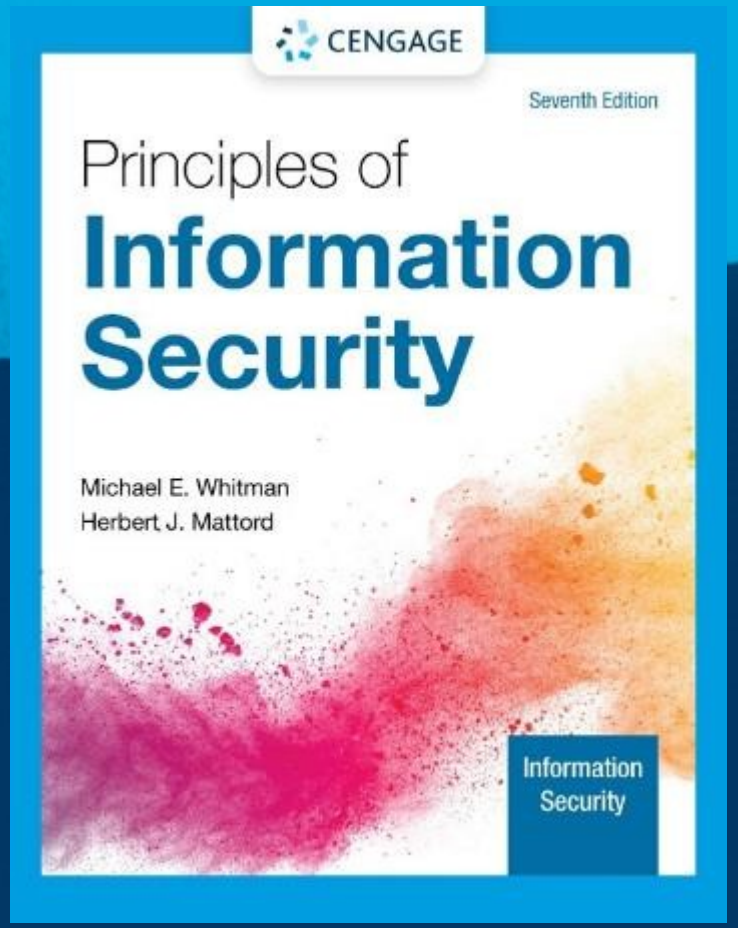

Module 4

Risk Management

Module Objectives

By the end of this module, you should be able to:

4.1 Define risk management and describe its importance

4.2 Explain the risk management framework and process model, including major components

4.3 Define risk appetite and explain how it relates to residual risk

4.4 Describe how risk is identified and documented

4.5 Discuss how risk is assessed based on likelihood and impact

4.6 Describe various options for a risk treatment and risk control strategy

4.7 Discuss conceptual frameworks for evaluating risk controls and formulate a cost-benefit analysis

4.8 Compare and contrast the dominant risk management methodologies

Introduction to Risk Management

- The upper management of an organization is responsible for overseeing, enabling, and supporting the structuring of IT and information security functions to defend its information assets.
- Part of upper management's information security governance requirement is the establishment and support of an effective risk management (RM) program.
- To keep up with the competition, organizations must design and create safe environments in which their business processes and procedures can function.
- These environments must maintain confidentiality and privacy and assure the integrity of an organization's data—objectives that are met by applying the principles of risk management.

Sun Tzu and the Art of Risk Management

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

The Risk Management Framework (1 of 4)

- Risk management involves discovering and understanding answers to some key questions about the risk associated with an organization's information assets:
  1. Where and what is the risk (risk identification)?
  2. How severe is the current level of risk (risk analysis)?
  3. Is the current level of risk acceptable (risk evaluation)?
  4. What do I need to do to bring the risk to an acceptable level (risk treatment)?

The Risk Management Framework (2 of 4)

- **Risk management:** the process of identifying risk, assessing its relative magnitude, and taking steps to reduce it to an acceptable level.
- **Risk identification:** the recognition, enumeration, and documentation of risks to an organization's information assets.
- **Risk assessment:** a determination of the extent to which an organization's information assets are exposed to risk.
- **Risk treatment (risk control):** the application of safeguards or controls that reduce the risks to an organization's information assets to an acceptable level.

Knowledge Check Activity 1

The identification, analysis, and evaluation of risk as initial parts of risk management is known as risk _____.

a. control

b. assessment

c. treatment

d. enforcement

Knowledge Check Activity 1: Answer

The identification, analysis, and evaluation of risk as initial parts of risk management is known as risk _____.

Answer: b. assessment

Risk treatment is the application of safeguards or controls to reduce the risks to an organization's information assets to an acceptable level, and risk control is a synonym for risk treatment. Risk enforcement is not defined in the module.

The Risk Management Framework (3 of 4)

- Risk management (RM) is a complex operation that requires a formal methodology.
- Risk management involves two key areas: the RM framework and the RM process.
- The **RM framework** is the overall structure of the strategic planning and design for the entirety of the organization's RM efforts.
- The **RM process** is the implementation of risk management, as specified in the framework.
- In other words, the RM framework (planning) guides the RM process (doing), which conducts the processes of risk evaluation and remediation.

The Risk Management Framework and Process

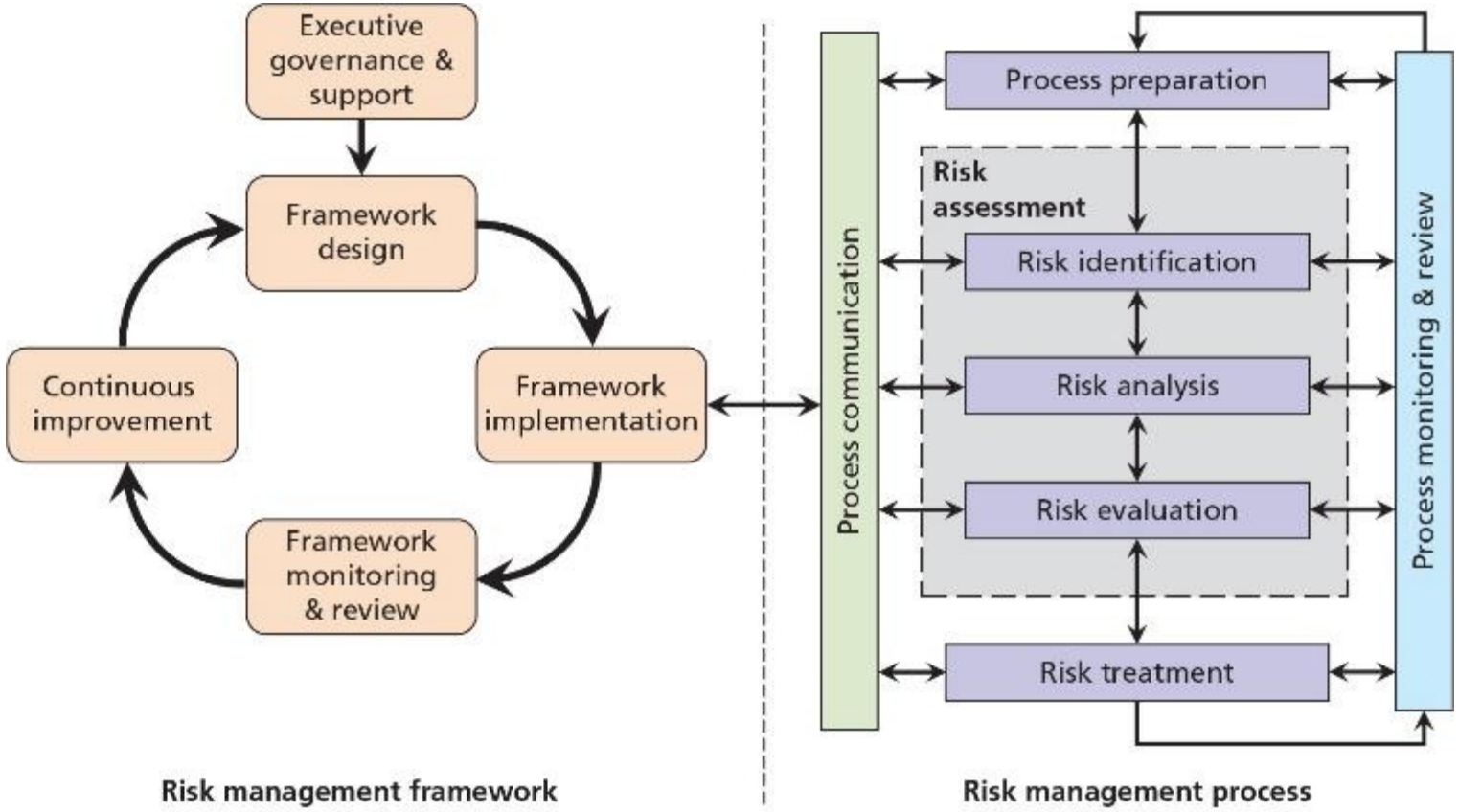

Figure 4-1 The risk management framework and process

The Risk Management Framework (4 of 4)

- The RM framework consists of five key stages:
  1. Executive governance and support
  2. Framework design
  3. Framework implementation
  4. Framework monitoring and review
  5. Continuous improvement

The Roles of the Communities of Interest

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

The Risk Management Policy (1 of 2)

- This policy converts the instructions and perspectives provided to the RM framework team by the governance group into cohesive guidance that structures and directs all subsequent risk management efforts within the organization.
- The **RM policy**, much like the enterprise information security policy (EISP), is a strategic document that formalizes much of the intent of the governance group.

The Risk Management Policy (2 of 2)

- Most RM policies include the following sections:
  - Purpose and scope
  - RM intent and objectives
  - Roles and responsibilities
  - Resource requirements
  - Risk appetite and tolerances
  - RM program development guidelines
  - Special instructions and revision information
  - References to other key policies, plans, standards, and guidelines

Framework Design

- In this stage, the framework team begins designing the RM process by which the organization will understand its current levels of risk and determine what, if anything, it needs to do to bring those levels down to an acceptable level in alignment with the risk appetite specified earlier in the process.
- In addition to coordinating with the governance group on the tasks outlined in the previous section, the framework team must also formally document and define the organization's risk appetite and draft the **risk management (RM) plan**.

Defining the Organization's Risk Tolerance and Risk Appetite

- **Risk appetite:** the quantity and nature of risk that organizations are willing to accept as they evaluate the trade-offs between perfect security and unlimited accessibility.
- **Residual risk:** the risk to information assets that remains even after current controls have been applied.
- **Risk tolerance (risk threshold):** the assessment of the amount of risk an organization is willing to accept for a particular information asset.
- The goal of information security is to bring residual risk in alignment with risk appetite.

Framework Implementation

- The implementation of the RM plan, specifically including the RM process, is likely to be influenced by the organization's risk appetite.
- Implementation methods could include:
  - Desk check
  - Pilot-test
  - Phased approach
  - Direct cutover (cold-turkey conversion)

Framework Monitoring and Review

- After the initial implementation and as the RM effort proceeds, the framework team continues to monitor the conduct of the RM process while simultaneously reviewing the utility and relative success of the framework planning function itself.
- Once the RM process is implemented and operating, the framework team is primarily concerned with the monitoring and review of the overall RM process cycle.

The Risk Management Process

- The RM plan guides the implementation of the RM process, in which risk evaluation and remediation is conducted.
- This process uses the following tasks:
  - Establishing the context
  - Identifying risk
  - Analyzing risk
  - Evaluating the risk and comparing uncontrolled risks against the risk appetite
  - Treating the unacceptable risk
  - Summarizing the findings

RM Process Preparation—Establishing the Context (1 of 2)

- As the RM process team convenes, it is initially briefed by representatives of the framework team and possibly by the governance group.
- These groups seek to provide executive guidance for the work to be performed by the RM process team, and to ensure that the team's efforts are in alignment with managerial intent, as documented in the RM policy.
- The context in this phase is the understanding of the external and internal environments the RM team will be interacting with as it conducts the RM process.

RM Process Preparation—Establishing the Context (2 of 2)

- NIST's Special Publication (SP) 800-30, Rev. 1, "Guide for Conducting Risk Assessments," recommends preparing for the risk process by performing the following tasks:
  - Identify the purpose of the assessment;
  - Identify the scope of the assessment;
  - Identify the assumptions and constraints associated with the assessment;
  - Identify the sources of information to be used as inputs to the assessment; and
  - Identify the risk model and analytic approaches.

Risk Assessment: Risk Identification

- The first operational phase of the RM process is the identification of risk.
- At this stage, managers must:
  1. Identify the organization's information assets
  2. Classify them
  3. Categorize them into useful groups
  4. Prioritize them by overall importance

Organizational Assets Used in Systems (1 of 2)

Information System Components	Risk Management Components	Example Risk Management Components
People	Internal personnel External personnel	Trusted employees Other staff members People we trust outside our organization Strangers
Procedures	Procedures	IT and business standard procedures IT and business-sensitive procedures
Data	Data/information	Transmission Processing Storage

Organizational Assets Used in Systems (2 of 2)

Information System Components	Risk Management Components	Example Risk Management Components
Software	Software	Applications Operating systems Utilities Security components
Hardware	Hardware	Systems and peripherals Security devices Network-attached process control devices and other embedded systems (Internet of Things)
Networking	Networking	Local area network components Intranet components Internet or extranet components Cloud-based components

Assessing the Value of Information Assets

- As each information asset is identified, categorized, and classified, a relative value must be assigned to it to ensure that the most valuable information assets are given the highest priority when managing risk.
- Which information asset:
  - Is most critical to the organization's success?
  - Generates the most revenue?
  - Generates the highest profitability?
  - Is the most expensive to replace?
  - Is the most expensive to protect?
  - Would be the most embarrassing or cause the greatest liability if lost or compromised?

Sample Asset Classification Scheme (1 of 2)

System Name: SLS E-commerce

Date Evaluated: February 2018

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

Sample Asset Classification Scheme (2 of 2)

Information assets	Data classification	Impact to profitability
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

Prioritizing (Rank-Ordering) Information Assets

- The final step in the risk identification process is to prioritize, or rank-order, the assets.
- This goal can be achieved by using a weighted table analysis.
  - List information assets
  - Select criteria
  - Specify criteria weights
  - Assess each asset
  - Calculate weighted averages
  - Rank order by score

Knowledge Check Activity 2

When performing risk identification, which of these steps is performed last?

a. classifying

b. identifying

c. prioritizing

d. categorizing

Knowledge Check Activity 2: Answer

When performing risk identification, which of these steps is performed last?

Answer: c. prioritizing

You cannot assess the relative importance and assign priority until all assets are known, given a value, and classified and placed into categories.

Weighted Table Analysis of Information Assets (1 of 2)

	Criterion →	*Impact on Revenue*	*Impact on Profitability*	*Impact on Reputation*		
#	**Criterion Weight → Information Asset →**	**0.3**	**0.4**	**0.3**	**TOTAL (1.0)**	**Importance (0-5; Not Applicable to Critically Important)**
1	Customer order via SSL (inbound)	*5*	*5*	*5*	5	Critically Important
2	EDI Document Set 1-Logistics bill of lading to outsourcer (outbound)	*5*	*5*	*3*	4.4	Very Important

Weighted Table Analysis of Information Assets (2 of 2)

	Criterion →	*Impact on Revenue*	*Impact on Profitability*	*Impact on Reputation*		
3	EDI Document Set 2-Supplier orders (outbound)	*4*	*5*	*4*	4.4	Very Important
4	Customer service request via e-mail (inbound)	*3*	*3*	*5*	3.6	Very Important

Threat Assessment

- Realistic threats need investigation; unimportant threats are set aside.
- Weighted tables can assist in assessing threats.
- Threat assessment:
  - Which threats present an actual danger to our information assets?
  - Which threats are internal, and which are external?
  - Which threats have the highest probability of occurrence?
  - Which threats have the highest probability of success?
  - Which threats could result in the greatest loss if successful?
  - Which threats can the organization handle least effectively?
  - Which threats cost the most to protect against?
  - Which threats cost the most to recover from?

Threats to Information Security

Threat	Examples
Compromises to intellectual property	Software piracy or other copyright infringement
Deviations in quality of service from service providers	Fluctuations in power, data, and other services
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, flood, earthquake, lightning, etc.
Human error or failure	Accidents, employee mistakes, failure to follow policy
Information extortion	Blackmail threat of information disclosure
Sabotage or vandalism	Damage to or destruction of systems or information
Software attacks	Malware: viruses, worms, macros, denial of services, or script injections
Technical hardware failures or errors	Hardware equipment failure
Technical software failures or errors	Bugs, code problems, loopholes, back doors
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of equipment or information

Vulnerability Assessment

- 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.
- The process works best when people with diverse backgrounds within an organization work iteratively in a series of brainstorming sessions.
- At the end of the risk identification process, a prioritized list of assets with their vulnerabilities is achieved.
  - Can be combined with weighted list of threats to form threats-vulnerabilities-assets (TVA) worksheet

Vulnerability Assessment of a DMZ Router (1 of 2)

Threat	Possible Vulnerabilities
Compromises to intellectual property	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised.
Espionage or trespass	Router has little intrinsic value, but other assets protected by this device could be attacked if it 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	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised.
Quality-of-service deviations from service providers	Unless suitable electrical power conditioning is provided, failure is probable over time.

Vulnerability Assessment of a DMZ Router (2 of 2)

Threat	Possible Vulnerabilities
Sabotage or vandalism	IP is vulnerable to denial-of-service attacks. Device may be subject to defacement or cache poisoning.
Software attacks	IP is vulnerable to denial-of-service attacks. Outsider IP fingerprinting activities can reveal sensitive information unless suitable controls are implemented.
Technical hardware failures or errors	Hardware could fail and cause an outage. Power system failures are always possible.
Technical software failures or errors	Vendor-supplied routing software could fail and cause an outage.
Technological obsolescence	If it is not reviewed and periodically updated, a device may fall too far behind its vendor support model to be kept in service.
Theft	Router has little intrinsic value, but other assets protected by this device could be attacked if it is stolen.

The TVA Worksheet (1 of 2)

	Asset 1	Asset 2	Asset 3	. . .	. . .	. . .	. . .	. . .	. . .	Asset n
Threat 1	T1V1A1 T1V2A1 T1V3A1 . . .	T1V1A2 T1V2A2 . . .	T1V1A3 . . .	T1V1A4 . . .						
Threat 2	T2V1A1 T2V2A1 . . .	T2V1A2 . . .	T2V1A3 . . .							
Threat 3	T3V1A1 . . .	T3V1A2 . . .								
Threat 4	T4V1A1 . . .									

The TVA Worksheet (2 of 2)

	Asset 1	Asset 2	Asset 3	. . .	. . .	. . .	. . .	. . .	. . .	Asset n
Threat 5										
Threat 6										
. . .										
. . .										
Threat n										
Legend: Priority of effort	1	2	3	4	5	6	7	8	. . .	

These bands of controls should be continued through all asset-threat pairs.

Risk Assessment: Risk Analysis

- Risk analysis assesses the relative risk for each vulnerability and assigns a risk rating or score to each information asset.
- The goal is to develop a repeatable method to evaluate the relative risk of each vulnerability that has been identified and added to the list.
- If a vulnerability is fully managed by an existing control, it can be set aside.
- If it is partially controlled, you can estimate what percentage of the vulnerability has been controlled.

NIST Generic Risk Model with Key Risk Factors

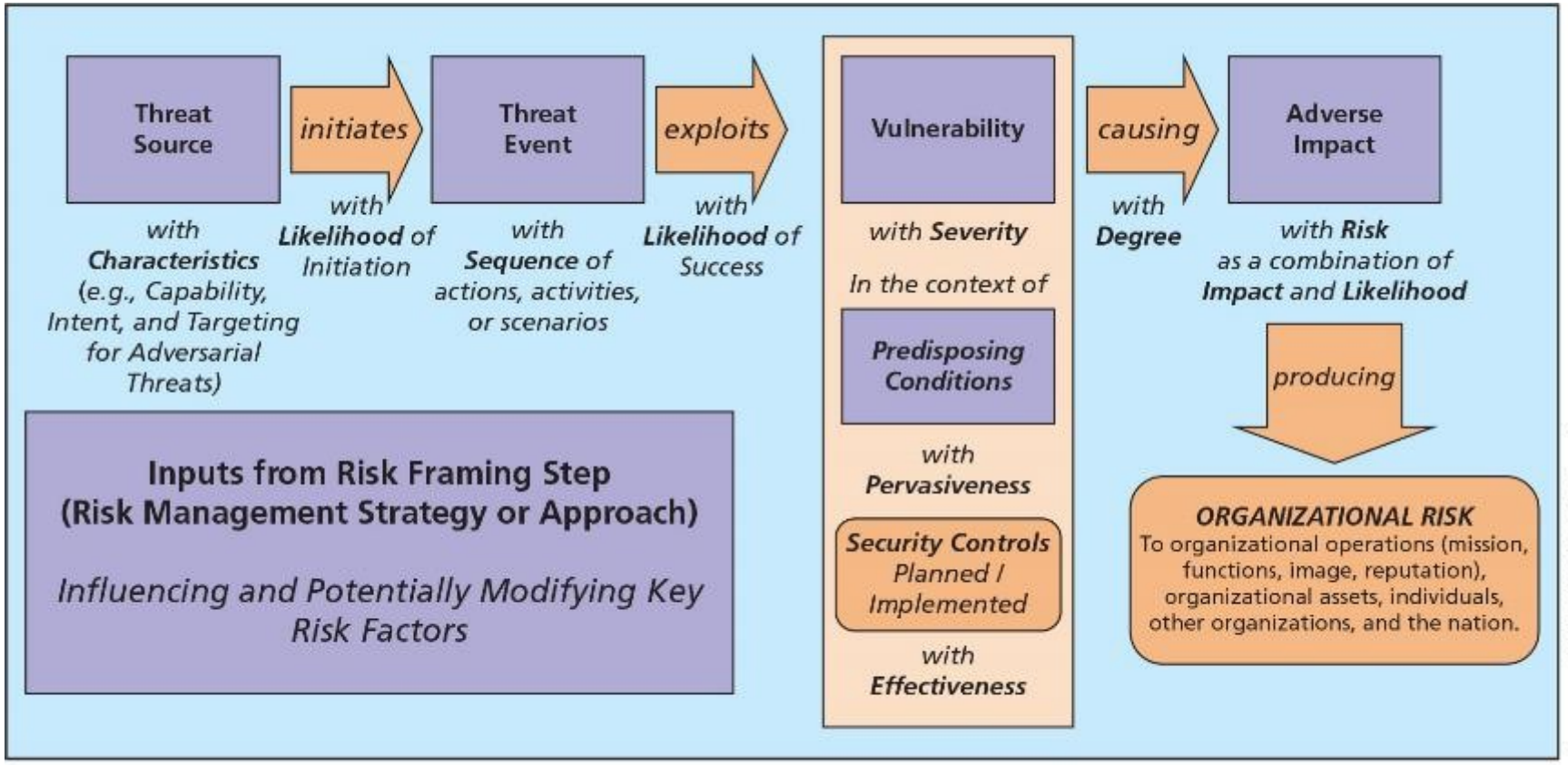

Figure 4-4 NIST generic risk model with key risk factors

Determining the Likelihood of a Threat Event

- **Likelihood** is the overall rating—a numerical value on a defined scale—of the probability that a specific vulnerability will be exploited or attacked, commonly referred to as a threat event.
- *The likelihood of occurrence is a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities). The likelihood risk factor combines an estimate of the likelihood that the threat event will be initiated with an estimate of the likelihood of impact (i.e., the likelihood that the threat event results in adverse impacts). For adversarial threats, an assessment of likelihood of occurrence is typically based on: (i) adversary intent; (ii) adversary capability; and (iii) adversary targeting. For other than adversarial threat events, the likelihood of occurrence is estimated using historical evidence, empirical data, or other factors (NIST SP 800-30, r. 1).*

Risk Likelihood

Rank	Description	Percent Likelihood	Example
0	Not Applicable	0% likely in the next 12 months	Will never happen
1	Rare	5% likely in the next 12 months	May happen once every 20 years
2	Unlikely	25% likely in the next 12 months	May happen once every 10 years
3	Moderate	50% likely in the next 12 months	May happen once every 5 years
4	Likely	75% likely in the next 12 months	May happen once every year
5	Almost Certain	100% likely in the next 12 months	May happen multiple times a year

Assessing Potential Impact on Asset Value

- Once the probability of an attack by a threat has been evaluated, the organization typically looks at the possible **impact or consequences** of a successful attack.
- *The level of impact from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability…*
- *Organizations make explicit: (i) the process used to conduct impact determinations; (ii) assumptions related to impact determinations; (iii) sources and methods for obtaining impact information; and (iv) the rationale for conclusions reached with regard to impact determinations (NIST SP 800-30, r. 1).*

Risk Impact

Rank	Description	Example	# of Records	Productivity Hours Lost	Financial Impact
0	Not applicable threat	No impact	N/A	N/A	N/A
1	Insignificant	No interruption, no exposed data	0	0	0
2	Minor	Multi-minute interruption, no exposed data	0	2	$20,000
3	Moderate	Multi-hour interruption, minor exposure of data	499	4	$175,000
4	Major	One-day interruption, exposure of data	5,000	8	$2,000,000
5	Severe	Multi-day interruption, major exposure of sensitive data	50,000	24	$20,000,000

Aggregation and Uncertainty

- If the RM process begins to overwhelm an organization, the RM team can begin merging or aggregating groups of assets, threats, and their associated risks into more general categories.
- It is not possible to know everything about every vulnerability, such as the likelihood of an attack against an asset or how great an impact a successful attack would have on the organization.
- The degree to which a current control can reduce risk is also subject to estimation error.
- A factor that accounts for uncertainty must always be considered; it consists of an estimate made by the manager using good judgment and experience.

Risk Determination

- Once the likelihood and impact are known, the organization can perform risk determination using a formula that seeks to quantify certain risk elements.
- In this formula, risk equals likelihood of threat event (attack) occurrence multiplied by impact (or consequence), plus or minus an element of uncertainty.

Clearwater IRM Risk Rating Matrix

Risk Rating Matrix

Impact						
	Severe (5)	Low	Medium	High	High	Critical
	Major (4)	Low	Medium	Medium	High	High
	Moderate (3)	Low	Low	Medium	Medium	High
	Minor (2)	Low	Low	Low	Medium	Medium
	Insignificant (1)	Low	Low	Low	Low	Low
		Rare (1)	Unlikely (2)	Moderate (3)	Likely (4)	Almost Certain (5)
		Likelihood				

Risk = Likelihood X Impact

Figure 4-8 Clearwater IRM risk rating matrix

Source: Clearwater Compliance IRM.

Risk Rating Worksheet (1 of 3)

Asset	Vulnerability	Likelihood	Impact	Risk-Rating Factor
Customer service request via e-mail (inbound)	E-mail disruption due to hardware failure	3	3	9
Customer service request via e-mail (inbound)	E-mail disruption due to software failure	4	3	12
Customer order via SSL (inbound)	Lost orders due to Web server hardware failure	2	5	10

Risk Rating Worksheet (2 of 3)

Asset	Vulnerability	Likelihood	Impact	Risk-Rating Factor
Customer order via SSL (inbound)	Lost orders due to Web server or ISP service failure	4	5	20
Customer service request via e-mail (inbound)	E-mail disruption due to SMTP mail relay attack	1	3	3
Customer service request via e-mail (inbound)	E-mail disruption due to ISP service failure	2	3	6

Risk Rating Worksheet (3 of 3)

Asset	Vulnerability	Likelihood	Impact	Risk-Rating Factor
Customer service request via e-mail (inbound)	E-mail disruption due to power failure	3	3	9
Customer order via SSL (inbound)	Lost orders due to Web server denial-of-service attack	1	5	5
Customer order via SSL (inbound)	Lost orders due to Web server software failure	2	5	10
Customer order via SSL (inbound)	Lost orders due to Web server buffer overrun attack	1	5	5

Risk Evaluation

- Once the risk ratings are calculated for all TVA triples, the organization needs to decide whether it can live with the analyzed level of risk.
- If residual risk is greater than risk, look for treatment strategies to further reduce the risk.
- If residual risk is less than risk appetite, document the results and proceed to the latter stages of risk management.

Documenting the Results of Risk Assessment

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

Risk Assessment Deliverables

Deliverable	Purpose
Information asset and classification worksheet	Assembles information about information assets, their sensitivity levels, and their value to the organization
Information asset value weighted table analysis	Rank-orders each information asset according to criteria developed by the organization
Threat severity weighted table analysis	Rank-orders each threat to the organization's information assets according to criteria developed by the organization
TVA controls worksheet	Combines the output from the information asset identification and prioritization with the threat identification and prioritization, identifies potential vulnerabilities in the "triples," and incorporates extant and planned controls
Risk ranking worksheet	Assigns a risk-rating ranked value to each TVA triple, incorporating likelihood, impact, and possibly a measure of uncertainty

Risk Treatment/Risk Response (1 of 2)

- After the risk management (RM) process team has identified, analyzed, and evaluated the level of risk currently inherent in its information assets (risk assessment), it then must treat the risk that is deemed unacceptable when it exceeds its risk appetite.
- This process is also known as risk response or risk control.
- As risk treatment begins, the organization has a list of information assets with currently unacceptable levels of risk; the appropriate strategy must be selected and then applied for each asset.

Risk Treatment/Risk Response (2 of 2)

- Once the project team for InfoSec development has identified the information assets with unacceptable levels of risk, the team must choose one of four basic strategies to treat the risks for those assets:
  - Mitigation
  - Transference
  - Acceptance
  - Termination

Risk Mitigation

- The **mitigation risk treatment strategy**, sometimes referred to as **risk defense** or simply **risk mitigation**, attempts to prevent the exploitation of the vulnerability.
- This is the preferred approach, and it is accomplished by means of countering threats, removing vulnerabilities in assets, limiting access to assets, and adding protective safeguards.
- In essence, the organization is attempting to improve the security of an information asset by reducing the likelihood or probability of a successful attack.

Risk Transference

- The **transference risk treatment strategy**, sometimes known as **risk sharing** or simply **risk transfer**, attempts to shift risk to another entity.
- This goal may be accomplished by rethinking how services are offered, revising deployment models, outsourcing to other organizations, purchasing insurance, or implementing service contracts with providers.
- The key to an effective transference risk treatment strategy is the implementation of an effective **service level agreement (SLA)**.

Risk Acceptance

- The **acceptance risk treatment strategy**, or simply **risk acceptance**, is the decision to do nothing beyond the current level of protection to shield an information asset from risk and to accept the outcome from any resulting exploitation.
- Acceptance is a valid strategy only when the organization has:
  - Determined the level of risk to the information asset
  - Assessed the probability and likelihood
  - Estimated the potential impact of a successful attack
  - Evaluated potential controls
  - Performed a thorough risk assessment
  - Determined that the costs to treat the risk do not justify the cost of the controls

Risk Termination

- The **termination risk treatment strategy**, also known as **risk avoidance** or simply **risk termination**, is based on the organization's intentional choice not to protect an asset.
- The organization does not want the information asset to remain at risk and removes it from the operating environment by shutting it down or disabling its connectivity to potential threats.
- Sometimes the cost of protecting an asset outweighs its value.
- In any case, termination must be a conscious business decision, not simply the abandonment of an asset.

Knowledge Check Activity 3

Applying controls and safeguards that eliminate or reduce the remaining uncontrolled risks is known as _____.

a. acceptance

b. termination

c. transference

d. mitigation

Knowledge Check Activity 3: Answer

Applying controls and safeguards that eliminate or reduce the remaining uncontrolled risks is known as _____.

Answer: d. mitigation

Transference is the shifting risks to other areas or to outside entities; acceptance is understanding the consequences of choosing to leave an information asset's vulnerability facing the current level of risk, but only after a formal evaluation and intentional acknowledgment of this decision; and termination is the removal of the information asset from the organization's operating environment.

Process Communications, Monitoring, and Review

- As the process team works through the various RM activities, it needs to continually provide feedback to the framework team about the relative success and challenges of its RM activities, to improve not only the process but the framework as well.
- **Process communications** involve requesting and providing information as direct feedback about issues that arise in the implementation and operation of each stage of the process.
- **Process monitoring and review** involves establishing and collecting formal performance measures and assessment methods to determine the relative success of the RM program.

Managing Risk

- The goal of InfoSec is to bring residual risk in line with an organization's risk appetite, not to bring risk to zero.
- Rules of thumb for selecting a strategy:
  - *When a vulnerability exists in an important asset*—Implement security controls to reduce likelihood.
  - *When a vulnerability can be exploited*—Apply controls to minimize the risk or prevent the occurrence of an attack.
  - *When the attacker's potential gain is greater than the costs of attack*—Apply protections to increase the attacker's cost or reduce the attacker's gain.
  - *When the potential loss is substantial*—Apply protections to limit the extent of the attack, reducing the potential for loss.

Residual Risk

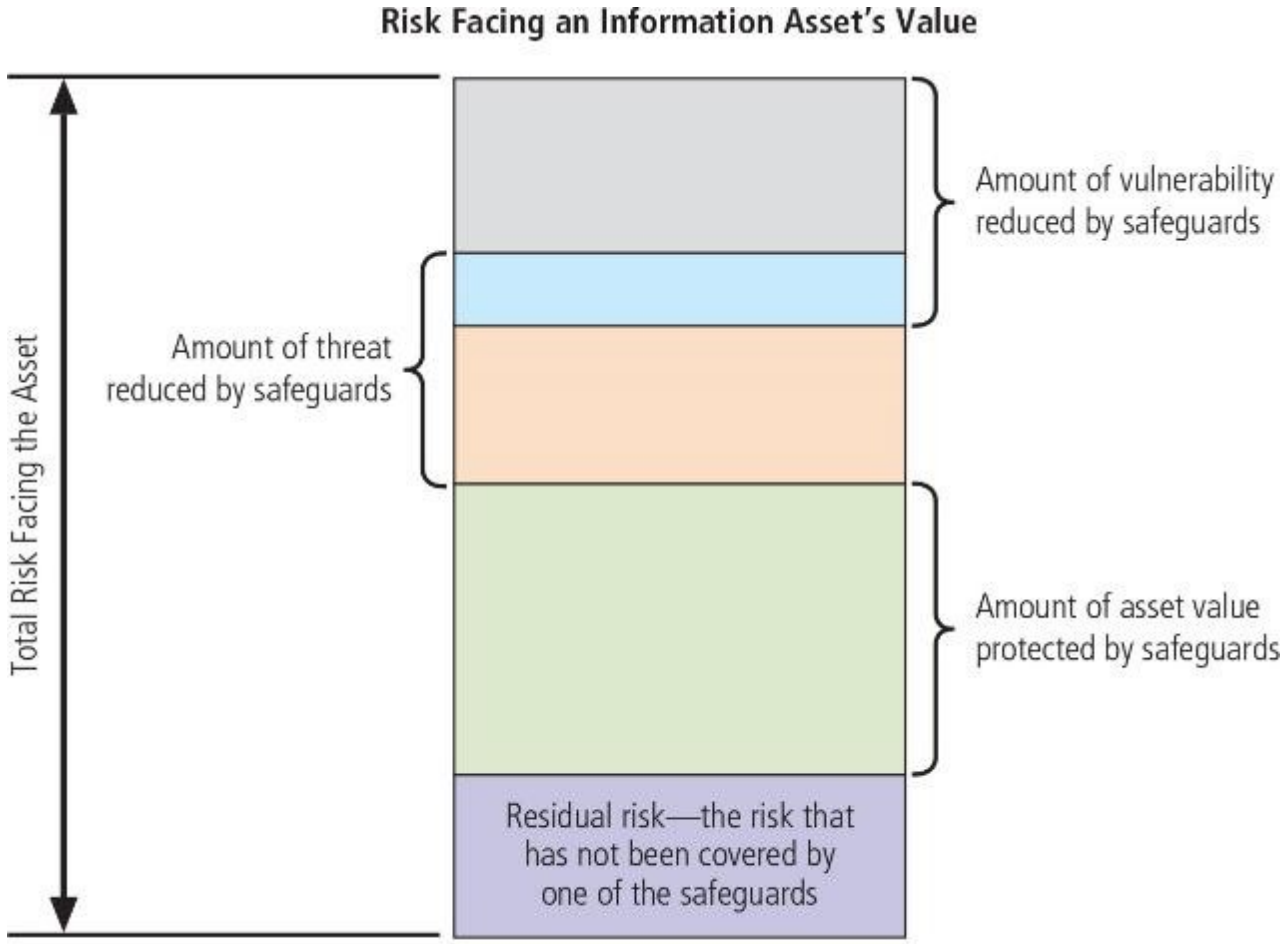

Figure 4-11 Residual risk

Risk-Handling Action Points

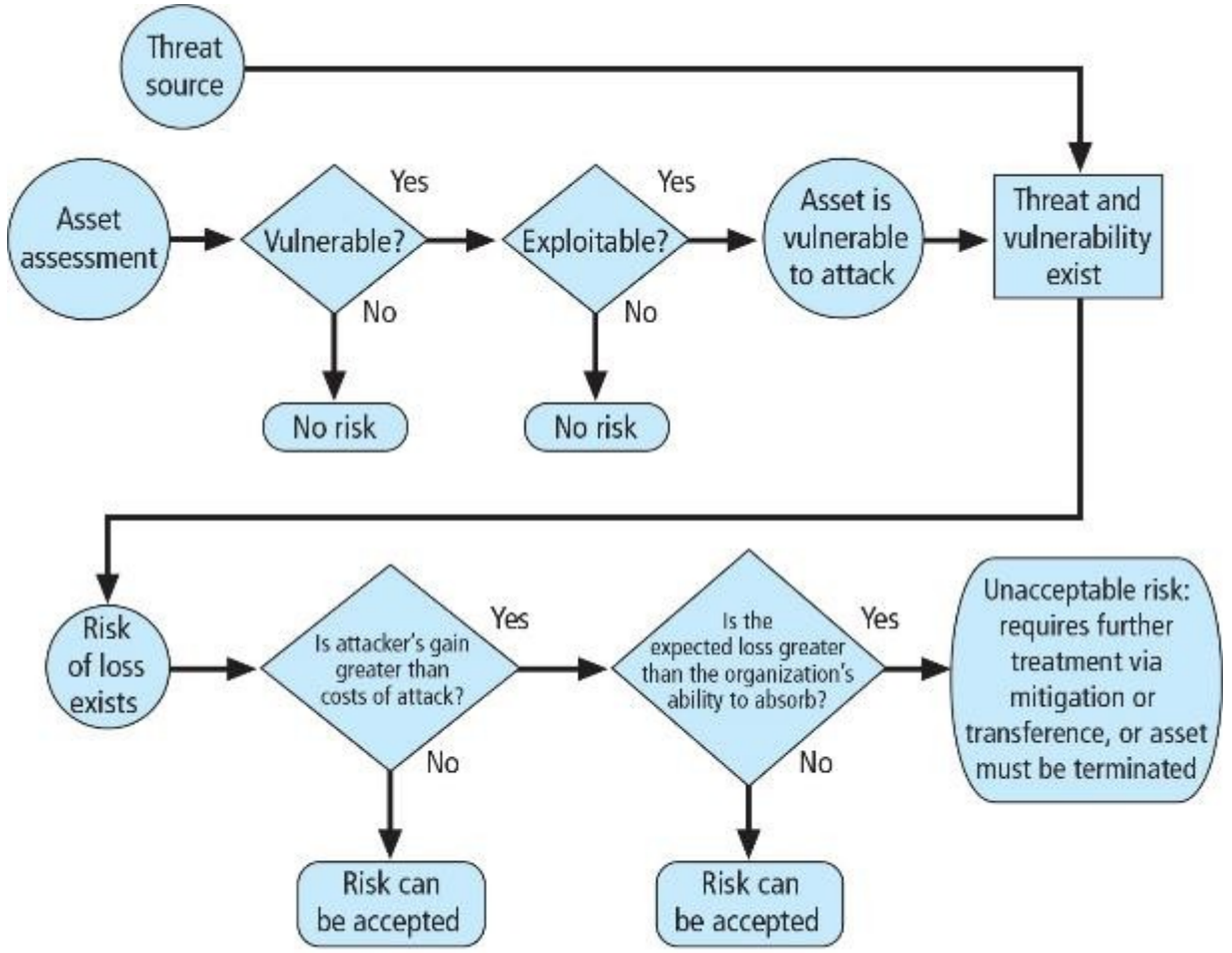

Figure 4-12 Risk-handling action points

Risk Treatment Cycle

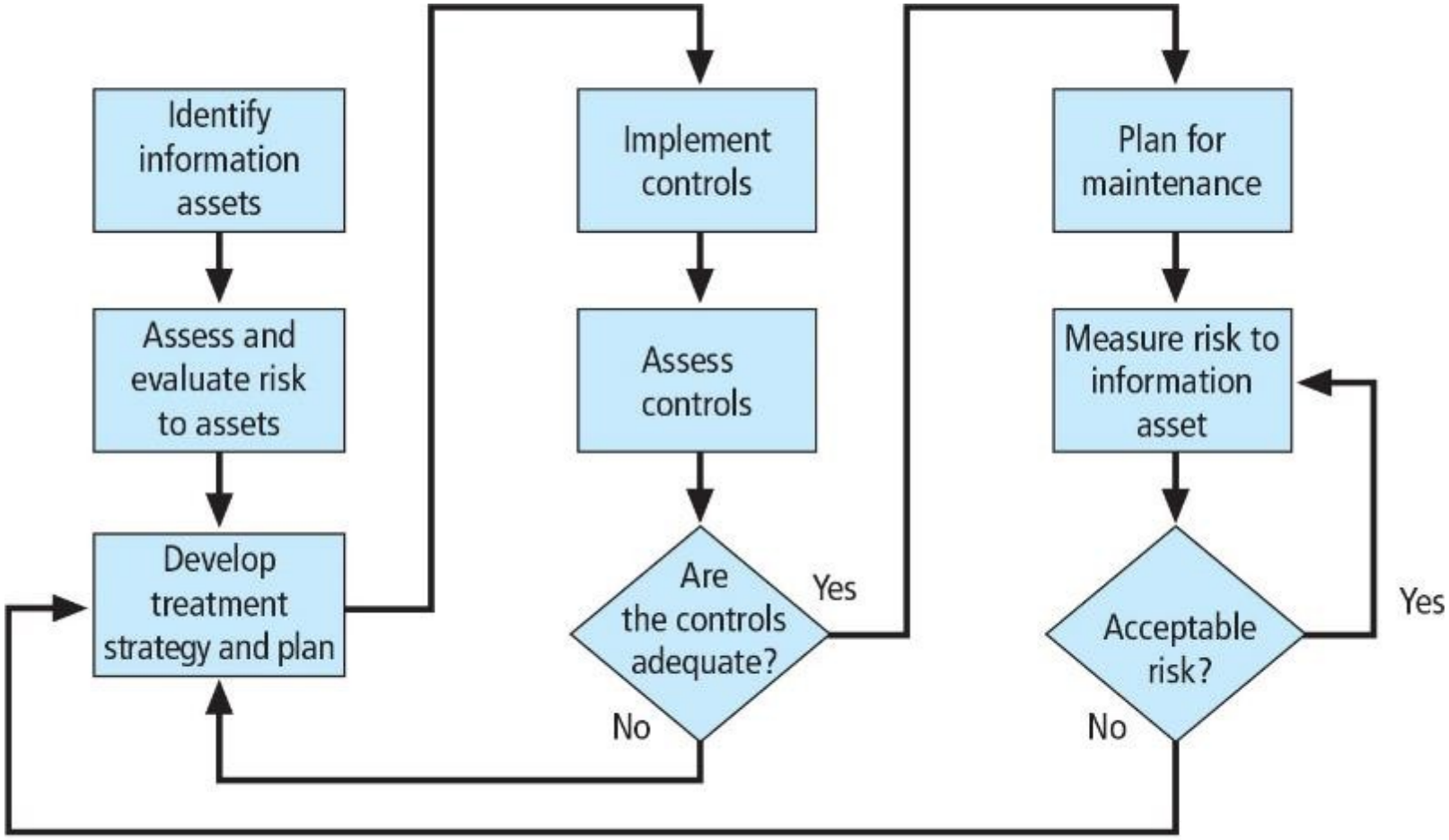

Figure 4-13 Risk treatment cycle

Feasibility and Cost-Benefit Analysis

- Before implementing one of the control strategies for a specific vulnerability, the organization must explore all consequences of vulnerability to information assets.
- There are several ways to determine the advantages/disadvantages of a specific control.
- Items that affect the cost of a control or safeguard include cost of development or acquisition, training fees, implementation cost, service costs, and cost of maintenance.
- Common sense dictates that an organization should not spend more to protect an asset than it is worth; this decision-making process is called a **cost-benefit analysis (CBA)** or an economic feasibility study.

Asset Valuation (1 of 2)

- 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)

Asset Valuation (2 of 2)

- CBA determines if an alternative being evaluated is worth the cost incurred to control the 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 the 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.

Alternate Risk Management Methodologies

- The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Method was a risk evaluation methodology promoted by Carnegie Mellon University's Software Engineering Institute (SEI), and it had three versions:
  - The original OCTAVE Method, for large organizations
  - OCTAVE-S, for smaller organizations of about 100 users
  - OCTAVE-Allegro, a streamlined approach for InfoSec assessment and assurance
- Factor Analysis of Information Risk (FAIR), by Jack A. Jones, became CXOWARE, which built FAIR into an analytical software suite called RiskCalibrator. FAIR was adopted by the Open Group as an international standard for risk management and rebranded as Open FAIR™. Later, CXOWARE became RiskLens, and the FAIR Institute was established.

ISO and NIST RMF

- The International Organization for Standardization (ISO) has several standards related to information security and two that specifically focus on risk management:
  - ISO 27005 information technology — security techniques — information security risk management
  - ISO 31000 risk management – guidelines
- The National Institute of Standards and Technology (NIST) has modified its fundamental approach to systems management and certification/accreditation to one that follows the industry standard of effective risk management.
- Two key documents describe the RMF:
  - SP 800-37, Rev. 2 Risk Management Framework for Information Systems and Organizations
  - SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View

ISO 27005 Information Security Risk Management Process

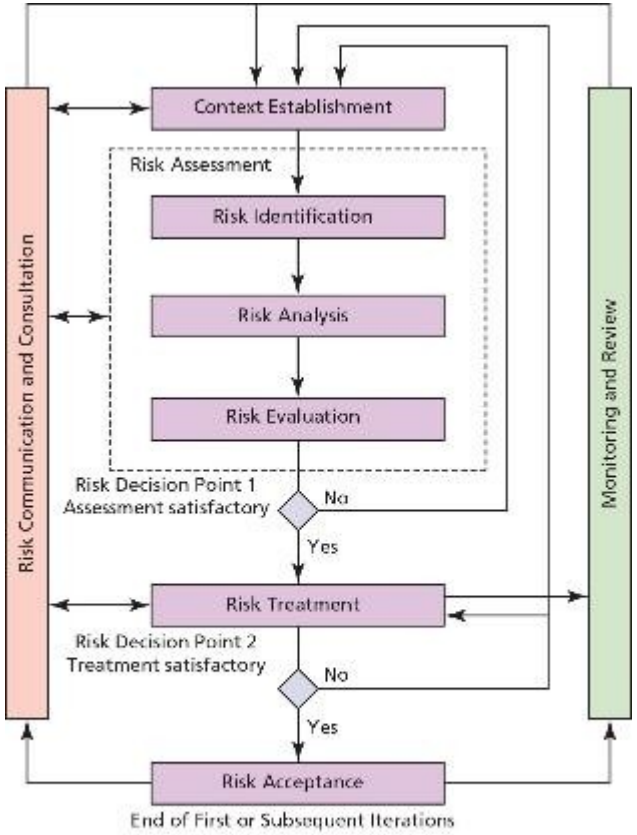

Figure 4-18 ISO 27005 information security risk management process[17]

Source: ISO 27005:2018.

ISO 31000 Risk Management Principles, Framework, and Process

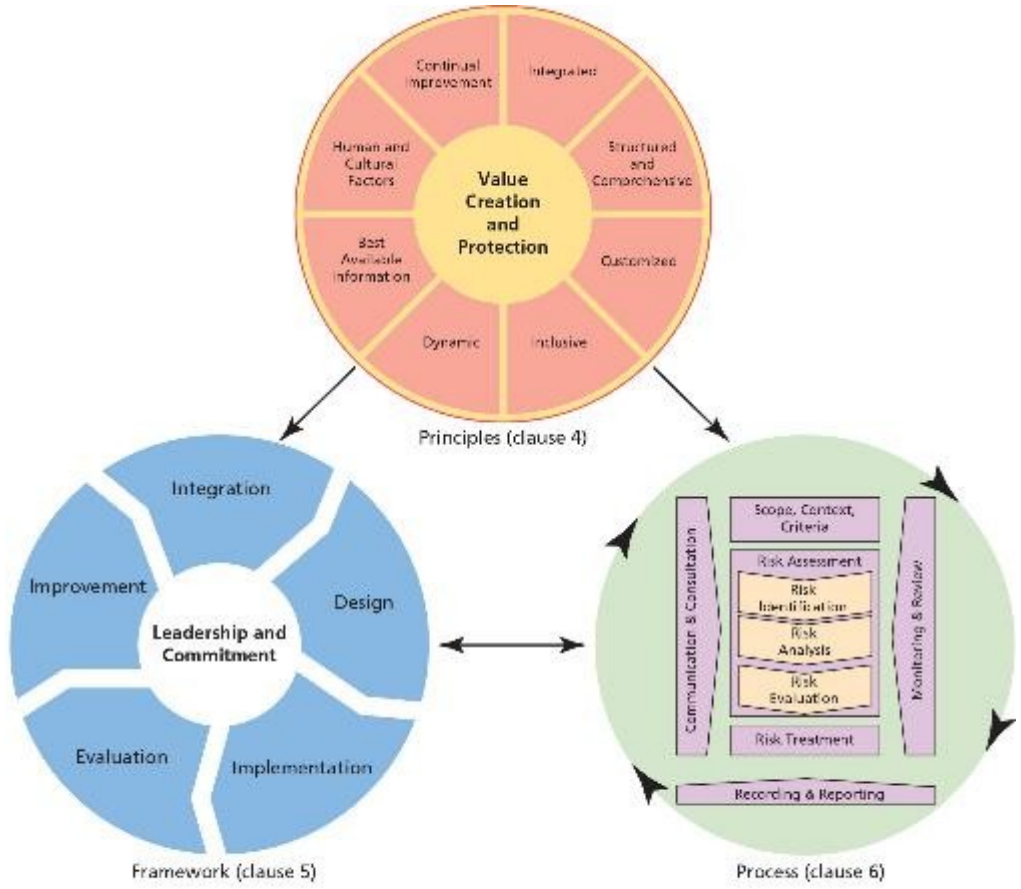

Figure 4-19 ISO 31000 risk management principles, framework, and process[18]

Source: ISO 31000:2018.

NIST Organization-Wide Risk Management Approach

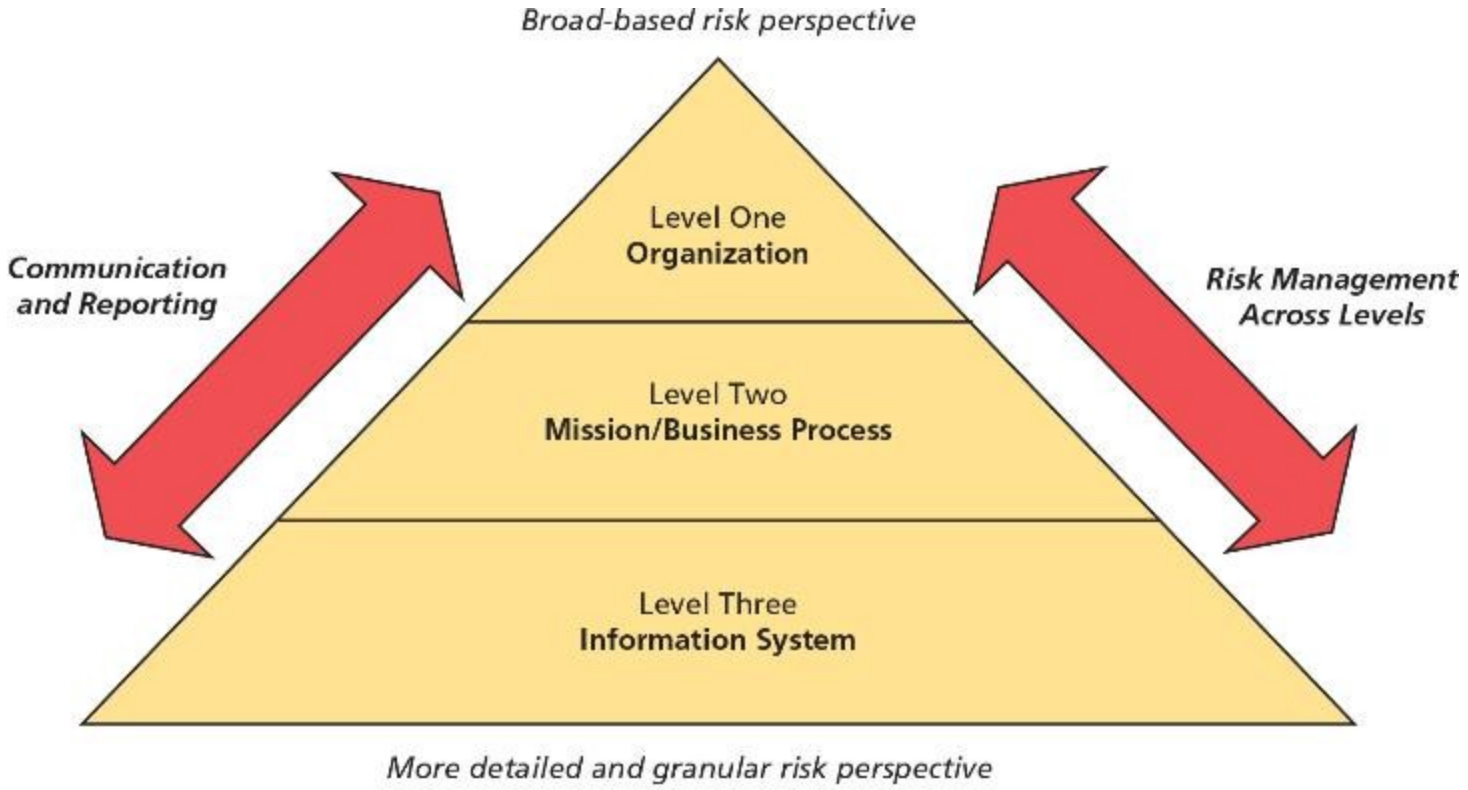

Figure 4-20 NIST organization-wide risk management approach[20]

Source: NIST SP 800-37, Revision 2, "Risk Management Framework for Information Systems and Organizations."

NIST RMF Framework

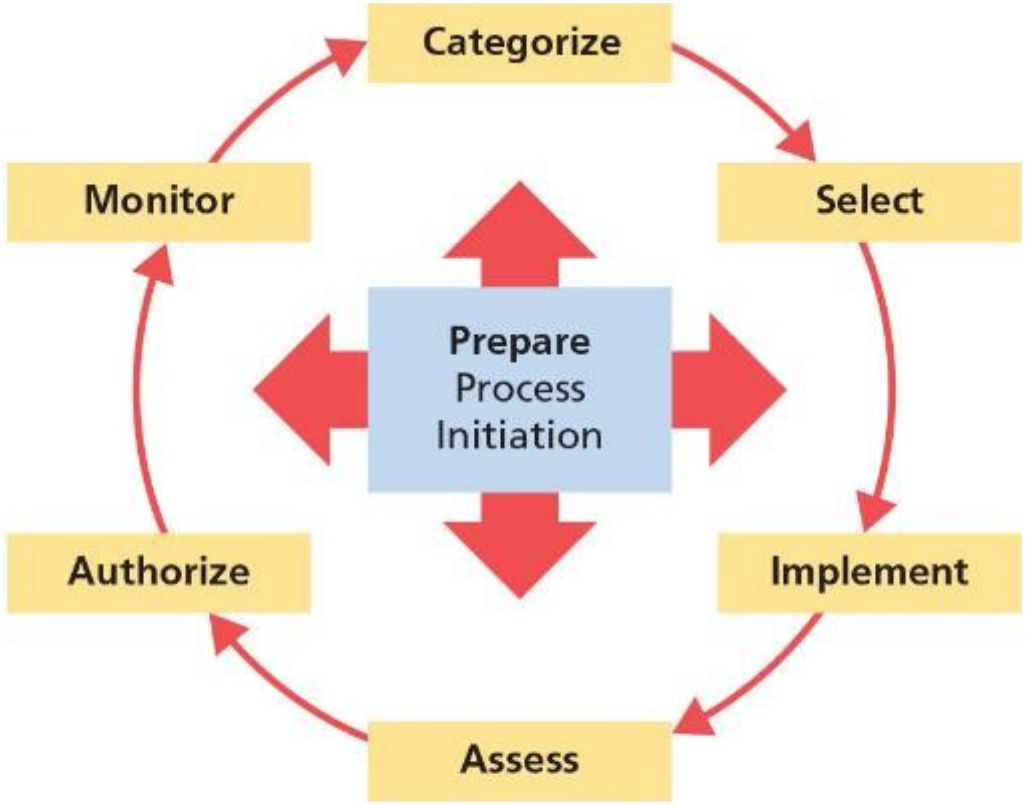

Figure 4-21 NIST RMF framework[21]

Source: NIST, SP 800-37, Revision 2, "Risk Management Framework for Information Systems and Organizations."

Selecting the Best RM Model

- For organizations that have no risk management process in place, a recommended approach is to begin by studying the models presented earlier in this module and identifying what each offers to the envisioned process.
- Other organizations may hire a consulting firm to provide or even develop a proprietary model.
- When faced with the daunting task of building a risk management program from scratch, it may be best to talk with other security professionals, perhaps through professional security organizations like ISSA, to find out how others in the field have approached this problem.
- No two organizations are identical, so what works well for one organization may not work well for others.

Summary (1 of 8)

- Risk management examines and documents an organization's information assets.
- Management is responsible for identifying and controlling the risks that an organization encounters. In the modern organization, the InfoSec group often plays a leadership role in risk management.
- Risk appetite defines the quantity and nature of risk that organizations are willing to accept as they evaluate the trade-offs between perfect security and unlimited accessibility.
- Residual risk is the amount of risk unaccounted for after the application of controls.
- A key component of a risk management strategy is the identification, classification, and prioritization of the organization's information assets.
- Assessment is the identification of assets, including all the elements of an organization's system: people, procedures, data, software, hardware, and networking elements.

Summary (2 of 8)

- The human resources, documentation, and data information assets of an organization are not as easily identified and documented as tangible assets, such as hardware and software. Less tangible assets should be identified and described using knowledge, experience, and judgment.
- You can use the answers to the following questions to develop weighting criteria for information assets:
  - Which information asset is the most critical to the success of the organization?
  - Which information asset generates the most revenue?
  - Which information asset generates the highest profitability?
  - Which information asset is the most expensive to replace?
  - Which information asset is the most expensive to protect?
  - Which information asset's loss or compromise would be the most embarrassing or cause the greatest liability?

Summary (3 of 8)

- After an organization identifies and performs a preliminary classification of information assets, the threats facing the organization should be examined. There are 12 general categories of threats to InfoSec.
- Each threat must be examined during a threat assessment process that addresses the following questions:
  - Which of the threats exist in the organization's environment?
  - Which are the most dangerous to the organization's information?
  - Which require the greatest expenditure for recovery?
  - Which require the greatest expenditure for protection?
- Each information asset is evaluated for each threat it faces; the resulting information is used to create a list of the vulnerabilities that pose risks to the organization. This process results in an information asset and vulnerability list, which serves as the starting point for risk assessment.

Summary (4 of 8)

- A threats-vulnerabilities-assets (TVA) worksheet lists assets in priority order along one axis and threats in priority order along the other axis. The resulting grid provides a convenient method of examining the "exposure" of assets, allowing a simple vulnerability assessment.
- The human resources, documentation, and data information assets of an organization are not as easily identified and documented as tangible assets, such as hardware and software. Less tangible assets should be identified and described using knowledge, experience, and judgment.
- You can use the answers to the following questions to develop weighting criteria for information assets:
  - Which information asset is the most critical to the success of the organization?
  - Which information asset generates the most revenue?
  - Which information asset generates the highest profitability?
  - Which information asset is the most expensive to replace?

Summary (5 of 8)

  - Which information asset is the most expensive to protect?
  - Which information asset's loss or compromise would be the most embarrassing or cause the greatest liability?
- After an organization identifies and performs a preliminary classification of information assets, the threats facing the organization should be examined. There are 12 general categories of threats to InfoSec.
- Each threat must be examined during a threat assessment process that addresses the following questions:
  - Which of the threats exist in the organization's environment?
  - Which are the most dangerous to the organization's information?
  - Which require the greatest expenditure for recovery?
  - Which require the greatest expenditure for protection?

Summary (6 of 8)

- Each information asset is evaluated for each threat it faces; the resulting information is used to create a list of the vulnerabilities that pose risks to the organization. This process results in an information asset and vulnerability list, which serves as the starting point for risk assessment.
- The goal of risk assessment is the assignment of a risk rating or score that represents the relative risk for a specific vulnerability of a specific information asset.
- It is possible to perform risk analysis using estimates based on a qualitative assessment.
- If any specific vulnerability is completely managed by an existing control, it no longer needs to be considered for additional controls.

Summary (7 of 8)

- The risk identification process should designate what function the resulting reports serve, who is responsible for preparing them, and who reviews them. The TVA worksheet and other risk worksheets are working documents for the next step in the risk management process: treating and controlling risk.
- Once vulnerabilities are identified and ranked, a strategy to control the risks must be chosen. Four control strategies are mitigation, transference, acceptance, and termination.
- Economic feasibility studies determine and compare costs and benefits from potential controls (cost-benefit analysis, or CBA). A CBA determines whether a control alternative is worth its associated cost.
- CBA calculations are based on costs before and after controls are implemented and the cost of the controls.

Summary (8 of 8)

- Other forms of feasibility analysis include analyses based on organizational, operational, technical, and political factors.
- An organization must be able to place a dollar value on each collection of information and information assets it owns. There are several methods an organization can use to calculate these values.
- Single loss expectancy (SLE) is calculated from the value of the asset and the expected percentage of loss that would occur from a single successful attack. Annualized loss expectancy (ALE) represents the potential loss per year.
- Alternative approaches to risk management include the OCTAVE Method, ISO 27005, the NIST risk management approach, and FAIR.

Self-Assessment

- Without using the textbook, think of your own original definition of risk management and write it down.
- Now compare your definition to the one found in the textbook. How is it different?
- How has this module changed the way you understand this concept or *risk*?
- What other questions do you have about risk management in this field?