



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

ACCA5034

Data Security and Compliance

Week 4 : Risk Management

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk

Learning Objective(s) and Key Concepts

Learning Objective(s)

- Define risk management and describe its importance
- Explain the risk management framework and process model, including major components
- Define risk appetite and explain how it relates to residual risk
- Describe how risk is identified and documented
- Discuss how risk is assessed based on likelihood and impact
- Describe various options for a risk treatment and risk control strategy
- Discuss conceptual frameworks for evaluating risk controls and formulate a cost-benefit analysis
- Compare and contrast the dominant risk management methodologies

Key Concepts

Introduction to Risk Management

- Upper management oversees and supports IT and information security to protect organisational assets.
- Effective risk management (RM) is a key governance requirement.
- Secure business environments are essential for maintaining competitiveness.
- Risk management principles ensure confidentiality, privacy, and data integrity.

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 organisation’s information assets

The Risk Management Framework

- Risk management involves discovering and understanding answers to some key questions about the risk associated with an organisation'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

- **Risk management** involves identifying, analysing, evaluating, and treating risks to an organisation's information assets.
- **Risk identification** recognises, lists, and documents potential risks.
- **Risk analysis & evaluation** assess the severity of risks and determine if they are acceptable.
- **Risk treatment** applies safeguards to reduce risks to an acceptable level.

The Risk Management Framework

- **Risk management (RM)** is a complex process requiring a formal methodology.
- **RM consists of two key areas:** the RM framework and the RM process.
- **The RM framework** provides the strategic structure for managing risk across the organisation.
- **The RM process** implements risk management, following the framework to evaluate and address risks.

The Risk Management Framework and Process

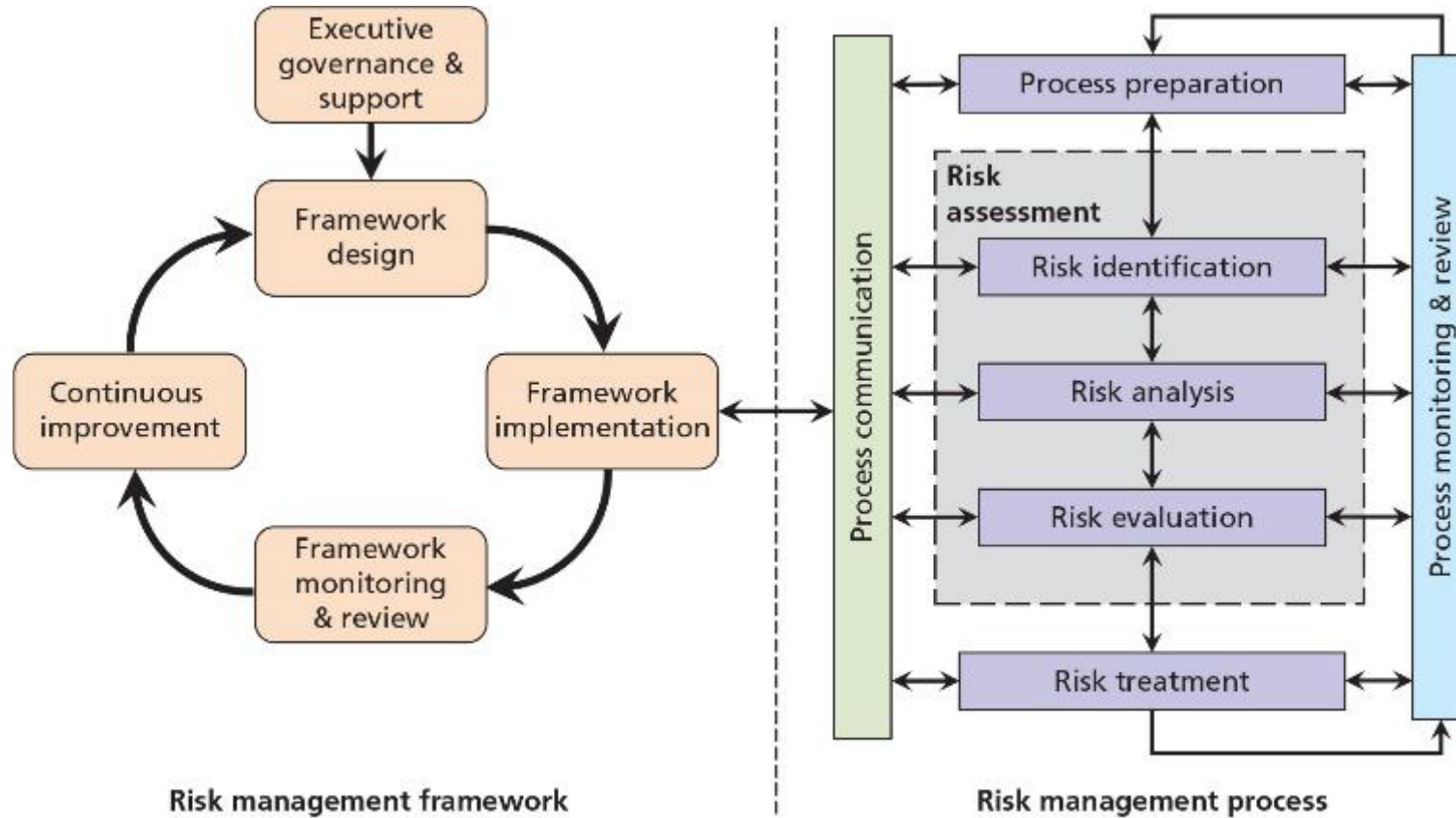


Figure 4-1 The risk management framework and process

The Risk Management Framework

- 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

Executive governance and support

- Collaboration between information security, IT, business management, and users is essential, with communities of interest evaluating, selecting, and maintaining risk controls.
- The RM policy translates governance instructions into structured guidance, covering purpose, objectives, roles, risk appetite, and key references.

Framework Design

- **Framework design** involves defining risk appetite, assessing current risk levels, and drafting the RM plan in alignment with governance directives.

Defining the Organisation's Risk Tolerance and Risk Appetite

- **Risk appetite** defines the level and type of risk an organisation is willing to accept.
- **Residual risk** is the remaining risk after applying existing controls.
- **Risk tolerance** specifies the acceptable risk level for a particular information asset.
- **Information security** aims to align residual risk with the organisation's risk appetite.

Framework Implementation

- Framework implementation aligns with the organisation's risk appetite and may use methods such as desk checks, pilot tests, phased approaches, or direct cutovers.
- Implementation methods could include:
 - Desk check – A theoretical review to identify potential issues before implementation.
 - Pilot test – A small-scale trial to assess effectiveness before full deployment.
 - Phased approach – Gradual implementation in stages to minimise risk.
 - Direct cutover – Immediate full transition, replacing the old system at once.

Framework Monitoring and Review

- Ongoing monitoring ensures the RM process is effectively executed and aligned with objectives.
- Regular reviews assess the success and relevance of the RM framework.
- The framework team focuses on overseeing and refining the 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
 - Analysing risk
 - Evaluating the risk and comparing uncontrolled risks against the risk appetite
 - Treating the unacceptable risk
 - Summarising the findings

RM Process Preparation

-Establishing the Context-

- Context establishment ensures the RM process aligns with managerial intent and organisational objectives.
- Executive guidance from the framework and governance teams helps set the direction for the RM process team.
- Preparation steps (as per NIST SP 800-30) include defining purpose, scope, assumptions, data sources, and analytical 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 organisation's information assets
 2. Classify them
 3. Categorise them into useful groups
 4. Prioritise them by overall importance

Organisational Assets Used in Systems

Information System Components	Risk Management (RM) Components	Example RM Components
People	Internal personnel	Trusted employees (Staff members)
People	External personnel	People we trust outside our organisation
Procedures	Procedures	IT and business standard procedures and /or sensitive procedures
Data	Data/information	Transmission Processing Storage
Software	Software	Applications, Operating systems, Utilities Security components
Hardware	Hardware	Systems and peripherals, Security devices Network-attached process control devices and other embedded systems (IoT)
Networking	Networking	LAN, Internet, Intranet, & Cloud-based components

Assessing the Value of Information Assets

- As each information asset is identified, categorised, 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 organisation'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 2025	Evaluated By: D. Jones
Information assets	Data classification	Impact to profitability
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 fulfilment advice (inbound)	Confidential	Medium
Customer order via SSL (inbound)	Confidential	Critical
Customer service request via e-mail (inbound)	Private	Medium
Edge router	Public	Critical
Web server #1 – Home page and core site	Public	Critical
Web server #2 – Application server	Private	Critical

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

Prioritising (Rank-Ordering) Information Assets

- The final step in the risk identification process is to prioritise, 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

Weighted Table Analysis of Information Assets

	Criterion →	<i>Impact on Revenue</i>	<i>Impact on Profitability</i>	<i>Impact on Reputation</i>		
#	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
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 organisation 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	Unauthorised 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 organisation's assets and vulnerabilities.
- The process works best when people with diverse backgrounds within an organisation work iteratively in a series of brainstorming sessions.
- At the end of the risk identification process, a prioritised 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

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 organisation 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.

The TVA Worksheet

	Asset 1	Asset 2	Asset 3	...	...	...	...	...	...	Asset n
Threat 1	T1V1A1 T1V2A1 T1V3A1 ...	T1V1A2 T1V2A2 ...	T1V1A3 ...	T1V1A4 ...						
Threat 2	T2V1A1 T2V2A1 ...	T2V1A2 ...	T2V1A3 ...							
Threat n	TnV1A1 ...	TnV1A2 ...								
Legend: Priority of effort	1	2	3	4	5	6	7	8	...	

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

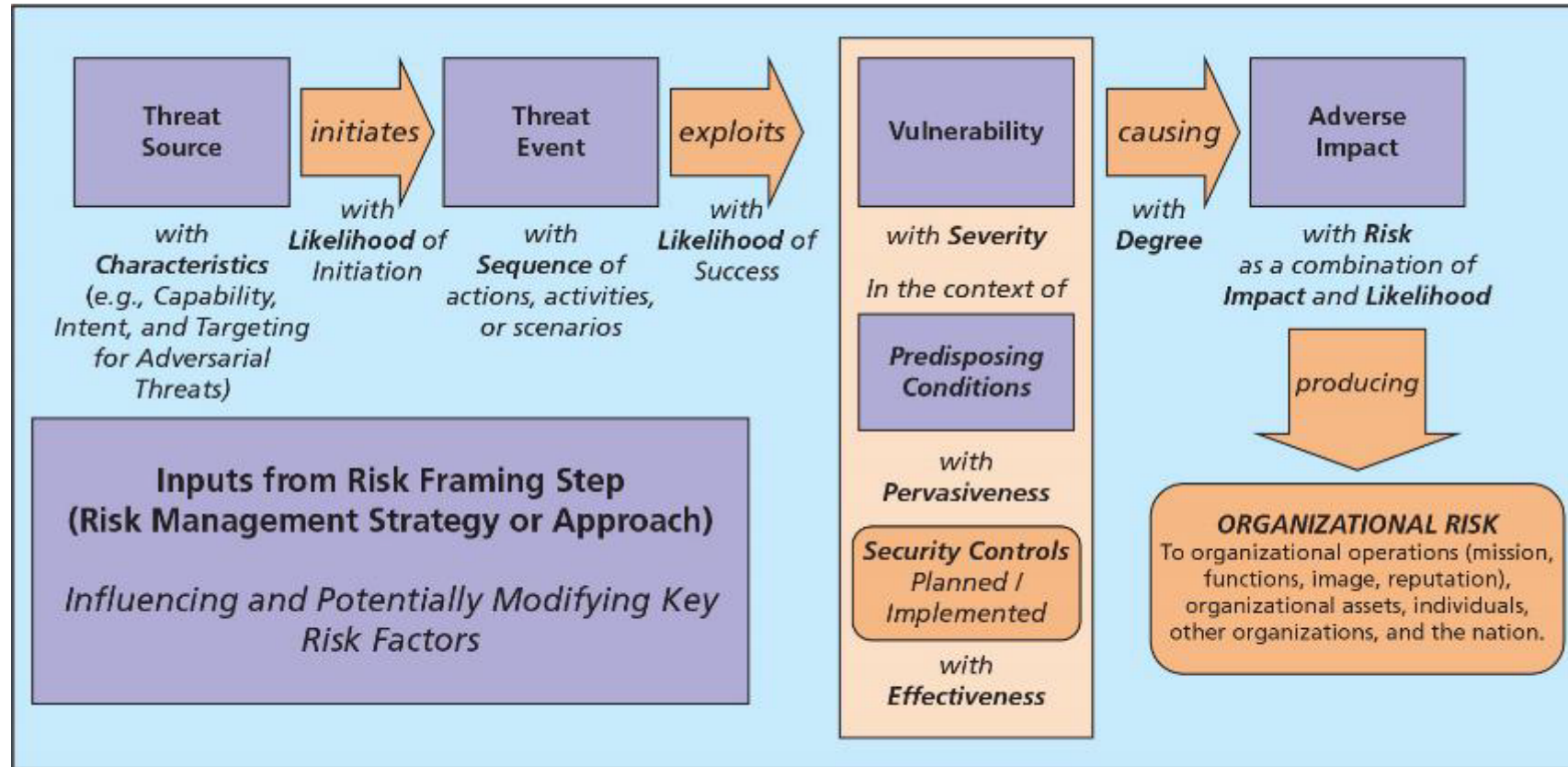


Figure 4-4 NIST generic risk model with key risk factors

Determining the Likelihood of a Threat Event

- **Likelihood** is the probability that a vulnerability will be exploited, rated on a defined scale.
- It combines the chance of a threat occurring and its potential impact.
- For **adversarial threats**, likelihood is assessed based on adversary intent, capability, and targeting.
- For other threats, likelihood is estimated using historical data or empirical evidence.

Assessing Potential Impact on Asset Value

- **Impact** refers to the potential harm from an attack, such as loss, modification, or destruction of information.
- Organisations assess the consequences of unauthorised actions and their effect on information or system availability.
- They clarify the process, assumptions, sources, and rationale used to determine the potential impact of a threat.

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

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 organisation, 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 organisation.
- 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 organisation 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						

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

Risk Rating Worksheet (example)

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 Evaluation

- Once the risk ratings are calculated for all TVA triples, the organisation needs to decide whether it can live with the analysed 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 summarised 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 organisation
Information asset value weighted table analysis	Rank-orders each information asset according to criteria developed by the organisation
Threat severity weighted table analysis	Rank-orders each threat to the organisation's information assets according to criteria developed by the organisation
TVA controls worksheet	Combines the output from the information asset identification and prioritisation with the threat identification and prioritisation, 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

- After risk assessment, the RM team must address risks deemed unacceptable and exceeding the organisation's risk appetite.
- This process, known as risk response or risk control, involves selecting appropriate strategies for each asset.
- Once assets with unacceptable risk levels are identified, the team must choose one of four strategies:
 1. **Mitigation** reduces the likelihood of a successful attack by countering threats, removing vulnerabilities, limiting access, and adding safeguards. This is the preferred strategy to improve security.

Risk Treatment/Risk Response

2. **Transference** shifts the risk to another entity, such as through outsourcing, insurance, or service contracts.
3. **Acceptance** involves deciding not to add further protection, instead accepting the risk after thorough assessment of probability, impact, and control costs.
4. **Termination** (or risk avoidance) involves removing the asset from the environment when the cost of protection outweighs its value, making it a conscious business decision.

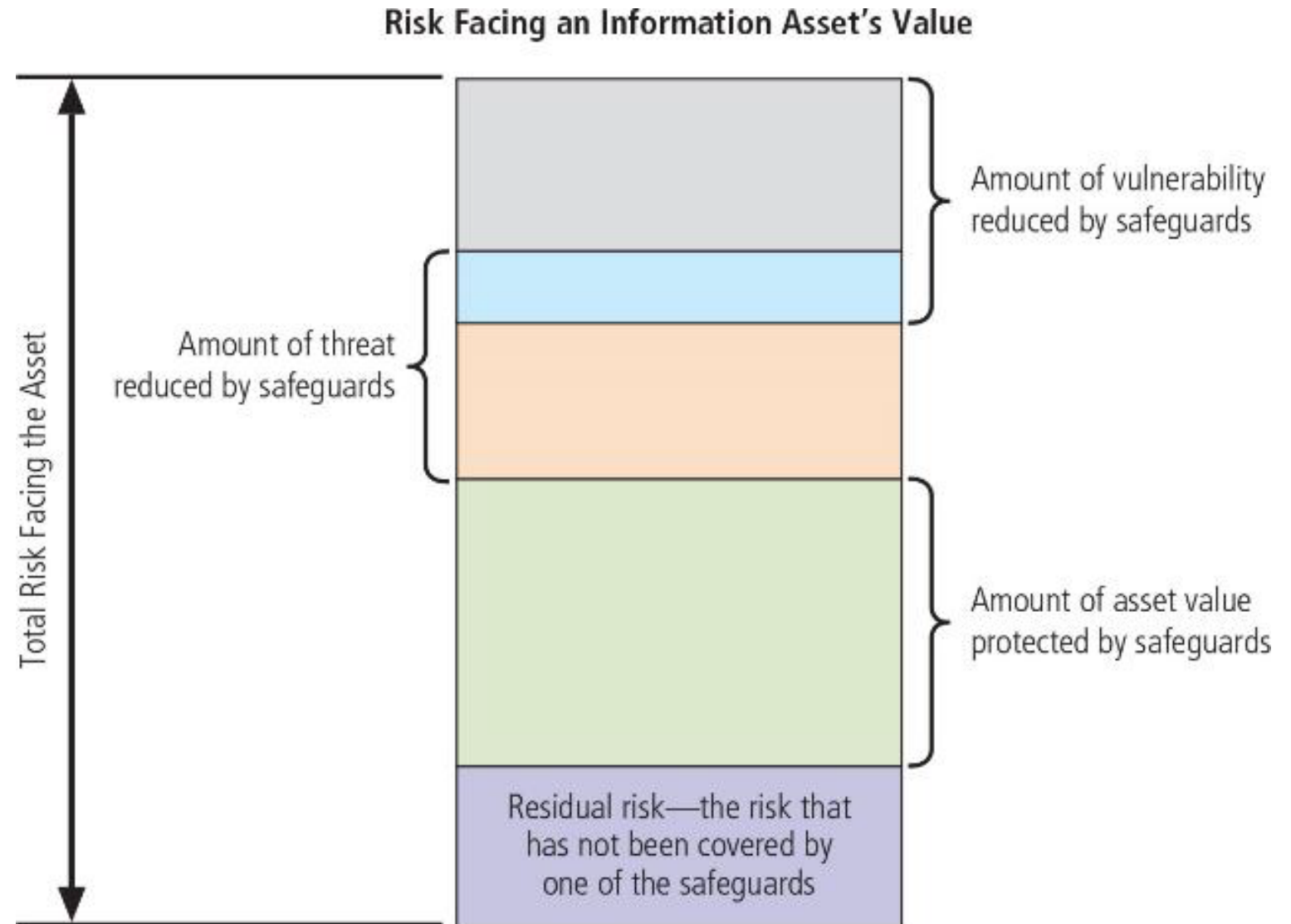
Process Communications, Monitoring, and Review

- Process communications, monitoring, and review involve continuous feedback between the process and framework teams to improve the RM activities and framework.
- Monitoring uses formal performance measures to assess the success of the RM program.

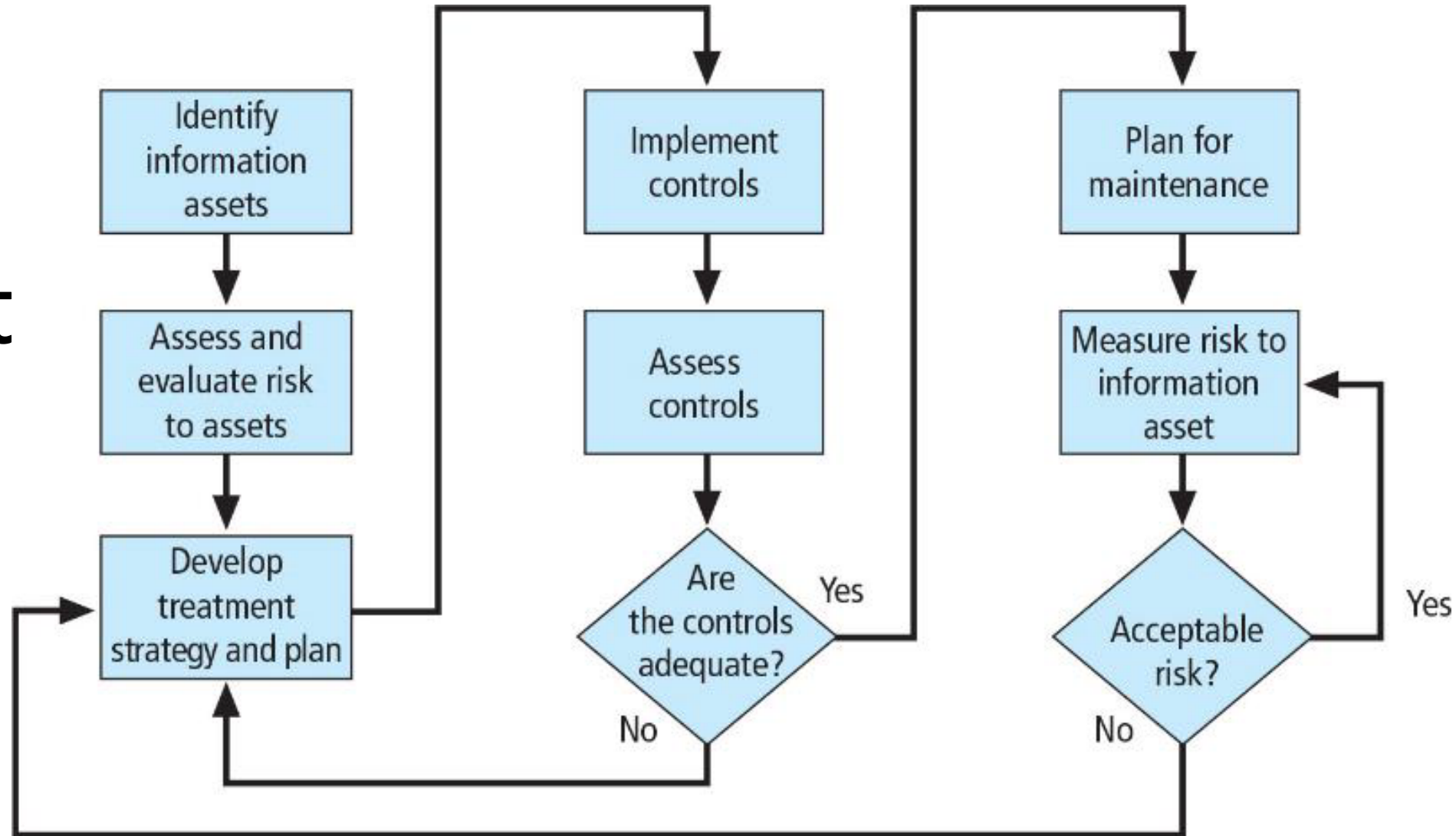
Managing Risk

- Managing risk aims to align residual risk with the organisation's risk appetite, not eliminate it entirely.
- Strategy guidelines:
 - For important assets with vulnerabilities, implement security controls to reduce likelihood.
 - If a vulnerability can be exploited, apply controls to minimise or prevent attacks.
 - When attackers' potential gain exceeds attack costs, increase the cost or reduce their gain.
 - For substantial potential loss, apply protections to limit attack impact.

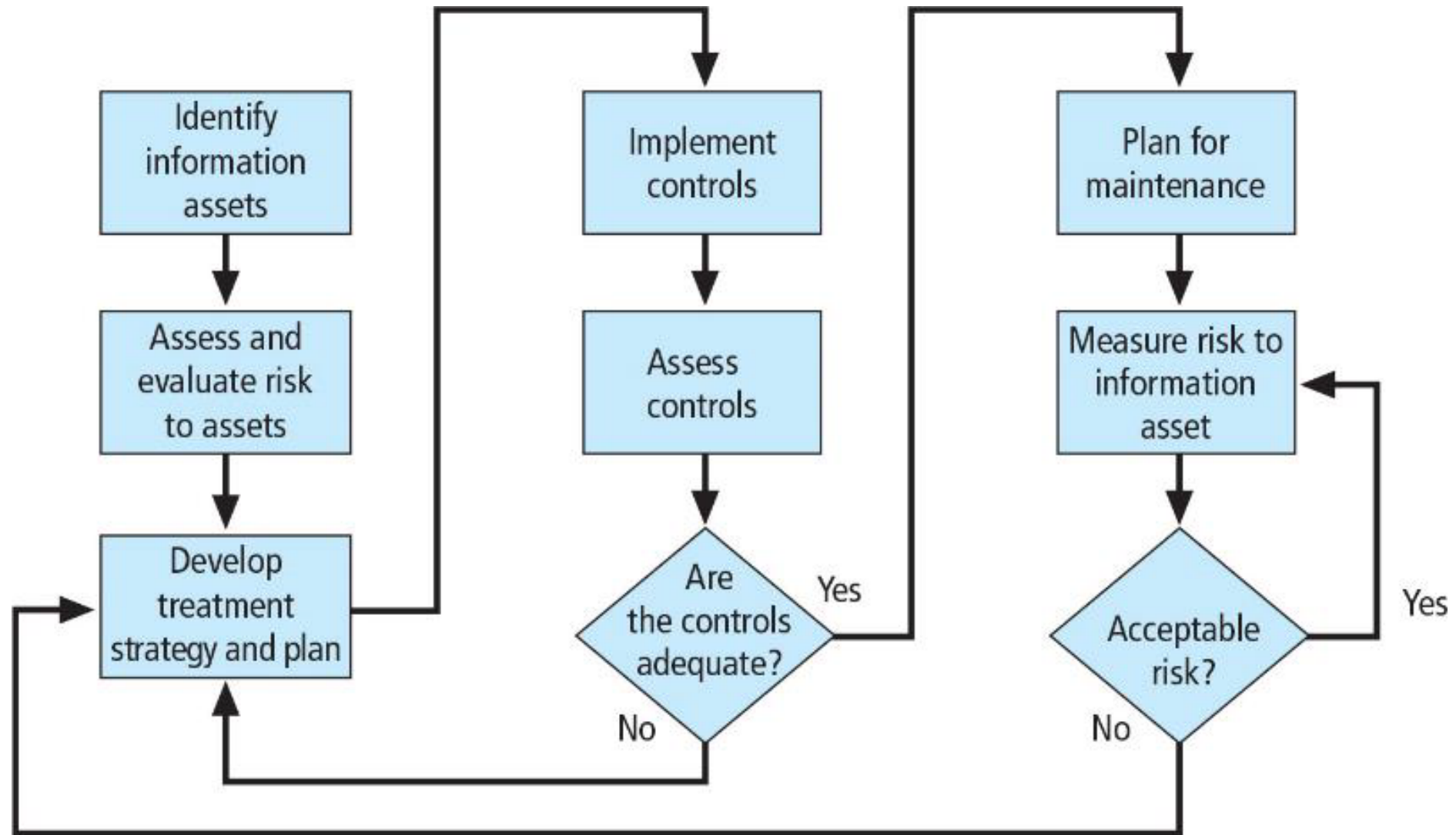
Residual Risk



Risk Treatment Cycle



Risk Treatment Cycle



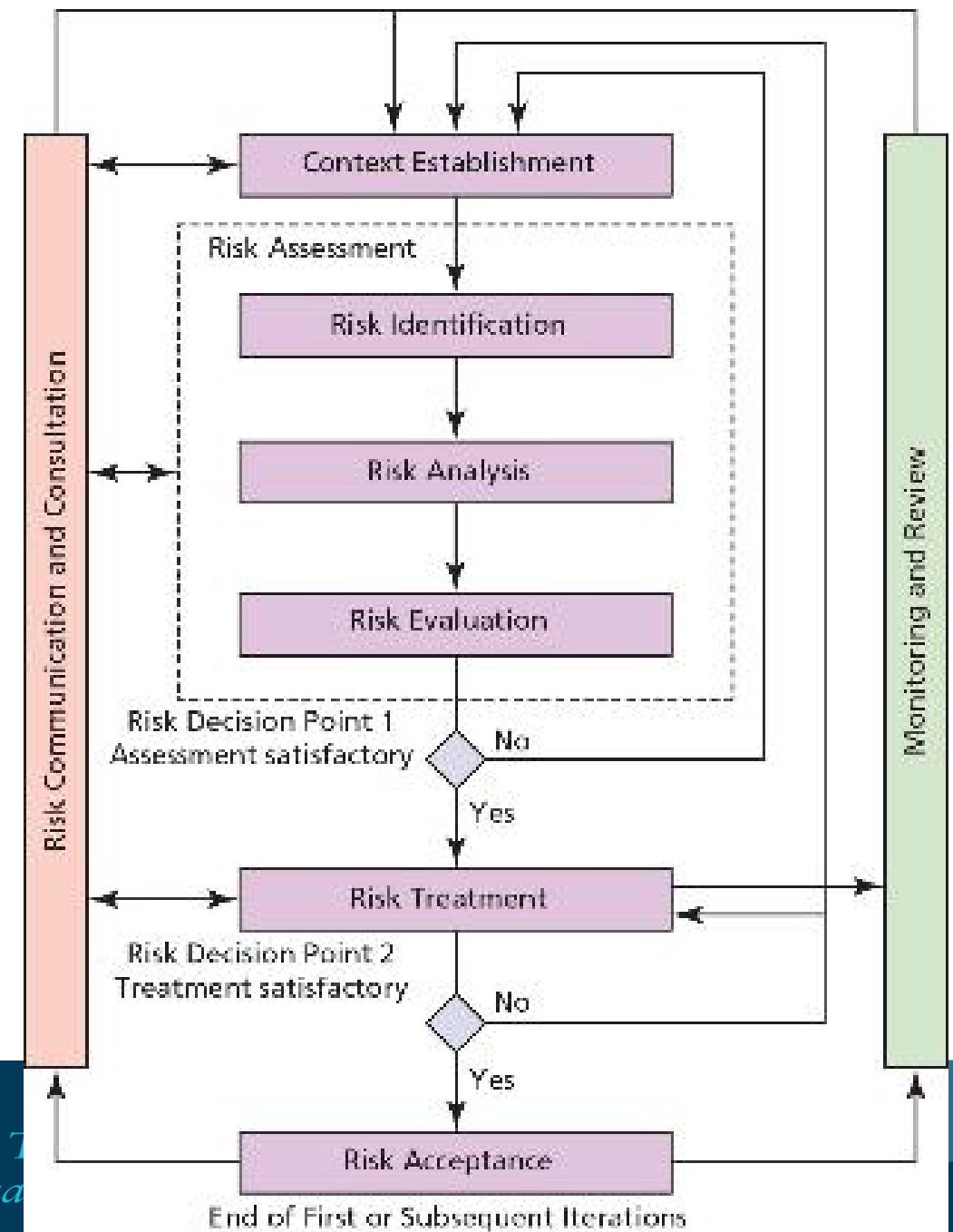
Feasibility and Cost-Benefit Analysis

- Before implementing a control strategy, the organisation must assess the potential consequences of a vulnerability.
- Factors affecting the cost of controls include development, training, implementation, service, and maintenance costs.
- **Cost-benefit analysis (CBA)** ensures that the cost of protection does not exceed the value of the asset.

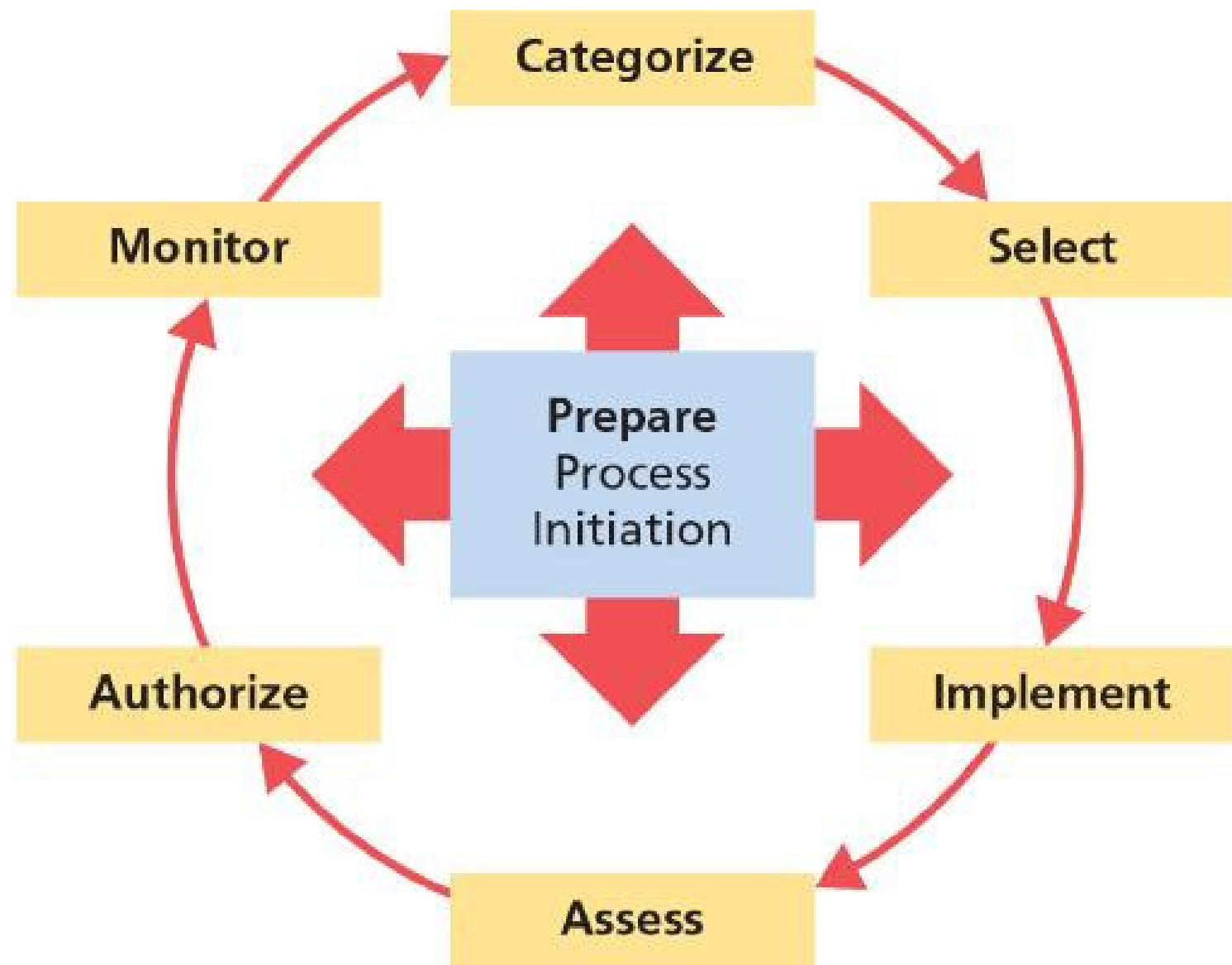
Asset Valuation

- Asset valuation estimates costs related to design, development, maintenance, protection, and recovery against loss or litigation.
- Expected loss per risk is calculated using the formula:
 - Annualised Loss Expectancy (ALE) = Single Loss Expectancy (SLE) × Annualised Rate of Occurrence (ARO)
 - SLE = Asset Value × Exposure Factor (EF)

ISO 27005 Information Security Risk Management Process



NIST RMF Framework



Selecting the Best RM Model

- Organisations without a risk management process should start by studying existing models and identifying what suits their needs.
- Some may hire consultants or develop a proprietary model.
- It's helpful to consult with other security professionals or organisations like ISSA to learn from their experiences.
- Since every organisation is unique, solutions that work for one may not work for another.

References

- Slides are devised from the recommended books:
 - Whitman, M.E., Mattord, H.J., Principles of Information Security . Cengage Learning 658.
- Some of the slides are devised from my own notes



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Any Questions?

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk