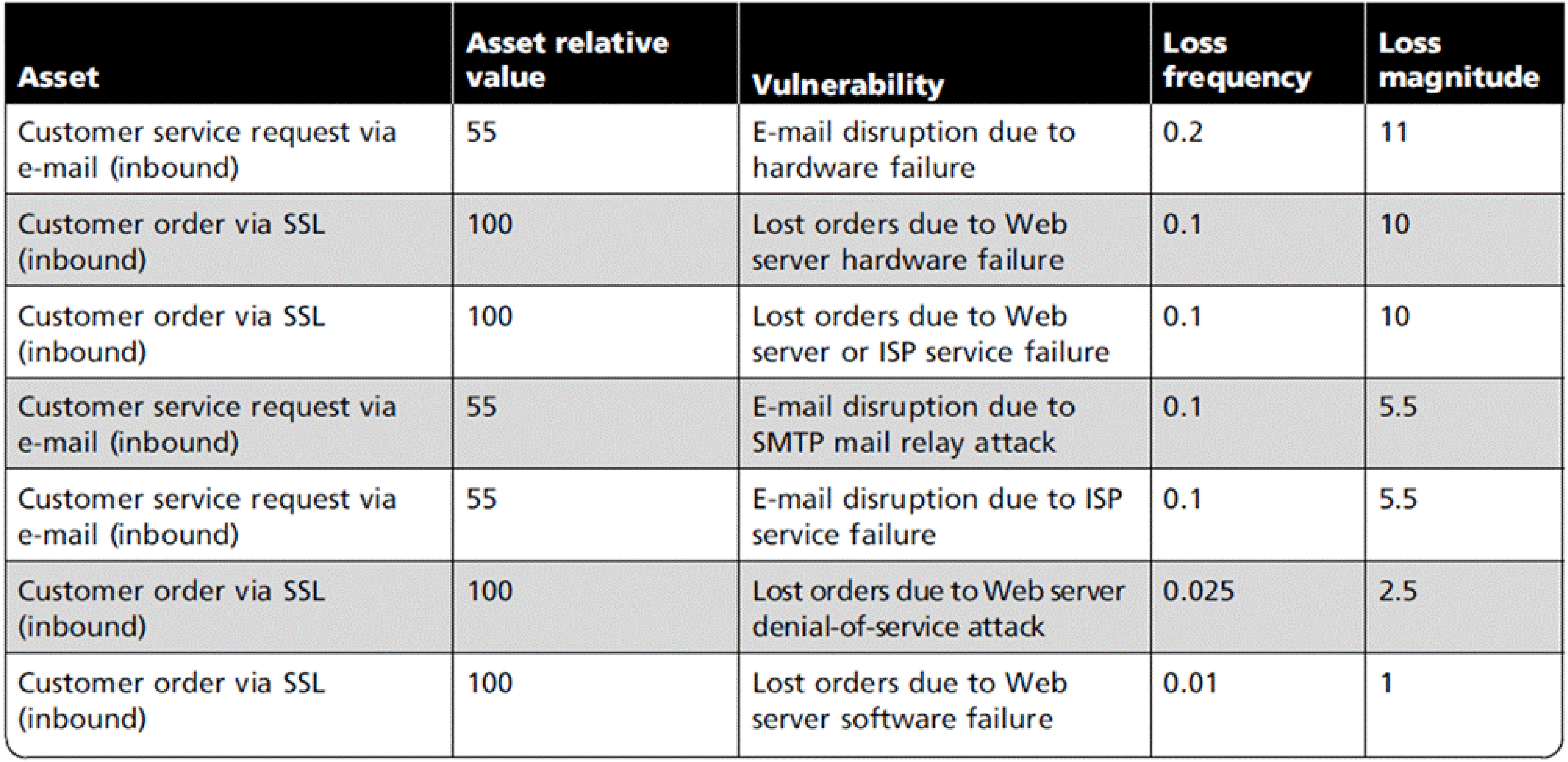
Figure 5-9 Factors of risk

Assessing Risk Acceptability

- For each threat and associated vulnerabilities that have residual risk, create ranking of relative risk levels.
- Residual risk is the left-over risk after the organization has done everything feasible to protect its assets.
- If risk appetite is less than the residual risk, it must look for additional strategies to further reduce the risk.
  - If risk appetite is greater than the residual risk, it must proceed to the latter stages of risk control.

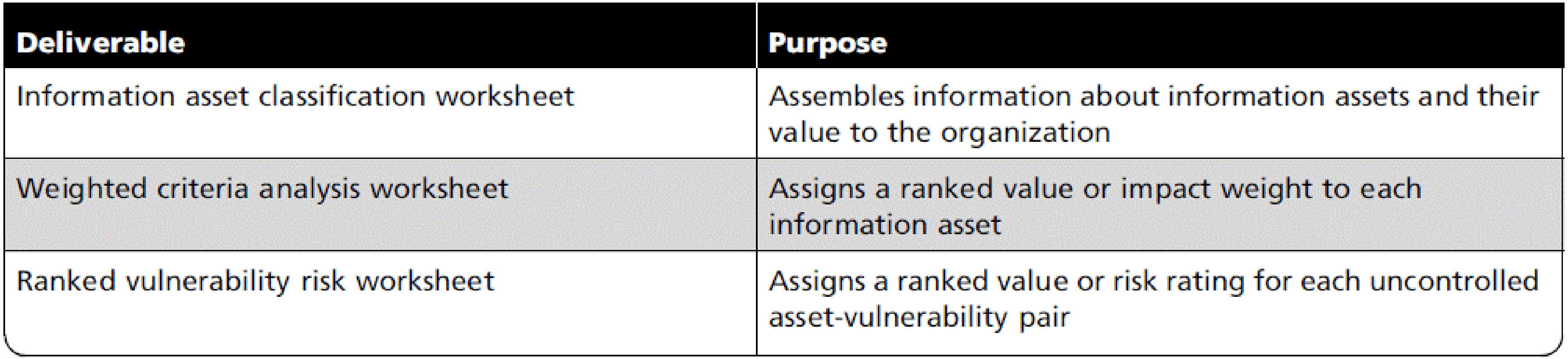
Documenting the Results of Risk Assessment

- The final summarized document is the ranked vulnerability risk worksheet.
- Worksheet describes asset, asset relative value, vulnerability, loss frequency, and loss magnitude.
- Ranked vulnerability risk worksheet is the initial working document for the next step in the risk management process: assessing and controlling risk.



Asset	Asset relative value	Vulnerability	Loss frequency	Loss magnitude
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 5-9 Ranked Vulnerability Risk Worksheet



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

Table 5-10 **Risk Identification and Assessment Deliverables**

The FAIR Approach to Risk Assessment

- Identify scenario components
- Evaluate loss event frequency
- Evaluate probable loss magnitude
- Derive and articulate risk

Risk Control

- Involves selection of control strategies, justification of strategies to upper management, and implementation/monitoring/ongoing assessment of adopted controls
- Once the ranked vulnerability risk worksheet is complete, the organization must choose one of five strategies to control each risk:
  - Defense
  - Transfer
  - Mitigation
  - Acceptance
  - Termination

Defense

- 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
  - Education and training
  - Applying technology

Transfer

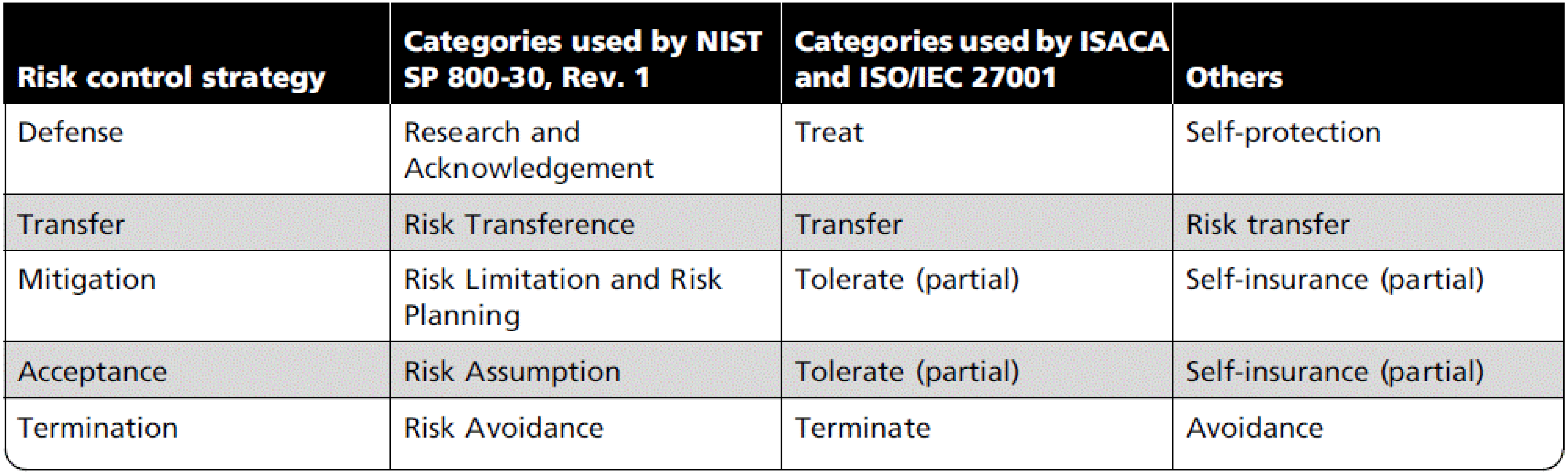
- Attempts to shift risk to other assets, processes, or organizations
- If lacking, the organization should hire individuals/firms that provide security management and administration expertise.
- The organization may then transfer the risk associated with management of complex systems to another organization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

Mitigate

- Attempts to reduce impact of attack rather than reduce success of attack itself
- Approach includes three types of plans:
  - Incident response (IR) plan: define the actions to take while incident is in progress
  - Disaster recovery (DR) plan: the most common mitigation procedure; preparations for the recovery process
  - Business continuity (BC) plan: encompasses the continuation of business activities if a catastrophic event occurs

Acceptance and Termination

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



Risk control strategy	Categories used by NIST SP 800-30, Rev. 1	Categories used by ISACA and ISO/IEC 27001	Others
Defense	Research and Acknowledgement	Treat	Self-protection
Transfer	Risk Transference	Transfer	Risk transfer
Mitigation	Risk Limitation and Risk Planning	Tolerate (partial)	Self-insurance (partial)
Acceptance	Risk Assumption	Tolerate (partial)	Self-insurance (partial)
Termination	Risk Avoidance	Terminate	Avoidance

Table 5-17 **Summary of Risk Control Strategies**

Selecting a Risk Control Strategy

- Level of threat and value of asset should play a major role in the 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 the potential gain
  - When potential loss is substantial

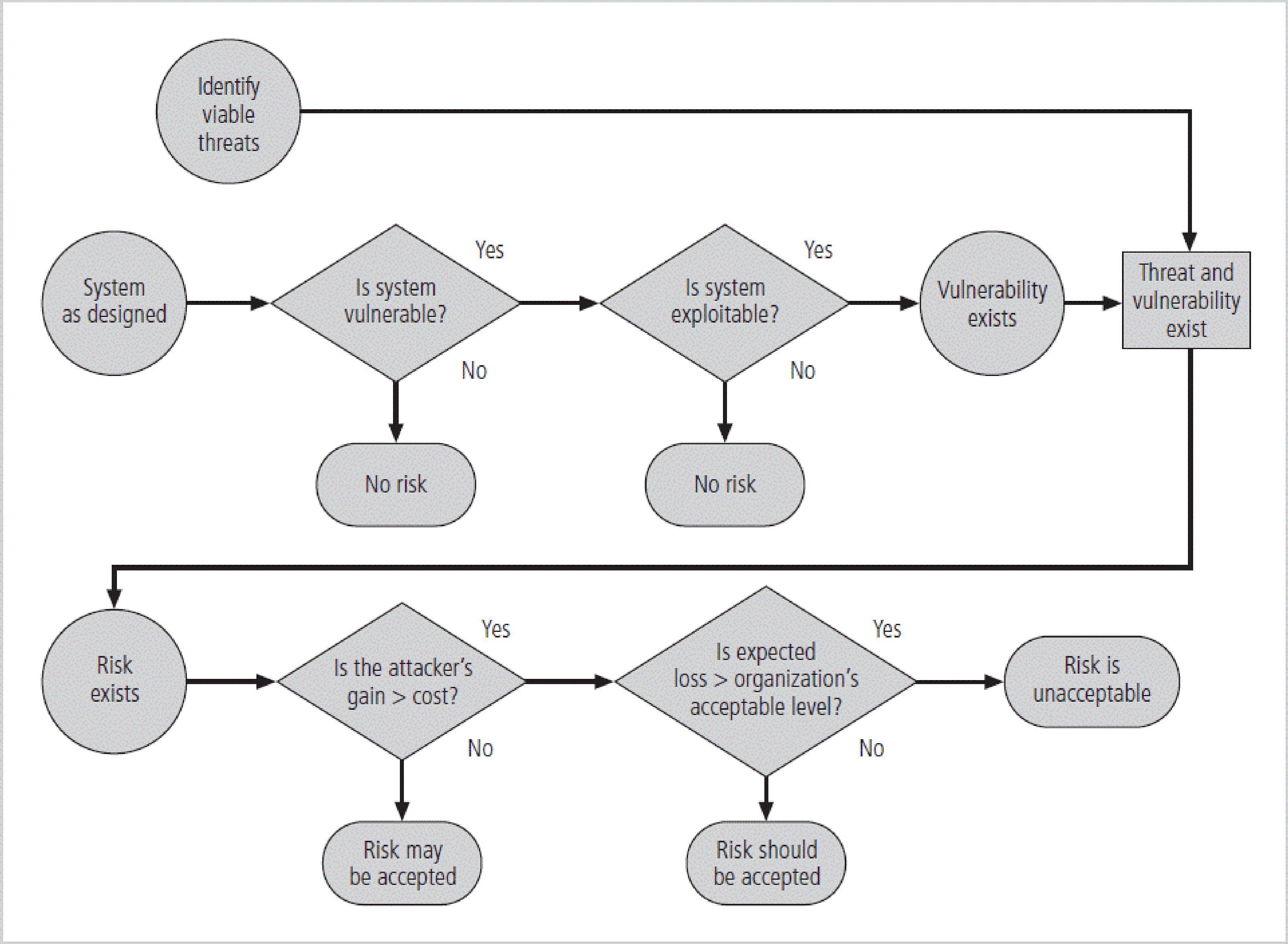


Figure 5-10 Risk handling decision points

Justifying Controls

- Before implementing one of the control strategies for a specific vulnerability, the organization must explore all consequences of vulnerability to information asset.
- Several ways to determine the advantages/disadvantages of a specific control
- Items that affect cost of a control or safeguard include cost of development or acquisition, training fees, implementation cost, service costs, and cost of maintenance.

Justifying Controls (cont'd)

- Asset valuation involves estimating real/perceived costs associated with design, development, installation, maintenance, protection, recovery, and defense against loss/litigation.
- Process result is the 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 an alternative being evaluated is worth the cost incurred to control vulnerability.
  - The CBA is most easily calculated using the ALE from earlier assessments, before implementation of the proposed control:
    - CBA = ALE(prior) – ALE(post) – ACS
  - ALE(prior) is the annualized loss expectancy of risk before implementation of control.
  - ALE(post) is the estimated ALE based on control being in place for a period of time.
  - ACS is the annualized cost of the safeguard.

Implementation, Monitoring, and Assessment of Risk Controls

- The selection of the control strategy is not the end of a process.
- Strategy and accompanying controls must be implemented and monitored on ongoing basis to determine effectiveness and accurately calculate the estimated residual risk.
- Process continues as long as the organization continues to function.

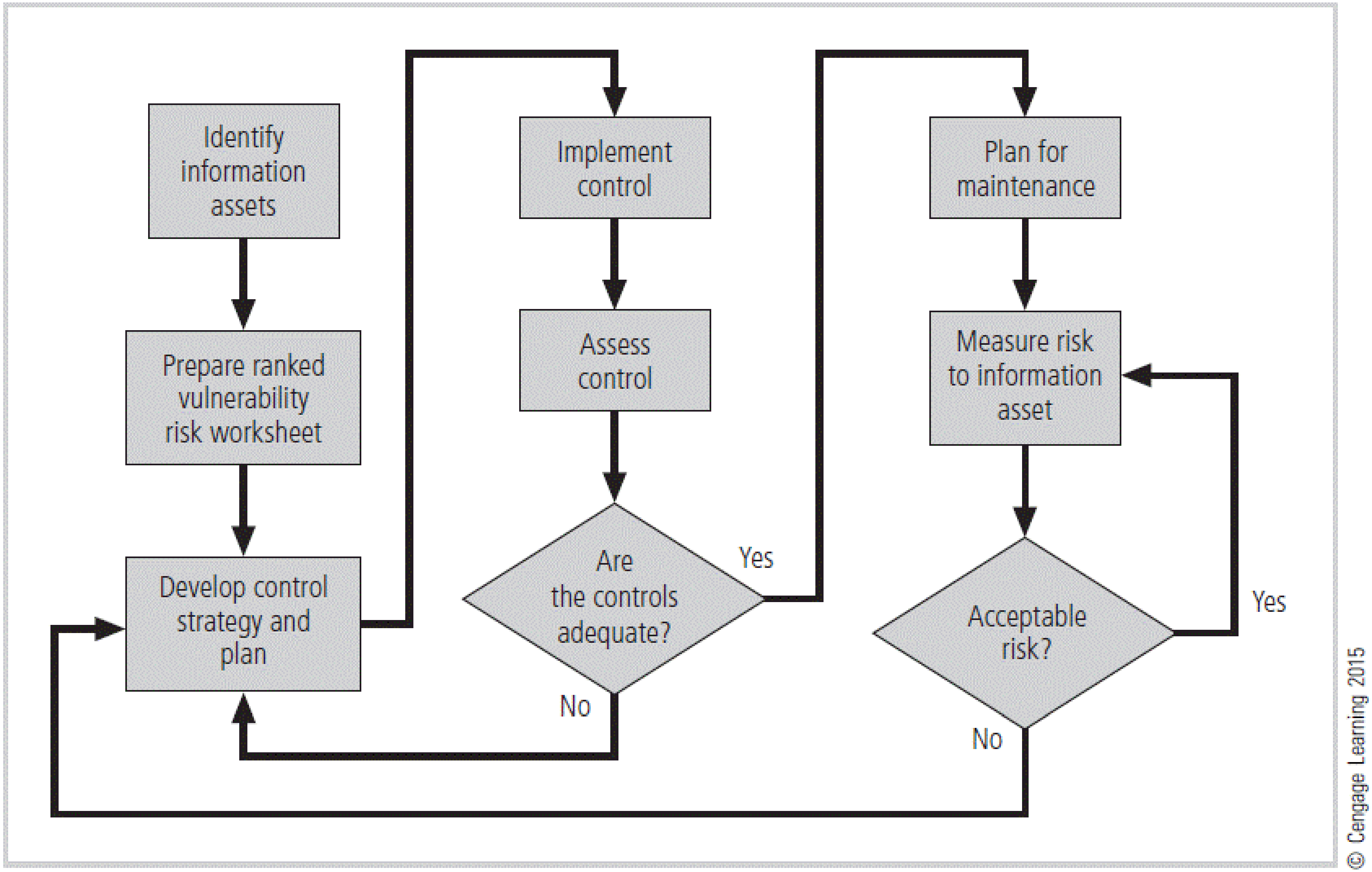

Identify information assets
Prepare ranked vulnerability risk worksheet
Develop control strategy and plan
Implement control
Assess control
Are the controls adequate?
Yes
No
Plan for maintenance
Measure risk to information asset
Acceptable risk?
Yes
No

Figure 5-11 Risk control cycle

Quantitative Versus Qualitative Risk Control Practices

- Performing the previous steps using actual values or estimates is known as quantitative assessment.
- Possible to complete steps using an evaluation process based on characteristics using nonnumerical measures, called qualitative assessment
- Utilizing scales rather than specific estimates relieves the organization from the difficulty of determining exact values.

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, based on numerical standards
  - Process-based measures, more strategic and less focused on numbers

Benchmarking and Best Practices (cont'd)

- Standard of due care: when adopting levels of security for a legal defense, the organization shows it has done what any prudent organization would do in similar circumstances.
- The application of controls at or above prescribed levels and the maintenance of standards of due care show due diligence on the organization's part.
- Failure to support standard of due care or due diligence can leave the organization open to legal liability.

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 identified target organization with best practice?
    - Are expendable resources 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.
  - Researching information security benchmarks doesn’t necessarily prepare a practitioner for what to do next.

Benchmarking and Best Practices (cont’d)

- Baselining
  - Performance value or metric used to compare changes in the object being measured.
  - In information security, baselining is the comparison of past security activities and events against an organization’s future performance.
  - Useful during baselining to have a guide to the overall process

Other Feasibility Studies

- Organizational: Assesses how well the proposed IS alternatives will contribute to an organization’s efficiency, effectiveness, and overall operation
- Operational: Assesses user and management acceptance and support, and the overall requirements of the organization’s stakeholders
- Technical: Assesses if organization has or can acquire the technology necessary to implement and support proposed control
- Political: Defines what can/cannot occur based on the consensus and relationships among communities of interest

Recommended Risk Control Practices

- Convince budget authorities to spend up to value of asset to protect from identified threat.
- Chosen controls may be a balanced mixture that provides 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.

Documenting Results

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

The NIST Risk Management Framework

- Describes risk management as a comprehensive process requiring organizations to:
  - Frame risk
  - Assess risk
  - Respond to determined risk
  - Monitor risk on ongoing basis

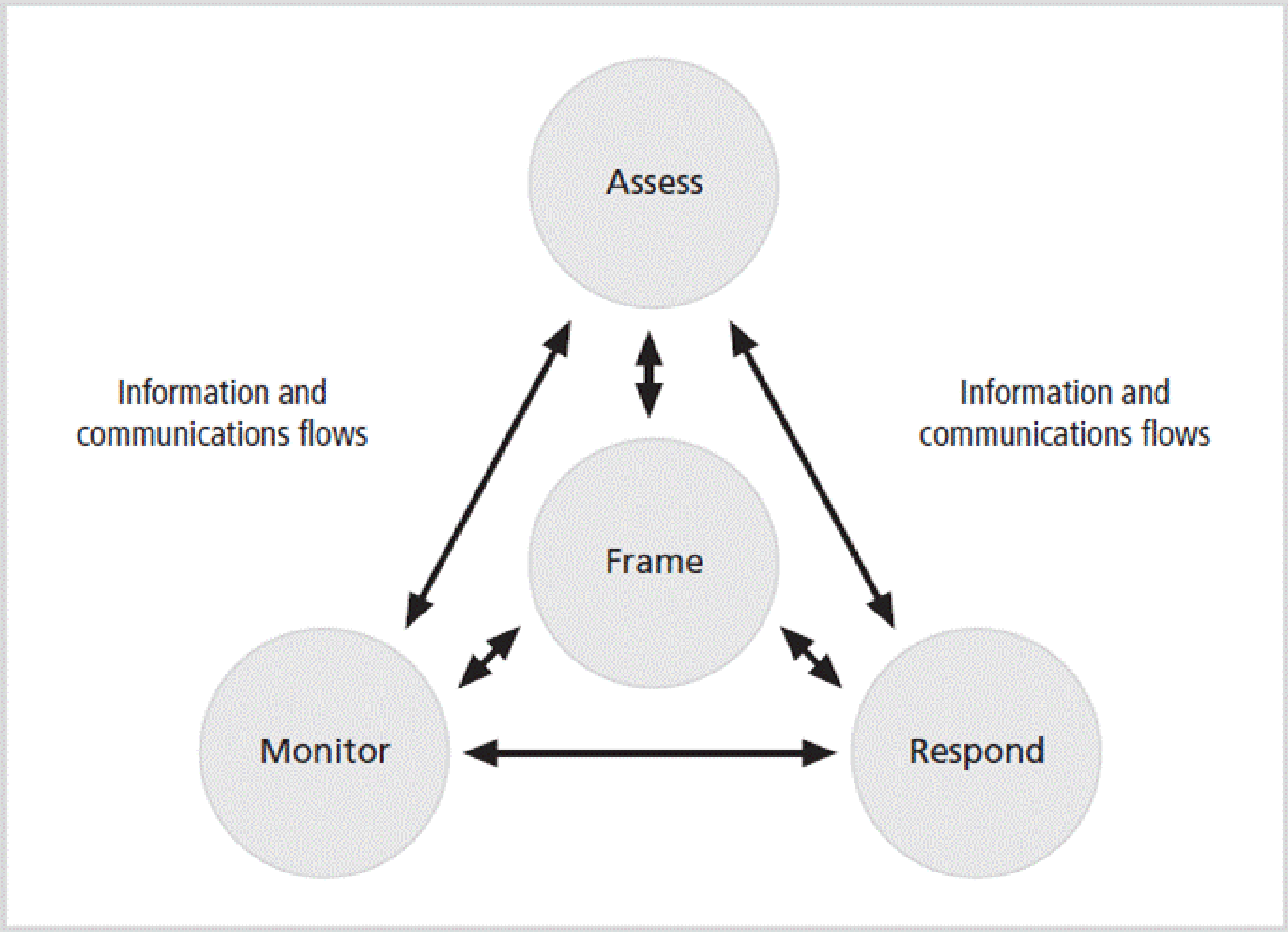

Assess
Information and communications flows
Information and communications flows
Frame
Monitor
Respond

Figure 5-12 NIST risk management process

Source: NIST.[30]

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 the 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 (cont’d)

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