CHAPTER 5

Risk Management

Principles of Information Security

Whitman & Mattord — 6th Edition

Topic	Edition	Chapter
Risk Management	6th (2018)	5 of 12

LEARNING OBJECTIVES

- Understand the importance of risk management in information security
- Learn the risk identification process and how to identify assets, threats, and vulnerabilities
- Apply risk assessment techniques including likelihood and impact analysis
- Understand quantitative and qualitative risk assessment methodologies
- Explore risk control strategies: avoidance, transference, mitigation, and acceptance
- Understand the risk management framework and continuous risk management cycle
- Apply cost-benefit analysis to information security decisions
- Understand the roles and responsibilities in managing organizational risk

5.1 Introduction to Risk Management

Why managing risk is the foundation of InfoSec

Risk management is one of the most critical disciplines in information security. Organizations face countless threats to their information assets, and it is impossible—and inadvisable—to protect against every conceivable threat with equal resources. Risk management provides a systematic framework for identifying, assessing, and controlling risks so that resources are directed where they provide the greatest protection.

Risk	The probability that something unwanted will happen to an information asset, combined with the anticipated impact of that event. Risk = Likelihood × Impact.
Risk Management	The process of identifying, assessing, and controlling threats to an organization's assets, including capital, earnings, and human resources. In InfoSec, this includes digital assets and information.
Risk Appetite	The level of risk an organization is willing to accept in pursuit of its objectives. Often set by senior management and the board of directors.
Residual Risk	The risk remaining after risk controls have been applied. No control eliminates risk completely; some residual risk always remains.

KEY Risk management is NOT about eliminating all risk — it is about making informed decisions about which risks to accept, mitigate, transfer, or avoid based on organizational priorities and available resources.

5.1.1 Risk Management vs. Risk Assessment

Students often confuse risk management and risk assessment. Risk assessment is a component of risk management:

Term	Scope	Output
Risk Assessment	Identify and evaluate risks at a point in time	Risk register, prioritized risk list
Risk Management	Ongoing process encompassing identification, assessment, control, and review	Risk management plan, continuous controls
Risk Analysis	Quantitative or qualitative examination of risk likelihood and impact	Risk ratings, ALE calculations

5.1.2 The Risk Management Process Overview

Whitman & Mattord describe risk management as a four-step iterative process:

- Step 1 — Risk Identification: Identify assets, threats, and vulnerabilities

- Step 2 — Risk Assessment: Evaluate the likelihood and impact of each threat
- Step 3 — Risk Control: Select and implement controls to address risk
- Step 4 — Risk Review: Monitor and reassess risk posture continuously

EXAM TIP The four-step risk management process is a frequent exam topic. Memorize: Identify → Assess → Control → Review (IACR).

5.2 Risk Identification

Cataloguing assets, threats, and vulnerabilities

Risk identification is the process of examining and documenting the security posture of an organization's assets, including information, systems, and supporting infrastructure. The goal is to build a comprehensive inventory of what needs protection and what could threaten it.

5.2.1 Asset Identification

Before risks can be assessed, organizations must understand what they are protecting. Assets are anything of value to the organization. Information security focuses on information assets, but physical and human assets also matter.

Asset	Any item, resource, or capability that has value to an organization and must be protected. Assets include information, hardware, software, personnel, and physical facilities.

Asset categories in information security:

- **Information assets:** data, databases, documentation, operational procedures, research data, customer records
- **Software assets:** application software, system software, development tools, utilities
- **Physical assets:** computer equipment, networking equipment, servers, storage media
- **Service assets:** IT services, communications infrastructure, utilities
- **Personnel:** staff competencies, qualifications, skills (human resources)
- **Intangible assets:** reputation, brand, goodwill, intellectual property

NOTE The textbook emphasizes that asset valuation should consider both the cost to replace/recreate the asset AND the cost of unauthorized disclosure, modification, or unavailability. Both tangible and intangible values matter.

5.2.2 Asset Valuation

Assigning value to assets is essential for cost-benefit analysis of controls. Asset value has several dimensions:

Valuation Factor	Description	Example
Cost to create/acquire	Original cost of creating or purchasing the asset	Software license: $50,000
Cost to replace	Cost to recreate or replace if destroyed or lost	Database rebuild: $200,000
Cost to protect	Annual expenditure required to maintain asset security	Firewall maintenance: $10,000/yr
Value to competitors	Competitive advantage the asset provides; what a competitor would pay	Trade secret: $500,000+
Value if compromised	Loss if asset is disclosed, modified, or unavailable	Customer PII breach: $2M fine
Liability if compromised	Legal, regulatory, and reputational liability	HIPAA violation: $50K–$1.9M per violation

5.2.3 Threat Identification

Threat	Any event or action that has the potential to cause harm to an information asset. Threats exploit vulnerabilities to cause harm.

Threats can be categorized as intentional or unintentional, and by their origin:

Threat Category	Type	Examples
Acts of Human Error/Failure	Unintentional	Employee mistakes, accidents, omissions
Compromises to Intellectual Property	Intentional	Software piracy, copyright infringement
Deliberate Acts of Espionage/Trespass	Intentional	Unauthorized data access, competitive intelligence gathering
Deliberate Acts of Information Extortion	Intentional	Ransomware, blackmail, data hostage scenarios
Deliberate Acts of Sabotage/Vandalism	Intentional	Website defacement, data destruction, DoS
Deliberate Acts of Theft	Intentional	Theft of equipment, data, intellectual property
Deliberate Software Attacks	Intentional	Malware, viruses, worms, ransomware, Trojans
Forces of Nature	Unintentional	Fire, flood, earthquake, storm
Deviations in Quality of Service	Either	ISP failures, power outages, utility disruptions
Technical Hardware Failures	Unintentional	Equipment malfunction, MTTR exceeded
Technical Software Failures	Unintentional	Software bugs, zero-day vulnerabilities
Technological Obsolescence	Unintentional	Outdated hardware/software, unsupported systems

EXAM TIP

The 12-category threat framework from Chapter 2 reappears here in the risk management context. Be prepared to classify threats by category and identify whether they are intentional or unintentional.

5.2.4 Vulnerability Identification

Vulnerability	A weakness or gap in protection efforts that can be exploited by a threat to gain unauthorized access to an asset or to cause harm to it.

Vulnerabilities can exist in systems, processes, or people. Common vulnerability categories include:

- Technical vulnerabilities: unpatched software, misconfigured systems, weak encryption, open ports
- Physical vulnerabilities: unlocked server rooms, poor badge access controls, lack of environmental controls
- Administrative vulnerabilities: inadequate policies, poor training, weak hiring practices, no separation of duties
- Human vulnerabilities: susceptibility to social engineering, lack of security awareness, poor password practices

Vulnerability Assessment	A systematic examination of an information system to identify security weaknesses. Often conducted using automated scanning tools alongside manual review.

IMPORTANT

A threat alone does not constitute risk. Risk requires BOTH a threat AND a corresponding vulnerability. If there is no vulnerability, the threat cannot be realized. This threat-vulnerability pairing is central to risk identification.

5.3 Risk Assessment

Evaluating likelihood and impact to prioritize risk

Once threats and vulnerabilities are identified, the next step is risk assessment — evaluating the likelihood that a threat will exploit a vulnerability and the impact that would result. Risk assessment enables organizations to prioritize risks and allocate security resources effectively.

5.3.1 Quantitative Risk Assessment

Quantitative risk assessment uses numeric values to express risk. It provides concrete dollar amounts for expected losses, which are useful for cost-benefit analysis of controls. The core metrics are:

ASSET VALUE (AV)

`AV = Fair Market Value of the Asset`

The value of the asset in dollars. Used as the baseline for loss calculations.

EXPOSURE FACTOR (EF)

`EF = Percentage of Asset Value Lost to a Threat`

A percentage (0%–100%) representing the proportion of asset value that would be lost if a specific threat were realized. EF = 1.0 means 100% loss.

SINGLE LOSS EXPECTANCY (SLE)

`SLE = AV × EF`

The expected loss in dollars for a single occurrence of a specific threat. SLE = Asset Value multiplied by Exposure Factor.

ANNUALIZED RATE OF OCCURRENCE (ARO)

`ARO = Estimated Frequency of Threat per Year`

How many times per year the threat is expected to occur. ARO = 0.1 means once every 10 years. ARO = 2 means twice per year.

ANNUALIZED LOSS EXPECTANCY (ALE)

`ALE = SLE × ARO`

The expected annual loss in dollars from a specific threat. This is the KEY metric used in cost-benefit analysis. ALE = SLE × ARO = AV × EF × ARO.

WORKED EXAMPLE

Asset: Customer database — AV = $500,000
Threat: SQL injection attack resulting in data breach
Exposure Factor (EF) = 0.40 (40% of data compromised on average)
SLE = AV × EF = $500,000 × 0.40 = $200,000
ARO = 0.25 (estimated once every 4 years)
ALE = SLE × ARO = $200,000 × 0.25 = $50,000 per year
A control costing less than $50,000/year is cost-effective.

5.3.2 Advantages and Disadvantages of Quantitative Assessment

Aspect	Advantages	Disadvantages
Precision	Provides concrete dollar values	Requires accurate estimates (often unavailable)
Communication	Easy to present to executives and boards	May create false sense of precision
Comparison	Enables direct cost-benefit analysis	Difficult to quantify intangible assets
Prioritization	Clear prioritization by ALE value	Time-consuming and resource-intensive
Validity	Objective and repeatable methodology	Historical data may not predict future events

5.3.3 Qualitative Risk Assessment

Qualitative risk assessment uses non-numeric scales (e.g., High/Medium/Low) to evaluate likelihood and impact. It is faster and easier to apply than quantitative assessment, particularly when reliable data for quantitative analysis is unavailable.

The most common approach uses a risk matrix (likelihood vs. impact matrix):

Likelihood \ Impact	Low Impact	Medium Impact	High Impact
High Likelihood	Medium Risk	High Risk	Critical Risk
Medium Likelihood	Low Risk	Medium Risk	High Risk
Low Likelihood	Very Low Risk	Low Risk	Medium Risk

Qualitative assessment typically involves subject matter experts (SMEs) assigning ratings through workshops or surveys. The Delphi method — using multiple rounds of anonymous expert input to reach consensus — is commonly used.

Delphi Method	A qualitative risk assessment technique in which a panel of experts anonymously submits opinions about risk likelihood and impact, then reviews aggregated responses iteratively until consensus is reached.

Aspect	Qualitative Assessment	Quantitative Assessment
Data Requirements	Low — uses expert judgment	High — requires historical data and statistics
Time to Complete	Faster	Slower
Precision	Relative (H/M/L)	Specific (dollar values)
Subjectivity	Higher — relies on expert opinion	Lower — based on measurable data
Cost-Benefit Analysis	Difficult to perform directly	Directly supported by ALE calculations
Best Used When	Limited data, early risk analysis	Mature data, financial justification needed

EX The exam may ask you to compare qualitative and quantitative methods or to calculate ALE. Practice the formula: ALE = AV × EF × ARO. Also know that both methods are valid and organizations often use both in combination.

AMTIP

5.3.4 Risk Register

Risk Register	A documented log of identified risks, including each risk's description, likelihood, impact, risk rating, assigned owner, and planned treatment strategy. The risk register is a living document updated throughout the risk management process.

A typical risk register entry includes:

- Risk ID — unique identifier for tracking
- Risk Description — clear statement of the risk event and its cause
- Affected Assets — which information assets are at risk
- Threat Category — classification from the threat taxonomy
- Likelihood — probability of occurrence (quantitative or qualitative)
- Impact — consequence severity if the risk is realized
- Risk Rating — combined score used for prioritization
- Risk Owner — individual responsible for managing the risk
- Control Strategy — avoidance, transference, mitigation, or acceptance
- Status — open, in progress, or closed

5.4 Risk Control Strategies

Responding to identified and assessed risks

Once risks are assessed and prioritized, management must decide how to respond to each risk. Whitman & Mattord describe four fundamental risk control strategies. The selection of strategy depends on the risk level, cost of controls, and organizational risk appetite.

5.4.1 Risk Avoidance

Risk Avoidance	A risk control strategy that eliminates the risk by eliminating the activity or technology that creates the risk. The organization chooses not to engage in the risky activity.

Risk avoidance is appropriate when the risk is too high to accept and no cost-effective control is available, or when the activity is not essential to the organization's mission.

- Example: An organization avoids storing Social Security numbers by using tokenization, eliminating the risk of SSN data breach.
- Example: A company decides not to deploy a new web application module because the security review identified unacceptable risks that cannot be mitigated in the release timeline.

NOTE

Avoidance is not always feasible — an organization cannot avoid all risks without ceasing operations. It is most appropriate for high-risk activities with limited business value.

5.4.2 Risk Transference (Transfer)

Risk Transference	A risk control strategy that shifts the financial consequences of a risk to another party. The risk is not eliminated but the financial burden is shared or transferred.

Common mechanisms for risk transference include:

- **Cyber liability insurance:** Transfers financial loss from data breaches, cyber attacks, and related incidents to an insurer.
- **Outsourcing:** Transfers operational risk to a managed service provider (but note: legal liability may remain with the original organization).
- **Contracts and SLAs:** Contractual provisions that assign liability for certain failures to vendors or partners.

CRITICAL

Transferring risk does NOT transfer legal liability. An organization that outsources data processing to a third party remains legally liable for the protection of customer data under regulations such as HIPAA, GDPR, and PCI DSS.

5.4.3 Risk Mitigation

Risk Mitigation	A risk control strategy that reduces the likelihood or impact of a threat through the application of security controls. Also called risk reduction. This is the most common risk response strategy.

Risk mitigation involves implementing controls. Controls can be categorized as:

Control Type	Also Called	Purpose	Examples
Preventive	Deterrent	Prevent the threat from occurring	Firewalls, access controls, encryption, security training
Detective	Discovery	Detect threats that occur despite prevention	IDS/IPS, audit logs, security cameras, anomaly detection
Corrective	Recovery	Reduce impact after an incident occurs	Backups, incident response plans, disaster recovery
Compensating	Alternative	Offset a weakness when primary control is infeasible	Manual approval processes, enhanced monitoring

Controls can also be classified by implementation type:

- **Administrative (managerial) controls:** policies, procedures, training, background checks, separation of duties
- **Technical (logical) controls:** firewalls, encryption, access control systems, intrusion detection, authentication
- **Physical controls:** locks, security guards, fences, badge readers, environmental controls

EXAM TIP Controls should be applied in layers (defense in depth). The exam may ask you to classify controls by both function (preventive/detective/corrective) and type (administrative/technical/physical). Both classification dimensions apply simultaneously to each control.

5.4.4 Risk Acceptance

Risk Acceptance	A risk control strategy in which management decides to accept the current level of risk without implementing additional controls. Appropriate when the cost of controls exceeds the expected loss, or when the risk level is within the organization's risk appetite.

Risk acceptance is not the same as ignoring risk. It is a deliberate, documented management decision that must include:

- Formal acknowledgment by appropriate management authority
- Documentation in the risk register with justification
- Periodic review to ensure the accepted risk level remains appropriate
- Identification of residual risk remaining after any partial controls

NOTE Some organizations distinguish between 'active acceptance' (deliberate choice with contingency plans) and 'passive acceptance' (failure to address risk). Only active, documented acceptance is appropriate risk management practice.

5.4.5 Comparing Risk Control Strategies

Strategy	Risk Eliminated?	Cost of Control	Best Used When
Avoidance	Yes	May sacrifice business value	Risk is unacceptably high; activity not essential
Transference	No (financial impact shifted)	Insurance premiums / outsourcing cost	Financial exposure can be insured; liability is primary concern
Mitigation	No (reduced)	Implementation + maintenance of controls	Risk can be reduced to acceptable level cost-effectively
Acceptance	No (unchanged)	None (or minimal)	Cost of control exceeds expected loss; risk within appetite

5.5 Selecting and Implementing Controls

Cost-benefit analysis and control selection

5.5.1 Cost-Benefit Analysis (CBA)

When choosing controls, organizations must determine whether the cost of implementing and maintaining a control is justified by the reduction in expected loss. The Cost-Benefit Analysis (CBA) provides this justification.

COST-BENEFIT ANALYSIS

`CBA = ALE(before control) − ALE(after control) − Annual Cost of Control (ACS)`

If CBA > 0, the control is cost-effective. If CBA < 0, the cost exceeds the benefit and acceptance or an alternative control should be considered.

WORKED EXAMPLE

Current ALE (without control): $50,000/year
ALE with proposed firewall upgrade: $10,000/year
Annual Cost of the firewall upgrade (ACS): $8,000/year
CBA = $50,000 − $10,000 − $8,000 = $32,000
Since CBA > 0 ($32,000 net benefit), the firewall upgrade is cost-effective.

Additional considerations beyond simple CBA:

- **Regulatory compliance:** some controls are legally required regardless of CBA (HIPAA, PCI DSS, SOX)
- **Reputational value:** quantitative CBA may undervalue the brand protection a control provides
- **Total cost of ownership:** include acquisition, implementation, training, maintenance, and operational costs
- **Opportunity cost:** resources spent on one control are unavailable for others

5.5.2 Control Implementation Considerations

When selecting controls, security managers must consider multiple factors:

Factor	Consideration
Effectiveness	Does the control actually reduce the likelihood or impact of the threat?
Efficiency	Does the control operate without creating excessive administrative burden or performance degradation?
Compatibility	Does the control integrate with existing systems, processes, and other controls?

Factor	Consideration
User Impact	Does the control impair users' ability to perform their legitimate work functions?
Auditability	Can the control's effectiveness be monitored and verified through logs and testing?
Maintainability	Can the control be updated, patched, and managed over its lifecycle?

5.5.3 Defense in Depth

Defense in Depth	A layered security strategy in which multiple security controls are deployed so that if one control fails, others continue to provide protection. Also called layered security or the 'onion model' of security.

Defense in depth layers typically include:

- Physical security layer: access controls, security cameras, environmental protection
- Network security layer: firewalls, IDS/IPS, network segmentation, VPNs
- Host security layer: OS hardening, endpoint protection, patch management
- Application security layer: secure coding practices, WAFs, input validation
- Data security layer: encryption at rest and in transit, DLP, access controls on data
- User security layer: identity management, MFA, security awareness training

KEY CONCEPT

Defense in depth accepts that no single control is perfect. By overlapping multiple controls at different layers, organizations ensure that an attacker who defeats one control still faces others. This is the opposite of 'security through obscurity.'

5.6 Risk Management Frameworks

Industry standards and regulatory frameworks

Organizations do not perform risk management in isolation. Numerous frameworks, standards, and methodologies provide structured guidance. Whitman & Mattord reference several key frameworks:

5.6.1 NIST Risk Management Framework (RMF)

The NIST Risk Management Framework (SP 800-37) provides a structured, flexible approach for integrating risk management into the system development life cycle (SDLC). It consists of six steps:

Step	Activity	Key Output
1. Categorize	Classify information system and data by impact level (FIPS 199)	System security category
2. Select	Select baseline security controls (NIST SP 800-53)	Security control baseline
3. Implement	Deploy selected security controls	Implemented controls
4. Assess	Evaluate control effectiveness	Security assessment report
5. Authorize	Senior official accepts risk and authorizes system operation	Authorization to Operate (ATO)
6. Monitor	Continuously monitor controls and report security status	Ongoing risk posture

5.6.2 ISO/IEC 27005 — Information Security Risk Management

ISO/IEC 27005 provides guidelines for information security risk management aligned with ISO/IEC 27001 (the ISMS standard). It follows an iterative process:

- Context establishment: define scope, objectives, and risk criteria
- Risk assessment: identify, analyze, and evaluate risks
- Risk treatment: select and implement risk controls
- Risk acceptance: document management's acceptance of residual risk
- Risk communication: share risk information with stakeholders
- Risk monitoring and review: track changes in risk environment

5.6.3 FAIR — Factor Analysis of Information Risk

FAIR (Factor Analysis of Information Risk)	A quantitative risk analysis model that defines risk in terms of probable frequency and probable magnitude of future loss. FAIR provides a structured ontology for understanding, analyzing, and measuring information risk.

FAIR's key distinction: it separates risk (probable frequency × probable magnitude) from controls, enabling precise calculation of risk reduction from specific security investments.

5.6.4 OCTAVE — Operationally Critical Threat, Asset, and Vulnerability Evaluation

OCTAVE	A risk assessment framework developed at Carnegie Mellon's CERT Coordination Center. OCTAVE focuses on organizational risk from an operational perspective, emphasizing people and processes over technology. Variants: OCTAVE, OCTAVE-S (small organizations), OCTAVE Allegro.

Framework	Origin	Approach	Best For
NIST RMF	NIST (US Gov)	Prescriptive, process-based	US federal agencies; regulated industries
ISO 27005	ISO/IEC	Principle-based, flexible	Organizations with ISO 27001 ISMS
FAIR	Open Group	Quantitative financial model	Financial justification of security investments
OCTAVE	Carnegie Mellon CERT	People/process focused, qualitative	Organizations prioritizing operational risk

5.7 Risk Management in Practice

Roles, responsibilities, and continuous improvement

5.7.1 Roles and Responsibilities

Effective risk management requires clear ownership and accountability across the organization:

Role	Risk Management Responsibilities
Board of Directors / Senior Executives	Set risk appetite; ultimate accountability; approve risk management policy
Chief Information Security Officer (CISO)	Lead risk management program; report risk posture to board; oversee risk treatment
Chief Risk Officer (CRO)	Enterprise-wide risk governance; integration of InfoSec risk with operational/financial risk
Information Security Manager	Conduct risk assessments; implement risk treatments; maintain risk register
System/Data Owners	Accept residual risk for their systems; ensure controls are implemented
IT Staff / Security Analysts	Implement technical controls; monitor for threats; report security events
End Users	Follow security policies; report suspicious activity; complete security training
Internal Audit	Independently assess effectiveness of risk controls; verify compliance

5.7.2 Continuous Risk Monitoring

Risk management is not a one-time activity. The risk environment changes continuously as new threats emerge, vulnerabilities are discovered, and organizational assets and operations evolve. Continuous monitoring includes:

- Regular vulnerability scanning and penetration testing
- Monitoring threat intelligence feeds for emerging threats
- Reviewing security logs and SIEM alerts for indicators of compromise
- Tracking security metrics and Key Risk Indicators (KRIs)
- Annual or event-driven updates to the risk register and risk assessments

- Reviewing effectiveness of implemented controls through audits and testing

Key Risk Indicator (KRI)	A metric used to signal increasing risk exposure. KRIs provide early warning that risk levels are approaching or exceeding acceptable thresholds. Examples: number of unpatched critical vulnerabilities, mean time to detect (MTTD) security events.

5.7.3 The Risk Management Cycle

Risk management follows a continuous cycle. There is no defined end — each cycle feeds into the next:

Phase	Activities	Frequency
Identify	Asset inventory, threat identification, vulnerability scanning	Ongoing; formal review annually
Assess	Likelihood/impact analysis, ALE calculation, risk rating	Annually or after major changes
Control	Select, implement, and test controls; update policies	As risks are identified and prioritized
Review	Audit controls, reassess risks, report to management	Continuously; formal review annually

5.8 Special Topics in Risk Management

Supply chain, cloud, and emerging risk considerations

5.8.1 Supply Chain Risk Management

Supply Chain Risk	Risk arising from the use of third-party products, services, or vendors. A compromise in a supplier's system can propagate to the organization through software, hardware, or services they provide.

Supply chain risk management involves:

- Vendor due diligence: evaluating suppliers' security programs before procurement
- Contractual security requirements: mandating security standards in vendor contracts
- Third-party risk assessments: auditing or assessing vendor security posture
- Software Bill of Materials (SBOM): tracking software components and their origins
- Monitoring vendor security advisories and patch releases

REAL-WOR

Supply chain attacks such as the SolarWinds SUNBURST attack (2020) demonstrated how a single compromised software vendor can provide attackers access to thousands of downstream organizations, including US government agencies. Supply chain risk is now a top priority in risk management.

L
D

5.8.2 Cloud Risk Considerations

Cloud computing introduces unique risk considerations that require modification of traditional risk management approaches:

Cloud Risk Factor	Description	Risk Control Approach
Shared Responsibility	CSP and customer share security responsibilities differently by service model (IaaS/PaaS/SaaS)	Clearly define and document responsibility boundaries in SLA
Data Sovereignty	Data may be stored in multiple jurisdictions with different legal requirements	Contractually specify data residency; understand local law
Multi-tenancy	Resources shared with other customers; risk of side-channel attacks or misconfigurations	Verify CSP isolation controls; use dedicated instances for sensitive data
Vendor Lock-in	Dependency on a single CSP creates concentration risk	Multi-cloud strategy; data portability provisions in contract
Incident Response	Limited visibility into CSP infrastructure during incidents	Negotiate incident notification and response SLAs; test IR plans

5.8.3 Insider Threat Risk

Insider Threat	A security risk that originates from within the organization — employees, contractors, or business partners with authorized access who misuse that access, either maliciously or negligently.

Insider threats are particularly challenging because:

- Insiders already have authorized access, bypassing perimeter defenses
- Actions may be subtle and difficult to distinguish from legitimate work
- Motivations include financial gain, grievance, ideology, or simple negligence
- Detection requires behavioral analytics and user activity monitoring

Risk controls for insider threats:

- **Principle of least privilege:** grant only the minimum access required for job function
- **Separation of duties:** require multiple people to complete sensitive transactions
- **User activity monitoring (UAM):** track and analyze user behavior for anomalies
- **Background checks:** pre-employment screening and periodic re-investigation for sensitive roles
- **Security awareness training:** educate employees on recognizing and reporting suspicious behavior

5.9 Chapter Summary & Exam Review

Key concepts, formulas, and review questions

Core Formulas — Must Memorize

SINGLE LOSS EXPECTANCY

$$SLE = AV \times EF$$

AV = Asset Value; EF = Exposure Factor (0.0–1.0)

ANNUALIZED LOSS EXPECTANCY

$$ALE = SLE \times ARO \quad \text{OR} \quad ALE = AV \times EF \times ARO$$

ARO = Annualized Rate of Occurrence (expected occurrences per year)

COST-BENEFIT ANALYSIS

$$CBA = ALE(before) - ALE(after) - ACS$$

ACS = Annual Cost of the Security control. Positive CBA = cost-effective control.

Key Terms Summary

Risk	Probability × Impact of a harmful event on an information asset
Threat	Potential event that can cause harm to an asset
Vulnerability	Weakness that a threat can exploit
Exposure Factor (EF)	Percentage of asset value lost in a single threat event
SLE	Expected dollar loss from a single occurrence of a threat
ARO	Expected annual frequency of a threat event
ALE	Expected annual dollar loss from a specific threat; ALE = SLE × ARO
Risk Avoidance	Eliminate the risky activity entirely
Risk Transference	Shift financial impact to another party (insurance, outsourcing)

Risk Mitigation	Reduce likelihood/impact through security controls (most common)
Risk Acceptance	Document and accept the risk without additional controls
Residual Risk	Risk remaining after controls are applied
Defense in Depth	Multiple overlapping security layers to ensure no single point of failure
Cost-Benefit Analysis	Determine if control cost is justified by reduction in expected loss
Risk Register	Living document cataloguing all identified risks with status and ownership
Delphi Method	Anonymous expert consensus method for qualitative risk assessment
NIST RMF	Six-step US government risk management framework: Categorize, Select, Implement, Assess, Authorize, Monitor
FAIR	Quantitative risk analysis model: risk = probable frequency × probable magnitude
OCTAVE	Carnegie Mellon people/process focused risk assessment methodology
KRI	Key Risk Indicator — metric signaling increasing risk exposure

Review Questions

#	Question	Answer / Guidance
Q1	A database worth $400,000 has an exposure factor of 0.50 for a malware attack. The attack is expected to occur 0.2 times per year. What is the ALE?	SLE = $400,000 × 0.50 = $200,000. ALE = $200,000 × 0.2 = $40,000/year.
Q2	A proposed antivirus solution costs $5,000/year and reduces the ALE for malware from $40,000 to $12,000. Is the control cost-effective?	CBA = $40,000 − $12,000 − $5,000 = $23,000. Positive CBA → cost-effective.
Q3	What is the difference between risk avoidance and risk acceptance?	Avoidance eliminates the risk by stopping the risky activity. Acceptance is a documented management decision to tolerate the risk without additional controls.

#	Question	Answer / Guidance
Q4	A company outsources its payroll processing to a third party. Has the company transferred its risk and legal liability?	Financial risk is transferred, but legal liability remains with the organization for its customers' data under applicable regulations.
Q5	What are the four steps of the risk management process?	Identify → Assess → Control → Review (IACR). This is a continuous, iterative cycle.
Q6	What distinguishes qualitative from quantitative risk assessment?	Qualitative uses scales (H/M/L) and expert judgment; quantitative uses dollar values and formulas (ALE). Both are valid; quantitative better supports CBA.

FINAL EXAM TIPS

Know the four risk control strategies by name and when each is appropriate.
Memorize SLE = AV × EF and ALE = SLE × ARO — calculation questions are common.
Understand why risk transference does NOT transfer legal liability.
Know that defense in depth is the solution to single points of failure.
Recognize that risk management is continuous — the review step feeds back into identification.
Be able to compare quantitative vs. qualitative assessment methods.
Know the six steps of the NIST RMF: Categorize, Select, Implement, Assess, Authorize, Monitor.