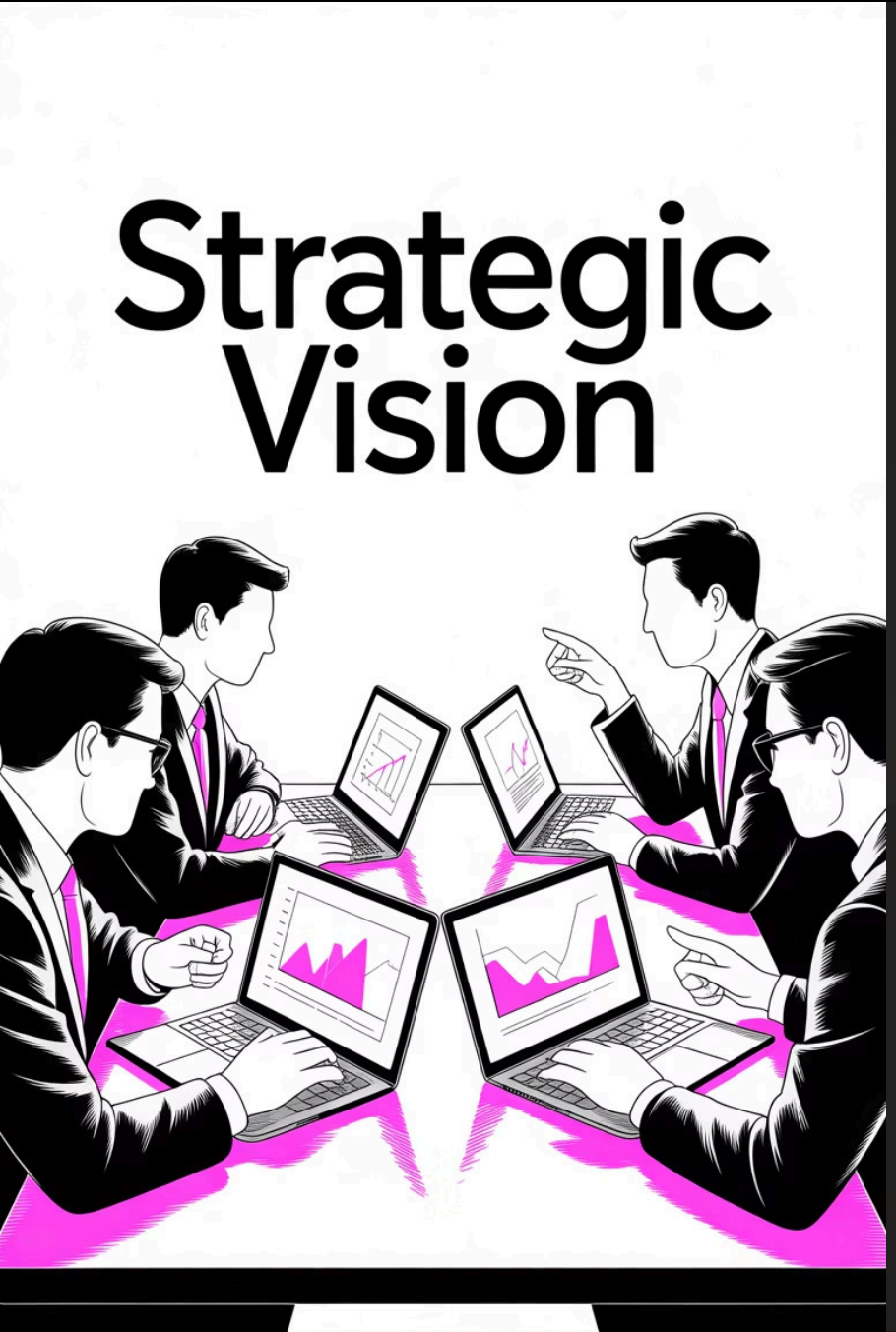


Risk Management

adapted from Dmitry Zhdanov Slides

YouTube

Risk management basics: What exactly is it?

David Hillson, The Risk Doctor, explains how to structure your risk process by asking (and answering) these six simple questions: Q1. What am I trying to achieve? (Objective...

Video Key Takeaways

1. **What are we trying to achieve?**
    a. This question leads to objective setting, understanding the scope, context, and environment for managing risk.
2. **What might affect me?**
    a. This is about risk identification, finding uncertainties that could hinder or help in achieving goals.
3. **Which of those things that might affect me are most important?**
    a. This involves risk assessment, evaluating or analyzing risks to prioritize them based on likelihood and potential impact (positive or negative).
4. **What should we do about it?**
    a. This focuses on designing responses to risks, such as avoiding or minimizing bad risks, or maximizing and exploiting good risks.
5. **Did it work?**
    a. This question assesses the effectiveness of planned actions and whether modifications are needed.
6. **What changed?**
    a. This emphasizes the dynamic nature of projects and businesses, requiring the identification of new risks that may have arisen.

Background

Decision-Making Process

Risk management is a systematic process for navigating uncertainty and making informed choices about potential threats and opportunities.

Avoiding Costly Oversights

Effective risk management prevents expensive mistakes and unexpected problems, protecting projects, reputation, and finances.

Ongoing Process

Best practices dictate that risk management is a continuous, evolving process, not a one-time activity.

Risk Management: An Overview

Risk management stands as an essential element of effective management across all industries and project types. It serves as the foundation for making informed decisions in uncertain environments.

Reduce Complexity

By breaking down complex scenarios into manageable components, risk management simplifies decision-making processes and makes overwhelming situations more approachable.

Increase Objectivity

Risk management provides structured frameworks that reduce emotional decision-making and bias, leading to more rational and consistent choices.

Identify Important Decision Factors

Through systematic analysis, risk management helps identify the critical variables that truly matter for project success and organizational goals.

The Business Case for Risk Management

In today's competitive business environment, taking calculated risks is crucial for innovation and maintaining a competitive edge. Risk management is integral to project management, enabling intelligent risk-taking while minimizing negative consequences. Effectively managing risks provides a significant competitive advantage.

The Dual Nature of Risk Management

Risk Management as a Skill

Risk management requires developed competencies in analysis, judgment, communication, and strategic thinking. These skills improve with experience and training.

Risk Management as a Task

Risk management also represents concrete activities and processes that must be completed as part of project execution and organizational operations.

The complexity of risk management varies significantly based on project scope and risk exposure. Small projects may require simple risk identification and monitoring, while large, complex initiatives demand sophisticated risk modeling and extensive mitigation strategies.

Macro-Level Example: International Banking

The Basel Committee on Banking Supervision exemplifies risk management at a global scale. Composed of government central-bank governors from around the world, this influential body demonstrates how risk management principles apply across international boundaries.

The Committee created a comprehensive, global risk management framework specifically designed to address market risk and credit risk in the banking sector. This framework serves as a model for how systematic risk management can be implemented across diverse organizations and regulatory environments.

Basel Committee Risk Management Framework

8%

Standard Capital Charge

International baseline requirement for all banks

0.37%

Minimum with Strong Controls

Reward for excellent risk management

45%

Maximum for Poor Controls

Penalty for inadequate risk management

This framework demonstrates the financial impact of risk management quality. For every $100 a bank loans, it must maintain reserves based on its risk management capabilities. Banks with superior risk mitigation procedures and controls can operate with significantly less capital tied up in reserves, improving their competitive position and profitability.

Understanding Risk Management

Key Terms

Risk

The possibility of suffering a loss due to uncertain events or conditions that could negatively impact project objectives or organizational goals.

Risk Management

The comprehensive decision-making process of identifying threats and vulnerabilities, assessing their potential impacts, and implementing appropriate responses.

Risk Assessment (Risk Analysis)

The systematic process of analyzing an environment to identify threats, vulnerabilities, and mitigating actions to determine the potential impact of events on projects, programs, or businesses.

Key Terms (Continued)

Asset

Any resource, information, system, or capability required by an organization to conduct its business operations and achieve its objectives.

Threat

Any circumstance, event, or actor with the potential to cause harm to an asset through exploitation of vulnerabilities.

Vulnerability

An inherent characteristic or weakness of an asset that can be exploited by a threat to cause harm or damage.

Impact

The actual loss or damage that occurs when a threat successfully exploits a vulnerability, resulting in negative consequences for the organization.

Additional Key Terms

Control (Countermeasure/Safeguard)

A measure, policy, or mechanism implemented to detect, prevent, or mitigate the risk associated with a threat exploiting a vulnerability.

Qualitative Risk Assessment

The process of subjectively determining the impact and likelihood of events using descriptive scales and expert judgment rather than numerical calculations.

Quantitative Risk Assessment

The process of objectively determining the impact and probability of events using mathematical models, statistical analysis, and numerical data.

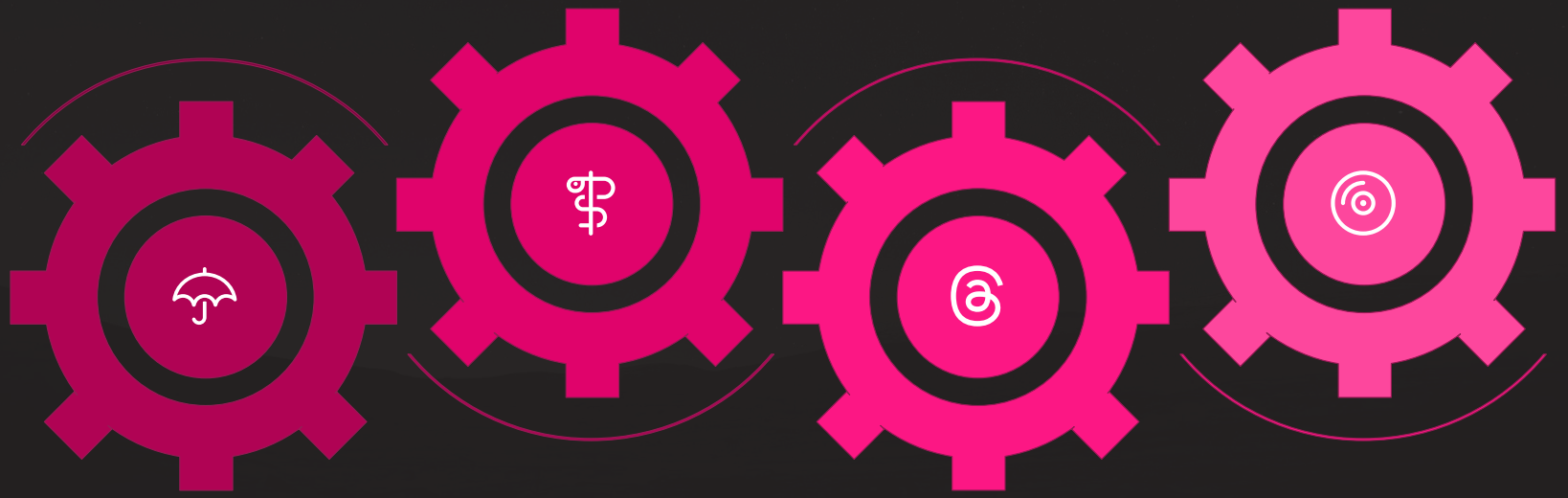
Risk Management Relationship Model

Vulnerability

Weakness that can be exploited

Impact

Resulting damage or loss



Asset

Valuable resource at the center

Threat

External danger targeting the asset

This diagram illustrates the fundamental relationships between core risk management concepts. Understanding how these elements interact is essential for effective risk identification and mitigation planning.

Advanced Risk Management Terms

Mitigation Actions

- **Mitigate:** Action taken to reduce the likelihood of a threat occurring or minimize its potential impact
- **Single Loss Expectancy (SLE):** The monetary loss or impact expected from each occurrence of a specific threat
- **Exposure Factor:** A measure of the magnitude of loss of an asset, expressed as a percentage

Frequency and Cost Metrics

- **Annualized Rate of Occurrence (ARO):** The frequency with which a specific event is expected to occur within a one-year period
- **Annualized Loss Expectancy (ALE):** The estimated cost per year of a specific risk, calculated by multiplying SLE by ARO

Defining Risk Management

> "Risk is the possibility of loss."

While this dictionary definition provides a foundation, professional organizations offer more comprehensive perspectives. Carnegie Mellon University's Software Engineering Institute (SEI) defines **continuous risk management** as a comprehensive approach involving processes, methods, and tools for managing risks throughout a project lifecycle.

Assess What Could Go Wrong

Systematically identify potential risks and failure modes

Determine Risk Importance

Prioritize risks based on likelihood and impact

Implement Risk Strategies

Deploy appropriate responses to address identified risks

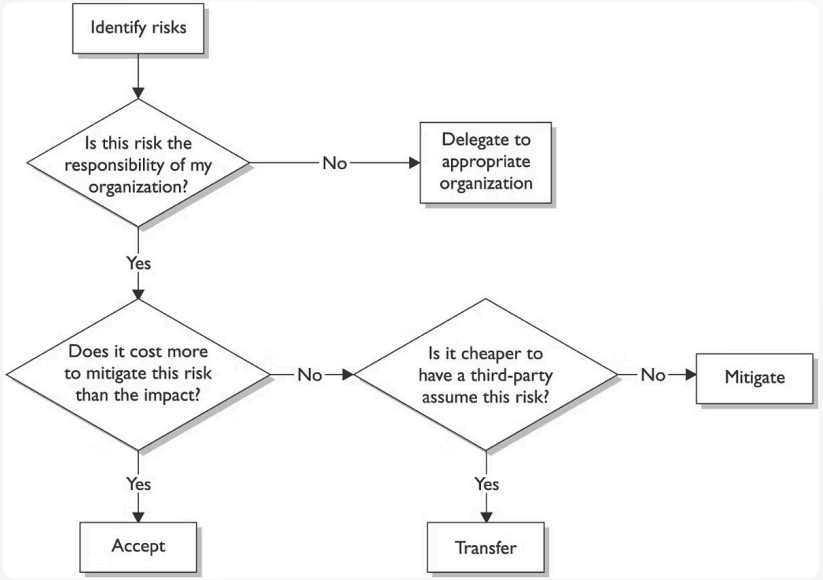
ISACA Risk Management Definition

> "In modern business terms, risk management is the process of identifying vulnerabilities and threats to an organization's resources and assets and deciding what countermeasures, if any, should be taken to reduce the level of risk to an acceptable level based on the value of the asset to the organization."

The Information Systems Audit and Control Association (ISACA) emphasizes the business-focused nature of risk management, highlighting the need to balance protection costs with asset values and acceptable risk levels.

Risk Management Decision Framework

This planning decision flowchart demonstrates the systematic approach to risk management decision-making. It shows how risk identification leads to assessment, which informs the selection of appropriate risk response strategies. The flowchart emphasizes the iterative nature of risk management and the importance of continuous monitoring and adjustment.



Business vs Technology Risk

Business Risk

Risks that directly affect business operations, strategy, and financial performance. These risks typically impact the organization's ability to achieve its business objectives.

Technology Risk

Risks associated with information technology systems, infrastructure, and processes that support business operations and enable digital capabilities.

In today's technology-dependent business environment, this distinction helps organizations structure their risk management efforts and assign appropriate expertise to different risk categories. However, these categories are increasingly interconnected as digital transformation makes technology risks business-critical.

Common Business Risks

Treasury Management

Risks related to cash flow, liquidity, foreign exchange, and financial instrument management

Revenue Management

Risks affecting income streams, pricing strategies, and market demand fluctuations

Contract Management

Risks arising from contractual obligations, vendor relationships, and legal agreements

Fraud

Risks from internal and external fraudulent activities targeting organizational assets

Environmental Risk Management

Risks related to environmental compliance, sustainability, and climate change impacts

Regulatory Risk Management

Risks from changing regulations, compliance failures, and legal penalties

Business Continuity Management

Risks that could disrupt normal business operations and service delivery

Common Technology Risks

Security and Privacy

Risks from cyber attacks, data breaches, unauthorized access, and privacy regulation violations that could compromise sensitive information.

IT Operations

Risks related to system availability, performance degradation, infrastructure failures, and service interruptions.

Business Systems Control

Risks from inadequate controls in business-critical systems, affecting accuracy, reliability, and effectiveness of operations.

Additional technology risks include business continuity management, information systems testing, reliability and performance management, IT asset management, project risk management, and change management. These risks require specialized technical expertise and often have cascading effects on business operations.

Risk Management Models

Organizations can choose from several established risk management models, each offering structured approaches to managing risk through various phases and processes.

The selection of appropriate models should align closely with business objectives, organizational culture, and strategic priorities. Different models may be more suitable for different types of projects or risk environments.

Two primary models are widely recognized: the **General Risk Management Model** and the **Software Engineering Institute Model**.

General Risk Management Model

01

Asset Identification

Systematically catalog and classify all valuable resources that require protection

02

Threat Assessment

Identify potential threats and vulnerabilities that could impact identified assets

03

Impact Definition and Quantification

Determine and measure the potential consequences of realized threats

04

Control Design and Evaluation

Develop and assess the effectiveness of risk mitigation measures

05

Residual Risk Management

Address remaining risks after implementing initial controls

Asset Identification Process

Asset identification forms the foundation of effective risk management. This critical first step requires organizations to systematically identify, catalog, and classify all assets, systems, and processes that need protection due to their vulnerability to threats.

This classification process serves multiple purposes: it helps prioritize protection efforts based on asset value and criticality, enables more accurate risk assessment, and provides a framework for evaluating the cost-effectiveness of risk mitigation measures. Without comprehensive asset identification, organizations cannot adequately protect what they don't know they have.

Types of Organizational Assets

Physical Assets

- Inventory and buildings
- Equipment and machinery
- Vehicles and facilities

Financial Assets

- Cash and cash equivalents
- Investments and securities
- Accounts receivable

Information Assets

- Information and data
- Hardware and software
- Intellectual property

Human and Intangible Assets

- Personnel and expertise
- Brand recognition
- Goodwill and reputation

Threat Assessment Fundamentals

Threats represent any circumstance or event with the potential to harm organizational assets. The threat assessment process involves identifying possible threats and vulnerabilities associated with each asset, along with evaluating the likelihood of their occurrence.

Threat Identification

Systematic identification of potential sources of harm that could exploit asset vulnerabilities

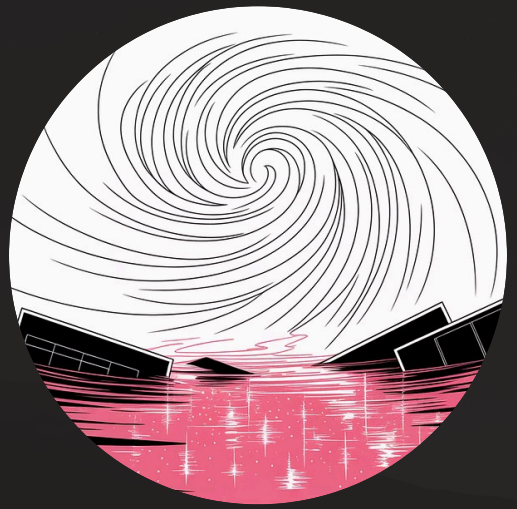
Vulnerability Analysis

Assessment of weaknesses that could be exploited by identified threats

Likelihood Assessment

Evaluation of the probability that specific threats will actually occur

Common Classes of Threats



Natural Disasters

Earthquakes, hurricanes, floods, fires, and other environmental events

Man-Made Disasters

Industrial accidents, infrastructure failures, and human-caused catastrophes

Malicious Attacks

Terrorism, cyber attacks, sabotage, and deliberate acts of harm

System and Human Failures

Equipment failures, software bugs, human errors, and operational mistakes

Understanding these threat categories helps organizations develop comprehensive threat assessment processes and implement appropriate protective measures for each type of potential harm.

Understanding Vulnerabilities

Vulnerabilities are inherent characteristics or weaknesses of resources that can be exploited by threats to cause harm. Identifying vulnerabilities is crucial for understanding how threats might successfully impact organizational assets.

- **Unprotected Facilities**

  Physical locations lacking adequate security controls, monitoring, or access restrictions

- **Unprotected Computer Systems**

  IT infrastructure without proper security configurations, patches, or monitoring capabilities

- **Unprotected Data**

  Information assets lacking encryption, access controls, or backup procedures

- **Insufficient Procedures and Controls**

  Inadequate policies, processes, or governance mechanisms to prevent or detect problems

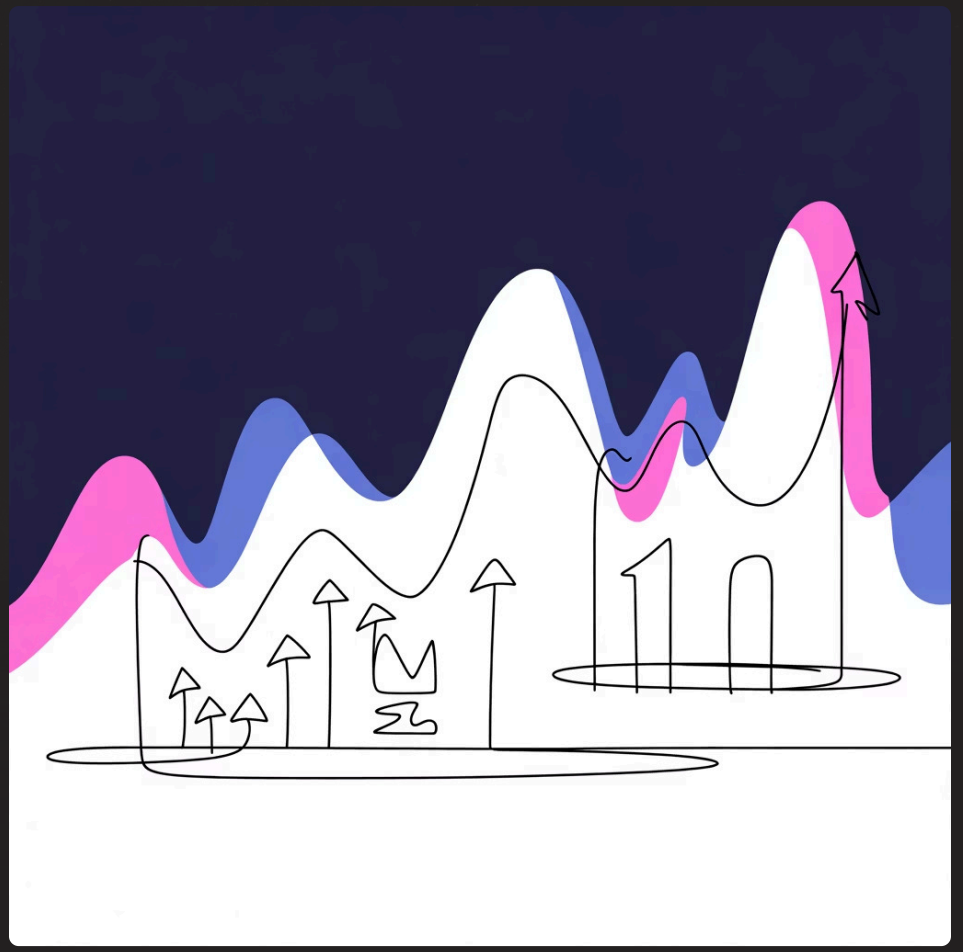
- **Personnel Deficiencies**

  Insufficient staffing levels, inadequate training, or lack of specialized expertise

Impact Definition and Quantification

When a threat successfully exploits a vulnerability, risk transforms into actual impact. Impact represents the concrete loss or damage created by the realization of a risk event.

Understanding and quantifying potential impacts is essential for making informed decisions about risk tolerance and mitigation investments. Organizations must consider both immediate and long-term consequences of risk events.



Impacts can be categorized as either tangible (measurable in concrete terms) or intangible (difficult to quantify but potentially significant). Both categories require careful consideration in comprehensive risk assessment.

Tangible Impacts

Direct Financial Loss

Immediate monetary losses including theft, damage to assets, legal settlements, regulatory fines, and emergency response costs

Safety Consequences

Endangerment of staff, customers, or the public resulting in potential injury, liability, and medical expenses

Business Opportunity Loss

Missed revenue opportunities, lost customers, failed partnerships, and competitive disadvantages

Operational Efficiency Reduction

Decreased productivity, increased costs, resource misallocation, and performance degradation

Business Activity Interruption

Service disruptions, production stops, communication failures, and supply chain interruptions

Intangible Impacts

Regulatory and Legal Breaches

Violations of legislation, regulatory requirements, industry standards, or contractual obligations that may result in legal action, penalties, or loss of operating licenses.

Reputation and Goodwill Loss

Damage to brand reputation, customer trust, market position, and organizational credibility that can have long-lasting effects on business relationships and market value.

Breach of Confidence

Loss of stakeholder trust, confidentiality violations, and relationship damage with partners, customers, employees, and investors that may be difficult to repair.

While intangible impacts are harder to quantify, they often have substantial long-term consequences that can exceed the cost of tangible impacts. Organizations should develop methods to assess and value these impacts for comprehensive risk management.

Control Design and Evaluation

Controls represent the defensive measures organizations implement to manage risk by reducing vulnerabilities to acceptable levels. These measures can take various forms including actions, devices, procedures, policies, or technologies.

Preventive Controls

Controls designed to prevent vulnerabilities from being exploited by threats, stopping potential impacts before they occur through barriers, restrictions, or protective measures.

Detective Controls

Controls that identify when a vulnerability has been exploited by a threat, enabling rapid response and minimizing damage through monitoring, alerting, and investigation capabilities.

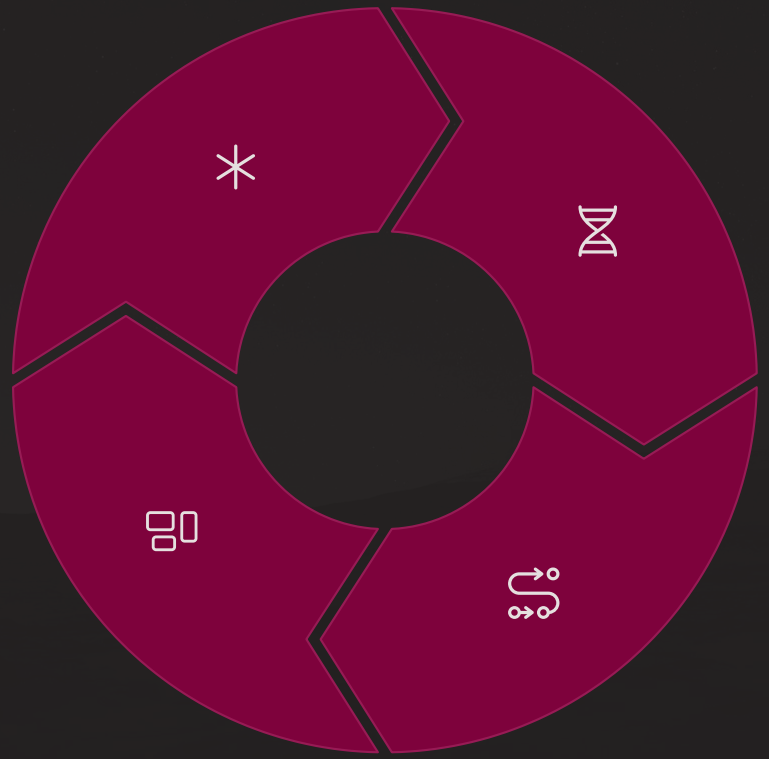
Residual Risk Management

Identify Residual Risks

Catalog risks remaining after control implementation

Evaluate Additional Controls

Assess need for supplementary risk reduction measures



Assess Control Effectiveness

Review and strengthen existing control activities

Monitor Process Changes

Track business process reengineering and organizational changes

Residual risks require ongoing attention because business process reengineering, organizational changes, and evolving threat landscapes can create new risks or weaken existing control activities. Regular reassessment ensures continued risk management effectiveness.

Software Engineering Institute Model

Identify

Proactively look for risks before they become problems that impact project success

Analyze

Convert raw risk data into actionable information for decision-making

Plan

Review and evaluate risks to decide on appropriate mitigation actions

Track

Monitor identified risks and the progress of mitigation plans

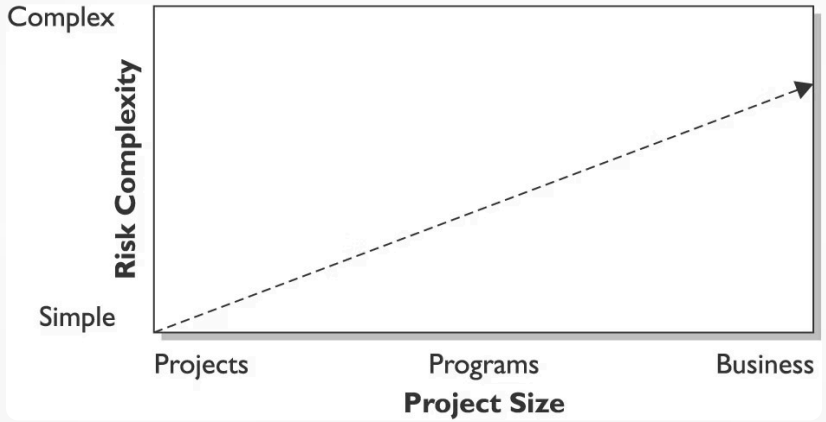
Control

Make corrections for deviations from risk mitigation plans

Risk Complexity vs Project Size

This diagram illustrates the relationship between project size and risk complexity, showing how risk management approaches must scale appropriately. Small projects may require simple risk identification and basic mitigation, while large projects demand comprehensive risk modeling and sophisticated response strategies.

Understanding this relationship helps project managers select appropriate risk management tools and allocate resources effectively based on project characteristics and risk exposure levels.



Qualitative Risk Assessment Principles

Qualitative risk assessment provides a practical approach to risk evaluation by comparing the impact of threats with their probability of occurrence using descriptive scales and expert judgment.

This methodology offers intuitive risk categorization that stakeholders can easily understand and act upon without requiring extensive mathematical analysis.

High Impact + High Probability

Results in high risk exposure requiring immediate attention and comprehensive mitigation strategies

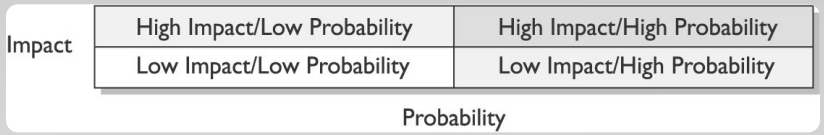
Low Impact + Low Probability

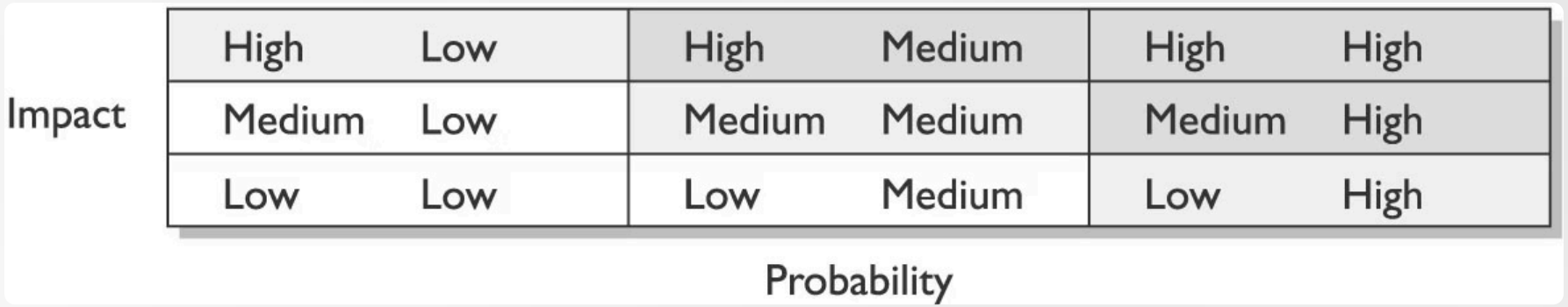
Results in low risk exposure that may be acceptable with basic monitoring procedures

Binary Risk Assessment

Binary assessment represents the simplest form of qualitative risk evaluation, using just two categories for both probability and impact. This approach provides quick risk categorization but offers limited granularity for complex decision-making scenarios.

While binary assessment is easy to understand and implement, it may oversimplify risk scenarios where more nuanced evaluation would provide better guidance for risk response planning.





Three-Level Risk Analysis

Three-level analysis expands risk evaluation to include High, Medium, and Low categories for both probability and impact dimensions. This approach provides better granularity than binary assessment while maintaining simplicity and ease of use.

The three-level system enables more nuanced risk prioritization and supports more sophisticated risk response strategies. It strikes a balance between analytical precision and practical usability for most organizational contexts.

Impact	Probability					
	Very high	Low	Very high	Medium	Very high	High
	High	Low	High	Medium	High	High
	Medium	Low	Medium	Medium	Medium	High
	Low	Low	Low	Medium	Low	High
	Very low	Low	Very low	Medium	Very low	High

Advanced Risk Assessment Matrix

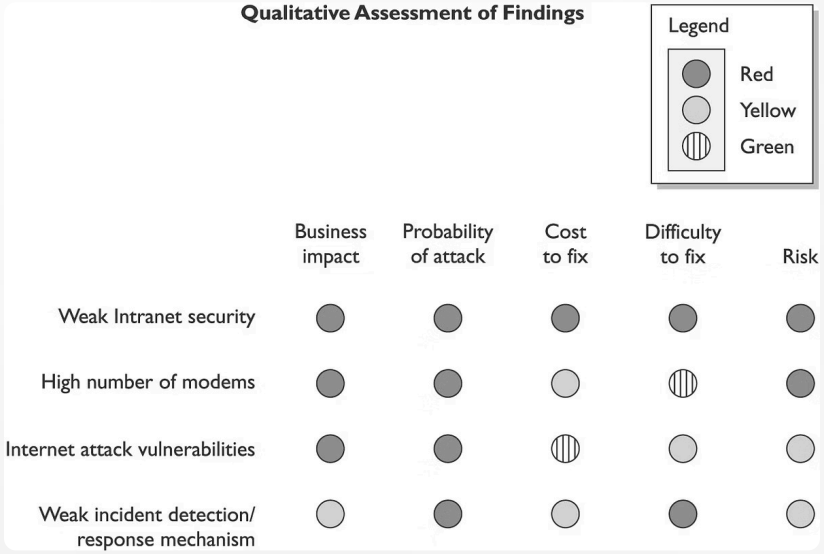
The 3x5 level analysis matrix provides enhanced granularity for risk assessment by using different scales for probability (3 levels) and impact (5 levels). This asymmetric approach recognizes that impact assessment often requires more detailed categorization than probability estimation.

This advanced matrix enables organizations to make more refined risk prioritization decisions and develop more targeted risk response strategies based on specific combinations of probability and impact levels.

Combination Risk Assessment Example

This comprehensive risk assessment matrix demonstrates how organizations can combine multiple assessment scales to create sophisticated risk evaluation frameworks. The matrix shows how different probability and impact combinations result in varying risk levels and corresponding response priorities.

Such detailed assessment matrices help organizations allocate risk management resources more effectively and ensure that high-priority risks receive appropriate attention while avoiding over-investment in lower-priority risks.



Quantitative Risk Assessment Fundamentals

Historical Data Analysis

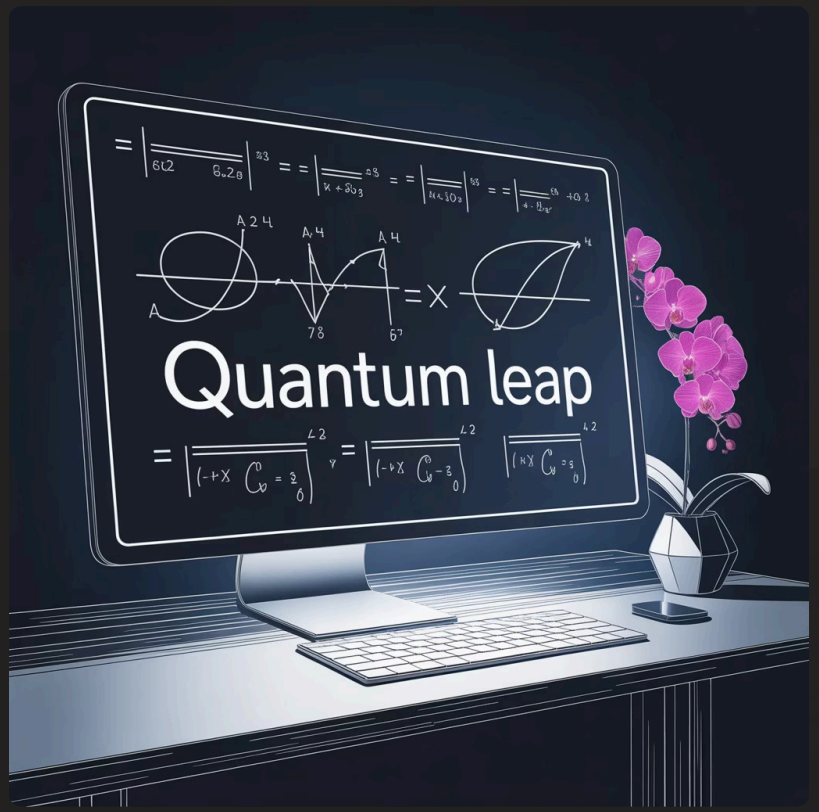
Quantitative risk assessment relies on historical information and trends to predict future performance, requiring robust data collection and analysis capabilities.

Data Collection Challenges

The effectiveness of quantitative assessment depends heavily on historical data availability, which can be difficult and expensive to gather comprehensively.

Organizations considering quantitative risk assessment must weigh the benefits of numerical precision against the costs and challenges of data collection, model development, and ongoing maintenance of quantitative risk management systems.

Quantitative Risk Models



Quantitative risk assessment often relies on sophisticated mathematical and statistical models to provide decision-making information in the form of quantitative metrics.

These models attempt to measure risk levels across a common scale, enabling direct comparison between different types of risks and facilitating more objective prioritization decisions.

Model-based approaches support data-driven decision-making and can provide detailed cost-benefit analysis for risk mitigation investments.

Limitations of Quantitative Models

Model Assumptions

Key assumptions underlie any quantitative model, and these assumptions may not accurately reflect real-world conditions or may become invalid over time.

Varying Results

Different quantitative models can produce significantly different results even when using identical input data, highlighting the importance of model selection.

Need for Expertise

Despite advances in risk analysis models, professional expertise and experience remain essential for effective risk assessment and decision-making.

Models should enhance rather than replace human judgment and experience in the decision-making process. The most effective risk management combines quantitative analysis with qualitative insights and professional expertise.

Impact	Explanation	Weight
Business impact	If exploited, would this have a material business impact?	4
Probability of attack	How likely is a potential attacker to try this technique or attack?	3
Cost to fix	How much will it cost in dollars and resources to correct this vulnerability?	2
Difficulty to fix	How hard is this to fix from a technical standpoint?	1

Adding Objectivity to Qualitative Assessment

This framework demonstrates how organizations can enhance qualitative risk assessments by adding weights and specific definitions to potential impact categories. By assigning numerical values to qualitative categories, organizations can maintain the intuitive nature of qualitative assessment while gaining some benefits of quantitative analysis.

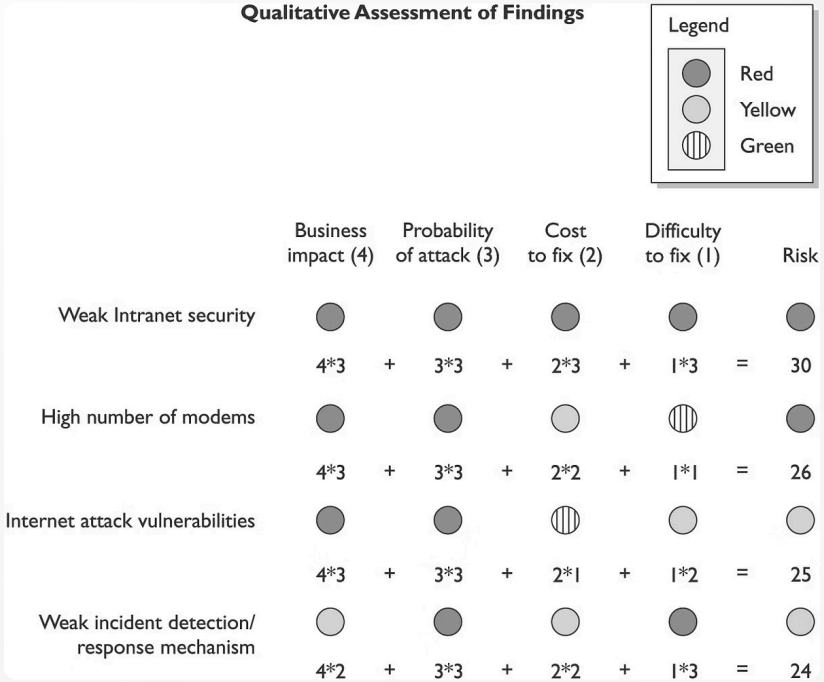
The weighted approach enables more consistent risk evaluation across different assessors and time periods while preserving the accessibility and understandability of qualitative methods.

Values-Based Assessment Approach

This assessment framework shows how organizations can add numerical values to qualitative assessments, creating a hybrid approach that combines the benefits of both methodologies. The value assignments enable mathematical calculations while maintaining the conceptual simplicity of qualitative categories.

This approach supports more sophisticated risk analysis, including risk scoring, prioritization algorithms, and trend analysis, while remaining accessible to non-technical stakeholders.

Assessment	Explanation	Value
Red	Many critical, unresolved issues	3
Yellow	Some critical, unresolved issues	2
Green	Few unresolved issues	1



Final Quantitative Assessment

This comprehensive assessment matrix represents the culmination of a structured risk evaluation process, showing how individual risk assessments can be synthesized into an overall risk profile for decision-making purposes.

The final quantitative assessment provides a foundation for risk-based decision-making, resource allocation, and strategic planning by presenting risk information in a format that supports comparison and prioritization across diverse risk categories.

Annualized Loss Expectancy Calculation

More complex quantitative models enable sophisticated analyses based on statistical and mathematical approaches. A widely-used method is the calculation of Annualized Loss Expectancy (ALE), which provides a standardized way to express risk in financial terms.

Single Loss Expectancy (SLE)

SLE = Asset Value × Exposure Factor

This formula calculates the expected monetary loss for each occurrence of a specific threat against an asset.

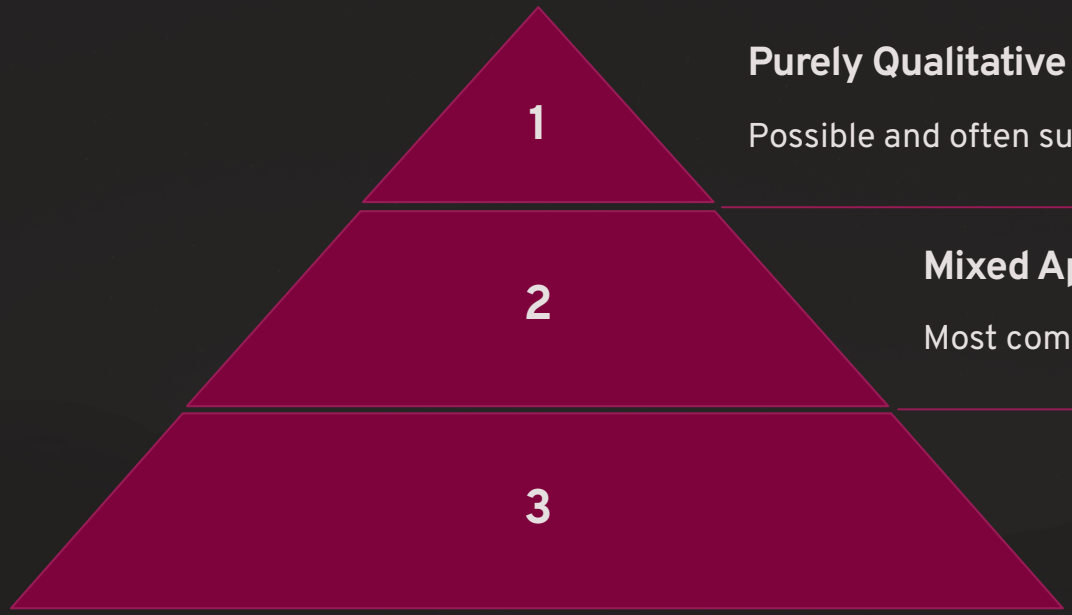
Annualized Loss Expectancy (ALE)

ALE = SLE × ARO

This calculation multiplies the single loss expectancy by the annualized rate of occurrence to determine annual expected losses.

These calculations enable organizations to express risks in financial terms, facilitating cost-benefit analysis for risk mitigation investments and supporting data-driven risk management decisions.

Qualitative versus Quantitative Approaches



Purely Qualitative

Possible and often sufficient

Mixed Approach

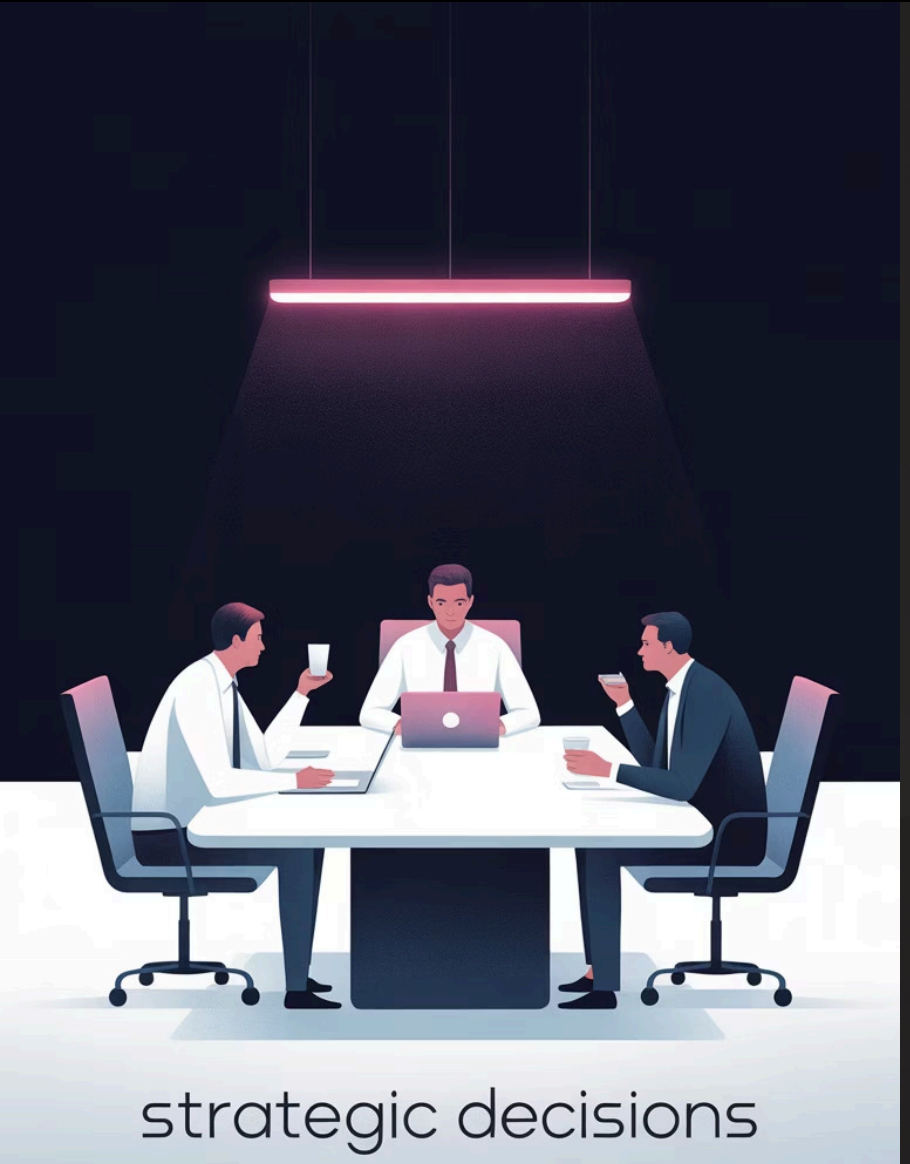
Most common in practice

Purely Quantitative

Impossible in most contexts

It is impossible to conduct risk management that is purely quantitative because risk assessment always involves some degree of judgment, assumption, and subjective evaluation. Most effective risk management programs combine both qualitative and quantitative elements, requiring analysis, professional judgment, and experience.

Organizations can successfully implement purely qualitative risk management, but the most sophisticated approaches typically integrate both methodologies to maximize effectiveness.



Choosing Assessment Approaches

The decision to use qualitative versus quantitative risk management approaches depends on several critical factors that organizations must carefully evaluate based on their specific circumstances and objectives.

Project Criticality

High-stakes projects may justify the additional investment in quantitative analysis methods

Available Resources

Quantitative approaches require more time, expertise, and financial resources than qualitative methods

Management Style

Organizational culture and leadership preferences influence the adoption of different analytical approaches

The final decision is also influenced by the degree to which fundamental risk management metrics can be quantitatively defined and the availability of reliable historical data for analysis.

Essential Risk Management Tools

Affinity Grouping

A systematic method for identifying related items and then determining the underlying principle that ties them together into coherent groups for analysis.

Baseline Identification and Analysis

The process of establishing a baseline set of risks, creating a comprehensive "snapshot" of all identified risks at a specific point in time for comparison purposes.

Cause and Effect Analysis

A systematic approach to identifying relationships between specific risks and the various factors that can cause or contribute to their occurrence.

Advanced Risk Management Tools

Cost/Benefit Analysis

A structured method for comparing cost estimates with the expected benefits of risk mitigation strategies to optimize resource allocation and investment decisions.

Gantt Charts

A visual management tool for diagramming project schedules, events, and activity duration, particularly useful for tracking risk mitigation implementation timelines.

Interrelationship Digraphs

An analytical method for identifying cause-and-effect relationships by systematically defining problems, identifying key elements, and describing their complex interrelationships.

Comprehensive Planning Tools

PERT Charts

Program Evaluation and Review Technique (PERT) charts provide detailed diagrams depicting interdependencies between project activities, showing the sequence and duration of each activity for comprehensive project risk planning.

Risk Management Plan

A comprehensive planning document that systematically documents how risks will be identified, assessed, monitored, and managed throughout a given project lifecycle, serving as the central reference for all risk management activities.

These tools provide the foundation for implementing systematic, professional risk management practices. Organizations should select tools that align with their risk management maturity level, project complexity, and available resources to maximize effectiveness while maintaining practical usability.