Risk Management - Supply Chain and Operations Perspective

RISK MANAGEMENT - SUPPLY CHAIN AND OPERATIONS PERSPECTIVE

AZIM ABBAS AND LARRY WATSON

Fanshawe College Pressbooks
London, Ontario

CONTENTS

Chapter 4: Identifying Risks

Chapter 5: Risk Analysis

Chapter 6: Risk Response and Risk Treatment

Chapter 7: Risk Monitoring

Chapter 8: Risk Management in Supply Chain and Operations Management

Chapter 9: Emerging Trends in Risk Management

Chapter 10: Risk Management from a Sustainability Perspective

ACKNOWLEDGEMENTS

This open textbook has been written by Azim Abbas & Larry Watson in partnership with the OER Design Studio and the Library Learning Commons at Fanshawe College in London, Ontario.

Cover Image was initially created in Pikaso and then modified by Sanaz Habibi.

Freepik. (2024). *Pikaso* [AI Image Generator]. https://www.freepik.com/pikaso/ai-image-generator

Prompt: Design a comprehensive guide on risk management, specifically focusing on supply chain and operations management. The cover should visually convey the interconnectedness of global supply chain elements, using a blend of colours and icons to highlight key areas like transportation, logistics, and infrastructure. The title should be bold and clear, with the subtitle offering additional context on the perspective of the book. The overall design should be modern, engaging, and informative, appealing to professionals and students in the field.

Collaborators

- Stephany Ceron Salas, *Instructional Design Student*
- Elisha Girard, Ancillary Resource Developer
- Sanaz Habibi, *Graphic Design Student*
- Wilson Poulter, *Copyright Officer*
- Catherine Steeves, *Instructional Design & Quality Assurance*
- Shauna Roch, *Project Lead*

ABOUT THIS BOOK

In this book, students will explore the critical field of risk management from the lens of supply chain and operations management. The chapters cover a broad spectrum of topics, starting with an insightful introduction to risk management, risk classification, the framework, and the process involved in managing risks. From identifying risks to conducting rigorous risk analyses, the book equips students with practical tools and strategies.

The second part of this book focuses on risk treatment, monitoring, and the unique challenges faced in the contexts of supply chains and operations while exploring emerging trends in risk management and sustainability as a crucial aspect of risk mitigation. For students, particularly from the supply chain & operations, this book provides valuable insights to enhance their risk management expertise.

Author Biographies

Azim Abbas, MSc (Engineering), MBA, BSc (Hons) Grad Cert SCM

Azim Abbas is a seasoned Supply Chain and Operations Management professional with extensive experience in academia and industry. He currently serves as a full-time faculty member at Fanshawe College as a Coordinator of the Operations Management program. Azim has held significant roles in various organizations, and his extensive professional experience spans significant roles in the aviation and maritime industries, where he managed global logistics and operations. His academic credentials include an MSc in Advanced Manufacturing Systems and Technology from the University of Liverpool and an MBA. Azim's diverse background and expertise make him a valuable contributor to the field of supply chain and operations management.

Larry Watson, CRM/CIP

Larry Watson is a seasoned risk management and insurance professional with a career spanning over four decades. He began his journey in 1977 as a physical risk inspector and concluded it as the Director of Loss Prevention National Solutions at Canada's largest insurance company. Larry possesses expert risk assessment, fire protection, crime, and liability knowledge. He has presented numerous seminars on loss prevention to insurers, insurance brokers, industry professionals, and municipal fire services across Canada. His insights have been published in national trade and insurance magazines. With over 30 years of teaching experience, Larry has educated students in risk and insurance at Fanshawe College, Western University, and the Insurance Institute of Ontario. He continues to teach risk management and insurance at Fanshawe College in the Insurance and Risk Management Graduate and Insurance Diploma programs, as well as in the supply chain and operations stream.

Feedback

Please share your adoption and any feedback you have about the book with us at oer@fanshawec.ca

Accessibility Statement

We are actively committed to increasing the accessibility and usability of the textbooks we produce. Every attempt has been made to make this OER accessible to all learners and is compatible with assistive and adaptive technologies. We have attempted to provide closed captions, alternative text, or multiple formats for on-screen and offline access.

The web version of this resource has been designed to meet Web Content Accessibility Guidelines 2.0, level AA. In addition, it follows all guidelines in Appendix A: Checklist for Accessibility of the *Accessibility Toolkit – 2nd Edition*.

In addition to the web version, additional files are available in a number of file formats, including PDF, EPUB (for eReaders), and MOBI (for Kindles).

If you are having problems accessing this resource, please contact us at oer@fanshawec.ca.

Please include the following information:

- The location of the problem by providing a web address or page description
- A description of the problem
- The computer, software, browser, and any assistive technology you are using that can help us diagnose and solve your issue (e.g., Windows 10, Google Chrome (Version 65.0.3325.181), NVDA screen reader)

CHAPTER 1: INTRODUCTION TO RISK MANAGEMENT

Chapter Overview

1.0 LEARNING OUTCOMES

Learning Objectives

At the end of this chapter, students will be able to:

- Define traditional and modern risk as they apply to the study of Risk Management.
- Outline the progression of Risk Management from Traditional to Enterprise Risk Management.
- Describe the benefits provided by Risk Management for an organization and the economy.
- Explain the importance of Basic Risk Measures on organizations.

1.1 WHAT IS RISK?

Risk is defined according to its context. Most would view risk as being negative; "I took the risk of being late for work by leaving home late." Insurance is based on the premise that risk can or will cause losses, and as a result, defines risk in negative but simple terms, which is the chance of loss. For insurance to exist, there must be insurable risks. Examples of insurable risks are risks associated with property, liability and personnel. Note that **insurable risks** are hazard risks, which in turn are considered to be pure risks comprised of property, liability and personnel risks.

- **Property Risks** are losses arising from the destruction or damage to property. An example would be a house fire.
- **Liability Risks** are losses associated with the legal obligation requiring an individual to pay damages to others as a result of that person's negligence. An example would be the manufacturing of a product that causes injury to a consumer.
- **Personnel Risks** are losses associated with bodily injury, loss of life or income resulting from death or disability.

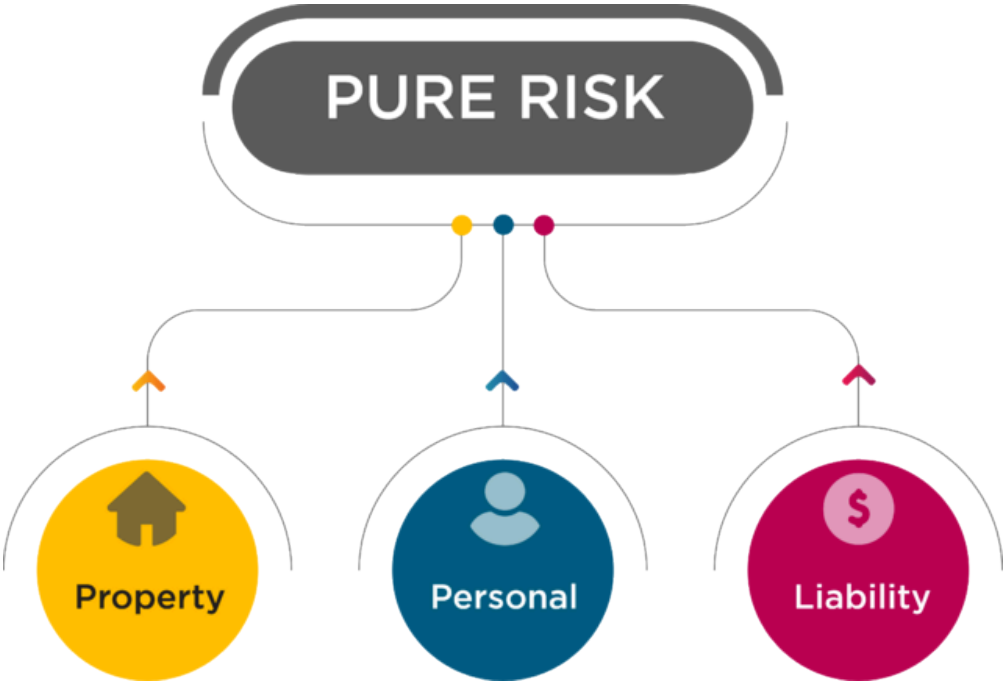

Figure 1.1.1. "Pure Risk" by Sanaz Habibi, CC BY-NC-SA 4.0

Definitions of risk in the modern risk management space include using the term uncertainty as it applies to outcomes. ISO 31000 defines **risk** as "the effect of uncertainty on objectives, whether positive or negative" (International Organization for Standardization, 2022). Risk, therefore, can have an upside and a downside. The **upside of risk** means that the risk can be a benefit to the organization, meaning that the risk is an advantage. In contrast, the **downside of risk** does not work in the organization's favour, and the risk is a disadvantage. International students arriving in Canada to attend Fanshawe College are exposed to risk. The upside of risk in this case is that they will experience life in Canada, meet new friends, enjoy success at school, and go on to a successful career. The downside of risk in this case is that students could have trouble adjusting to the climate, experience separation anxiety, face financial pressures, and struggle with the curriculum at school.

This book will consider risks to be multi-directional, meaning that they have an upside and a downside. The only exception will be hazard risks, which have downsides.

1.2 THE PRACTICE OF RISK MANAGEMENT

Risk management is the process of assessing, treating and monitoring all of an organization's risks in order to minimize their adverse effects on the organization.

The practice of Risk Management has gone through two major changes since its inception to keep pace with the evolution of risk and the fact that yesterday's practices are not able to address the threats of today. Although the management of risks has occurred throughout history, Traditional Risk Management was practiced as a science after World War II and continued in its original form until the mid-1950s. Traditional Risk Management, formally described as just risk management, has long been associated with only hazard risks, which are the subject of insurance based on accidental losses; that is, losses that are not intentional. **Hazard risk** is pure risk, meaning that the outcome is one of loss, no loss, but no gains can be realized. In comparison, **speculative risk,** which is not the subject of insurance, involves a chance of loss, no loss but the realization of a gain. The following statement is important to understanding hazard risk and its connection to insurance:

Pure Risk is Hazard Risk...Hazard Risk is an Insurable Risk

The next major step in the evolution of risk management was the introduction of Enterprise Risk Management, which emerged during the 1990s as an approach to address all an organization's risks. Enterprise Risk Management gained a lot of traction between the years 2000 and 2010, especially during and after the financial debacles occurring in 2007-2008.

Enterprise Risk Management (ERM) is a holistic approach to risk management, meaning there is a broader understanding of how all the risks affect the organization. **Traditional Risk Management** places individual risks into silos; **Enterprise Risk Management** views risks as being interrelated and, in a sense, wraps its arms around all the organization's risks allowing the risks to communicate with others.

Where Traditional Risk Management focuses only on hazard risk, Enterprise Risk Management focuses on all the categories of risk which include hazard, operational, financial, and strategic risks (HOFS). Included in these

four categories of risks are business risks, which are speculative in nature as they can result in a loss, no loss, but a gain can be realized.

Enterprise Risk Management or Enterprise-Wide Risk Management is an organizational approach to managing all key business risks and opportunities to maximize the potential of an organization to achieve its objectives.

Differences between Enterprise Risk Management (ERM) and Traditional Risk Management:

- ERM focuses on all of the organization's risks (hazard and business risks). Traditional Risk Management focuses only on Hazard Risks.
- ERM helps an organization maximize its productive potential. Traditional Risk Management restores an organization to its pre-loss condition prior to the occurrence of a negative event.
- ERM focuses on the worth of the organization. Traditional Risk Management focuses on the cost of the accidental loss.
- ERM focuses on the entire organization. Traditional Risk Management can be practiced separately or as a component of enterprise risk management.
- ERM focuses on a balance between the upside and downside of risk and can be applied to all organizations. Traditional Risk Management focuses on the downside of risk and can be applied to safeguard an organization against the adverse effects of insurable risk.

The focus of this course will be on the Enterprise Risk Management approach.

It is important to note that Enterprise Risk Management concepts, elements and techniques are applicable to all organizations regardless of size. They can be used by multinational organizations spanning the globe or by sole proprietors operating in much smaller environments; it is a matter of the size and scale of the risk management offering. Larger organizations will very likely have dedicated risk management departments consisting of risk officers, risk managers, loss control specialists, legal teams, and an insurance team.

Roles in Risk Management

- **Risk officer**: an individual with direct authority over the risk management team and reports to senior management.
- **Risk manager**: an individual who oversees the risk management process in the organization to protect its assets.
- **Loss control specialist:** an individual who has the expertise to perform physical risk inspections within the organization to identify risk and to make recommendations to minimize the frequency or severity of risk.
- **Legal team:** an individual who performs legal functions as lawyers, legal experts, or legal specialists in the organization.
- **Insurance team:** an individual with an insurance background who has the expertise to negotiate insurance contracts and manage claim settlements.

In a smaller organization, the responsibilities for risk management are often placed on top of the daily activities of individuals associated with operating the business.

1.3 BENEFITS OF RISK MANAGEMENT

All organizations operate in a world filled with risk. The practice of effective risk management will not only provide benefits to individual organizations but also to the economy.

Consider an established manufacturing plant in a small town in Ontario, Canada, employing most of the town's population. The local economy is advantageously affected by the continued success of the manufacturing plant as residents have mortgages, loans and income to spend, all dependent on the viability of the plant. Now consider a scenario where a fire causes the plant to shut down for an extended period, resulting in a decision to delay the re-opening, move it to another location or keep it permanently closed. This disruption to the economy creates systemic risk within this market as the loss of income to residents will prevent them from making good on loans, mortgages, and debts. A spin-off effect caused by the lack of revenue generated by local businesses after the fire may force these businesses to close.

Benefits of Risk Management for Organizations

- *Managing Cost of Risk*. Cost of risk is the total cost incurred by an organization because of the possibility of accidental losses. These could be costs associated with accidental losses not covered by insurance or other outside sources. Cost of risk also includes loss prevention activities (employee training), loss reduction activities(sprinkler systems) or the cost of administering risk management activities.
- *Reducing Uncertainty*. A risk adverse organization may be reluctant to undertake activities that are too risky, depriving the organization of potential benefits. The downside of risk cannot be eliminated, but its uncertainty can be managed by implementing strategies. Risk management can reduce the uncertainty of undertaking activities, which can increase profit and attract investors by making the company more attractive to suppliers of investment income.
- *Informed Risk Taking*. Opportunities based on the organization's risk appetite should be recognized and selected. The risk of pursuing the opportunity should be compared to the risk of not taking the opportunity, always keeping in mind the concept of risk versus reward.
- *Profitability.* Effective risk management can help the organization evaluate the risks and their potential returns while keeping within the boundaries of the organization's objectives and risk appetite.
- *Integrated Risk Management*. The implementation of Enterprise Risk Management will result in better decision-making and improved outcomes by providing the organization with a complete picture of its

risks and how one risk can impact another risk.

- *Regulatory Compliance.* Adherence to regulatory and compliance risks associated with laws and reporting requirements will allow auditors to report on an organization's risk management processes in support of mandatory obligations.

Benefits of Risk Management for the Economy

- *Minimizing Systemic Risks.* The inability to implement effective risk management by an organization can result in a failure not only for the organization but for the economy itself, as described in the opening paragraph of this section.
- *Retaining Resources.* An accidental loss such as a natural disaster or a fire could adversely affect quantities of available resources and, subsequently, an organization's ability to manufacture products. Allocating resources to risk management is a cost that could minimize the effects on or loss of productive resources.
- *Reducing Economic Resources*. The implementation of effective risk management will relieve the burden of uncertainty placed on an organization and the effects of its failures on the economy caused by the downside of risk. This will allow the organization to freely pursue activities intended to maximize profits, wages and return on investments.

1.4 BASIC RISK MEASURES

Successful risk management involves identifying and analyzing risks. The identification and analysis of risks is collectively referred to as a **risk assessment**. For an organization to meet its objectives, it must be able to measure its risks so that it can take steps to improve them. Activities such as benchmarking risks by looking at a comparison of industry averages or risk scoring by calculating a number based on criteria to determine the level of risk are techniques commonly used by organizations to measure risk.

There are six basic measures that apply to risk management: exposure, volatility, likelihood, frequency and severity.

Figure 1.4.1: *"Six Basic Measures of Risk Management"* by Sanaz Habib, CC BY-NC-SA 4.0

Exposure

This is a term that can mean many things depending on the context in which it is being used. In risk

management it refers to the level of risk faced by an organization that exists even in the absence of an actual loss with respect to gains or losses. Exposure provides a measure of the potential damage associated with an occurrence. The level of risk increases as the exposure increases. For example, drivers who are on the road 12 hours per day increase their exposure to having an accident significantly more than drivers who are on the road only 1 hour per day. Most risks are quantifiable, but there are many risks that are not easily quantifiable. For example, the reputational risk of an organization might have to be measured by assessing sales after a negative event which affects the organization. Exposure to risk can be calculated using a simple formula:

Risk Exposure = Probability of the Loss × Amount in dollars of a Total Loss

Example

Consider a building with a value of $2,000,000. Fire is a peril that has a low frequency but a high impact, so the probability can be estimated to be .04%. The risk exposure for the building with respect to fire is $80,000.00 (.04% × $2,000,000)

Volatility

This is a term applied to frequent fluctuations in the price of an asset. An increase in risk is directly proportional to an increase in volatility. The volatility of the stock market, commodity prices, and retail pricing can almost always be measured or quantified.

Likelihood

This is a key term that is used to measure the probability or frequency of an event occurring. The ability to calculate the likelihood of an event mathematically occurring is key to an insurance company's success and to the ability to respond to risk by the risk management team in an organization. The likelihood of a risk occurring is addressed by loss prevention techniques. **Loss prevention** is a loss control technique that consists

of measures that are taken before a loss occurs in an attempt to stop the loss from occurring. Employee training, reducing speed limits, and installing solid security locks on doors are all examples of loss prevention.

Consequences

This is a key term that is used to describe the impact or severity of an event that has occurred. The consequences involving the aftermath of an event that has occurred are addressed by loss reduction. The installation of an automatic sprinkler system, burglar alarms and emergency preparedness are examples of loss reduction. Loss reduction is comprised of pre-loss measures (before a loss occurs) and post-loss measures (after a loss occurs).

The Relationship Between Frequency And Severity

There is a relationship between the frequency and severity of losses, the responses by risk management and how they apply to hazard risks. The risk response to a hazard risk that is low frequency and high severity (fire) will be different than the risk response to a hazard risk that is low frequency and low severity (minor vandalism to a building).

- *Time Horizon*. Lengthy-time horizons pose more risk than shorter-time horizons because the potential for risk is in play for a longer period. It is sometimes difficult to manage the duration of time that an organization is exposed to a risk, but attempts to manage its uncertainty should be made as with any other risk.
- *Correlation*. If two or more risks are associated or similar, they are correlated. Highly correlated risks are subject to a high level of risk. A manufacturer's supply chain would be highly correlated if it relies on key suppliers who are all located in a region that is subject to the same geopolitical risk.

1.5 CHAPTER SUMMARY

Summary

This chapter introduced the concept of risk management, emphasizing that risk is often seen negatively as the chance of loss but also includes potential positive outcomes. Traditional risk management has historically focused on hazard risks—those associated with property, liability, and personnel—which are purely negative and insurable. In contrast, modern definitions, such as those from ISO 31000, consider risk as the effect of uncertainty on objectives, acknowledging that risks can have upsides and downsides. Enterprise Risk Management (ERM) emerged in the 1990s as a holistic approach that encompasses all types of risks (hazard, operational, financial, and strategic) and views them as interrelated, aiming to maximize shareholder value and manage risks to optimize the organization's overall performance.

The chapter also discussed the evolution of risk management practices and the benefits of effective risk management for organizations and the broader economy. ERM enables organizations to manage risks comprehensively, facilitating better decision-making and improved outcomes. It helps reduce the cost and deterrence effects of hazard risks, manage the downside of risks, and take intelligent risks that maximize profitability. The practice also ensures compliance with legal and regulatory requirements. Effective risk management can minimize resource wastage, improve the allocation of productive resources, and reduce systemic risks, thereby supporting organizational stability and economic health. Basic risk measures such as exposure, volatility, likelihood, and consequences are crucial for identifying and analyzing risks, collectively forming the foundation for successful risk management.

OpenAI. (2024, May 24). *ChatGPT.* [Large language model]. https://chat.openai.com/chat

Prompt: *Please take the chapter content in this document attached and summarize the key concepts into no more than two paragraphs. Reviewed by authors.*

Key Terms

- **Consequences** is a key term that is used to describe the impact or severity of an event that has occurred.
- **Downside of Risk** does not work in the organization's favour, and the risk is a disadvantage.
- **Enterprise Risk Management** views risks as being interrelated and, in a sense, wraps its arms around all the organization's risks, allowing the risks to communicate with others.
- **Exposure** refers to the level of risk faced by an organization that exists even in the absence of an actual loss with respect to gains or losses.
- **Hazard Risk** is pure risk, meaning that the outcome is one of loss, no loss, but no gains can be realized.
- **Insurable Risks** are hazard risks, which in turn are considered to be pure risks comprised of property, liability and personnel risks.
- **Insurance Team:** an individual with an insurance background who has the expertise to negotiate insurance contracts and manage claim settlements.
- **Legal Team:** an individual who performs legal functions as lawyers, legal experts, or legal specialists in the organization.
- **Liability Risks** are losses associated with the legal obligation requiring an individual to pay damages to others as a result of that person's negligence.
- **Likelihood** is a key term that is used to measure the probability or frequency of an event occurring.
- **Loss Control Specialist:** an individual who has the expertise to perform physical risk inspections within the organization to identify risk and to make recommendations to minimize the frequency or severity of risk.
- **Loss Reduction** is comprised of pre-loss measures (before a loss occurs) and post-loss

measures (after a loss occurs).

- **Personnel Risks** are losses associated with bodily injury, loss of life or income resulting from death or disability.
- **Property Risks** are losses arising from the destruction or damage to property.
- **Risk Assessment** is collectively referred to as the identification and analysis of risks.
- **Risk** ISO 31000 defines it as "the effect of uncertainty on objectives, whether positive or negative" (International Organization for Standardization, 2022).
- **Risk Management** is the process of assessing, treating, and monitoring all of an organization's risks in order to minimize their adverse effects on the organization.
- **Risk Manager**: an individual who oversees the risk management process in the organization to protect its assets.
- **Risk Officer**: an individual with direct authority over the risk management team and reports to senior management.
- **Speculative Risk**, which is not the subject of insurance, involves a chance of loss, no loss but the realization of a gain.
- **Traditional Risk Management** places individual risks into silos.
- **Upside of Risk** means that the risk can be a benefit to the organization, meaning that the risk is an advantage.
- **Volatility** is a term applied to frequent fluctuations in the price of an asset.

CHAPTER 2: RISK CLASSIFICATION AND CATEGORIES

Chapter Overview

2.0 LEARNING OUTCOMES

Learning Objectives

At the end of this chapter, students will be able to:

- Explain the different types of risk, including pure and speculative risk, subjective and objective risk, and diversifiable and non-diversifiable risk.
- Identify the characteristics of the four main types of risk from the risk quadrants: hazard, operations, strategic, and financial risks.
- Discuss the upside (potential gain) and downside (potential loss) associated with each type of risk.
- Measure hazard risks using frequency and severity and implement strategies to prevent and reduce losses.
- Assess financial risks like market and credit risks and strategic risks influenced by economic, demographic, and political factors using appropriate risk indicators.

2.1 RISK CLASSIFICATION AND ITS SIGNIFICANCE

For any organization, classifying risks helps them to understand and manage risk more efficiently. It also aligns them with their objectives to identify better tools and techniques to manage them.

Let us delve into a more detailed explanation of the importance of classifying risks within an organization.

Understanding and Managing Risks

Risk classification involves categorizing various types of risks based on common attributes or characteristics. By doing so, organizations better understand the risks they face. When risks are classified, it becomes easier to identify their specific nature, potential impact, and likelihood of occurrence. This understanding allows organizations to allocate appropriate resources and develop targeted risk management strategies.

Alignment with Objectives and Goals

Effective risk management requires alignment with an organization's objectives and risk management goals.

Organizations can tailor risk mitigation efforts to specific objectives by classifying risks. For instance:

- Financial risks may align with financial objectives.
- Operational risks may relate to process efficiency and effectiveness.
- Strategic risks may impact long-term goals and competitive positioning.

Assessing Risks

Similar risks often share common attributes. By grouping them into classifications, organizations can assess risks more efficiently. For example, technical risks related to implementing new laptops for a project can be categorized under the broader label of "Technical" risks. Assessing risks within the same classification allows for consistent evaluation and prioritization.

Risk Management Techniques

Different risk types may require distinct management approaches. When risks are classified, organizations can apply similar techniques to manage risks within the same category. For instance, technical risks may be mitigated using specific technical solutions, while financial risks may involve financial hedging strategies.

Administrative Function of Risk Management

Risk classification streamlines administrative processes. It ensures that risks within the same category receive consistent attention. By organizing risks, organizations reduce the likelihood of overlooking critical risks. Administrative tasks, such as reporting and monitoring, become more efficient when risks are well-organized.

Risk classification serves as a foundational step in effective risk management. It enhances understanding, aligns with organizational goals, facilitates assessment, enables targeted risk mitigation, and ensures administrative efficiency. Remember, managing risks is essential for successful project execution and organizational resilience.

2.2 RISK CLASSIFICATION

Risk can be classified in several ways, but the following classification has been used for clarity (Elliott, 2018):

1. Speculative and pure risk
2. Objective and subjective risk
3. Diversifiable and non-diversifiable risk
4. Quadrants of risk (Strategic, Financial, Operational, and Hazard)

Figure 2.2.1. "Classification of Risk" by Sanaz Habibi, CC BY-NC-SA 4.0. *Click to enlarge*

Image Description

Classifications of Risk diagrams.

Risk box with two branches: Pure and Speculative. Each of those is divided with a branch into Subjective and Objective boxes. Each Subjective and Objective is branched into a Diversifiable and Nondiversifiable box. The Pure, Objective, Diversifiable line of boxes is coloured as insurable risks are generally classified as pure, objective, and diversifiable.

Speculative and Pure Risk

Pure Risk

Pure risk is a category of risk that cannot be controlled and has two outcomes: complete loss or no loss at all, but no gain can be realized.

Pure Risk Examples

- Natural Disasters: Events like earthquakes, floods, hurricanes, and wildfires fall under pure risk. These disasters can cause significant damage or loss without any chance of gain.
- Death: The risk of losing a loved one due to illness, accidents, or other unforeseen circumstances is a pure risk.
- Theft: When the property is stolen, it results in a complete loss for the owner.
- Liability Risks: Legal situations where someone may sue for damages (e.g., slip and fall accidents) are also examples of pure risk

Although pure risks cannot be avoided, insurance can mitigate them. Insurance companies offer policies to transfer pure risk from individuals to themselves. For example, auto owners purchase auto insurance to protect against any damage to their vehicle and/or liability for damages.

Speculative Risk

Speculative risk refers to a category of risk where the outcome is uncertain and can result in either gains or losses. Unlike pure risk, which only involves the possibility of loss, speculative risk involves conscious choices made by individuals. Here are some key points about speculative risk:

- Speculative risk is the possibility that an investment will not appreciate in value. It arises from situations where the outcome is uncertain, and there is a chance of both gain and loss.
- Speculative risks are voluntary and not solely a result of uncontrollable circumstances.

Spectulitive Risk Examples

- Investing in Stocks: There is a speculative risk when investing in stocks. The stock price may rise, resulting in gains or falls and losses.
- Real Estate Investments: Buying property with the hope that its value will increase over time involves speculative risk.
- Starting a New Business: Entrepreneurship carries speculative risk. The success or failure of a new venture is uncertain.
- Sports Betting: Betting on sports events is speculative because the outcome is unpredictable.

Speculative risk can lead to both profits and losses, making it distinct from pure risk, where only losses are possible.

Speculative Risks in Investments

There is a significant Speculative Risk involved in the investments. The following risks cover areas within the investment:

- **Inflation Risk**: This risk results from the erosion of purchasing power caused by a general increase in the overall price level within the economy. Inflation can reduce the real value of investments.
- **Market Risk**: This risk arises from fluctuations in the prices of financial securities, including bonds and stocks. It reflects the potential for losses due to market movements.
- **Interest Rate Risk**: This risk pertains to a security's future value due to changes in interest rates. When rates rise, bond prices tend to fall, affecting the value of fixed-income investments.
- **Liquidity Risk**: This risk relates to the ease of selling an investment quickly and at a reasonable price. Illiquid assets may be challenging to convert into cash without significant loss.

Pure risk is all about unavoidable losses, while speculative risk involves conscious choices with the potential for both gains and losses. Understanding these distinctions is crucial for effective risk management and decision-making.

Subjective and Objective Risk

When people or organizations need to make decisions that involve risk, they typically rely on either opinions (which are subjective) or facts (which are objective) to assess that risk. Opinions are based on personal beliefs or feelings, while facts are based on verifiable evidence. So, it's important to consider both perspectives when evaluating risks.

Objective Risk

Objective risk refers to the probability of an event occurring based on concrete data and facts. It is quantifiable, measurable, and independent of personal opinions or biases.

Objective Risk Example

A car insurance company has analyzed accident data over the past decade. On average, 20% of policyholders file yearly claims due to accidents. This historical data provides an objective risk assessment.

Subjective Risk

Subjective risk is influenced by personal beliefs, perceptions, and experiences. It is more individualized and can vary from person to person.

Subjective Risk Example

A small business owner is considering expanding into a new market. They've done their homework, researching the market thoroughly and objectively evaluating risks like economic conditions,

competition, and regulatory changes. But despite all this analysis, they still feel uneasy. It's called subjective risk, where feelings or experiences play a role.

Subjective risk is influenced by perception, emotions, and cognitive factors, while objective risk relies on empirical evidence and statistical analysis. These differences can lead to substantial disparities in risk assessments.

Example

Scenario: A tech startup is developing a cutting-edge software product. They've objectively assessed the risks related to development costs, market demand, and competition.

Objective Risk: Based on historical data, they estimate a 10% chance of the project failing due to unforeseen technical issues.

Subjective Risk: However, the startup's lead developer has a gut feeling that the software might encounter compatibility problems with existing systems. This feeling isn't quantifiable but contributes to the overall subjective risk.

The startup weighs both objective and subjective risks. If they decide to proceed, they acknowledge that their intuition plays a role alongside the hard data.

Diversifiable and Non-Diversifiable Risk

Diversifiable Risk

Diversifiable risk refers to firm-specific risks that impact individual stock prices rather than affecting the entire industry or sector in which the firm operates.

Components of Diversifiable Risk:

- **Business Risk:** Arises from challenges specific to a firm's operations. For example, a pharmaceutical

company investing heavily in research and development but failing to find a patent for its new drug faces internal business risk.

- **Financial Risk**: An internal risk related to the firm's capital structure and cash flow. A robust capital structure helps the firm weather turmoil.
- **Management Risk**: The riskiest segment, influenced by leadership changes.

Diversifiable Risk Example

A firm facing a labour strike or regulatory penalty. Even if the industry is growing, this firm will face challenges, and shareholders might see lower stock prices due to these specific risks.

Non-Diversifiable Risk (Systemic Risk)

Non-diversifiable risk affects an entire class of assets or liabilities and is independent of overall market conditions.

Characteristics:

- **Market Risk:** Inherent risk in the marketplace as a whole, affecting all investments.
- **Interest Rate Risk:** Changes in interest rates impact various assets uniformly.
- **Economic Factors:** Factors like inflation, recession, and geopolitical events affect all investments.

Non-diversifiable Example

A global economic downturn affecting stock markets worldwide is a nondiversifiable risk. Diversification cannot eliminate this risk entirely. For example, COVID-19, where the entire world, irrespective of industries, is affected.

Risk Quadrants: Hazard, Operational, Strategic, and Financial Risks

Risks have been categorized differently in different regions and organizations. However, in North America, risks are normally placed into the following four quadrants (IRM's Risk Management Standard, 2002).

- Hazard
- Operational
- Strategic
- Financial

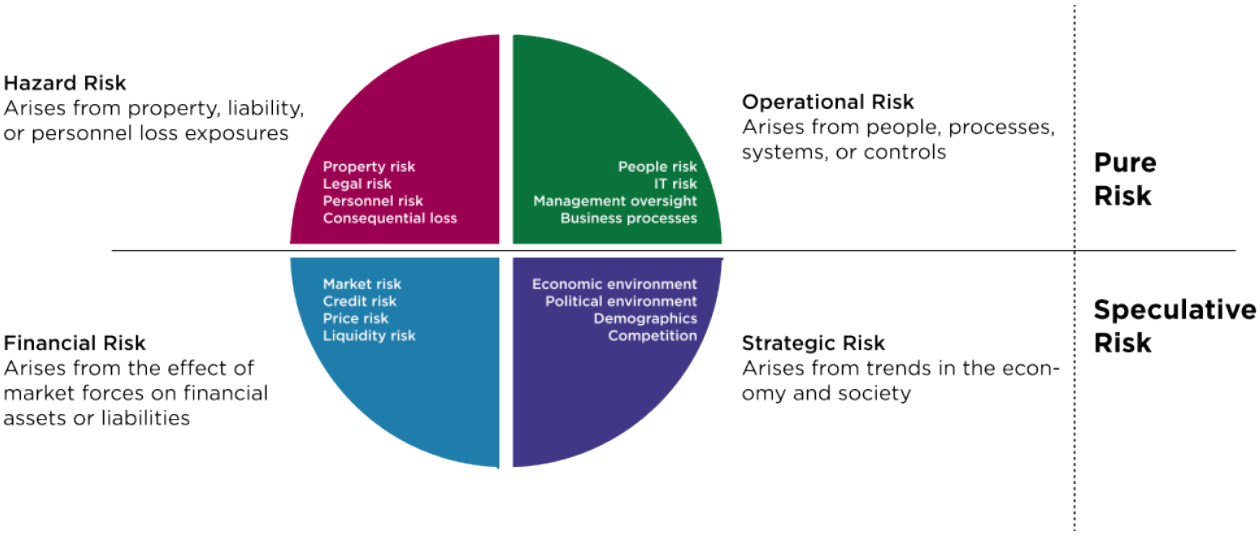

Figure 2.2.2: "Risk Quadrants" by Sanaz Habibi, CC BY-NC-SA 4.0. *Click to enlarge*

Image Description

Risk Quadrants Image.

A circle is divided into four quarters for each type of risk.

Clockwise from top left:

Hazard Risk: Arises from property, liability, or personnel loss exposures. Includes property risk, legal risk, personnel risk, and consequential risk.

Operational Risk: Arises from people, processes, systems, or controls. Includes people risk, IT risk, management oversight, and business processes.

Strategic Risk: Arises from trends in the economy and society. Includes economic environment, political environment, demographics, and competition.

Financial Risk: Arises from the effect of market forces on financial assets or liabilities. Includes market risk, credit risk, price risk, and liquidity risk.

Hazard Risk and Operational Risk are Pure Risk and Financial Risk and Strategic Risk are Speculative Risk.

2.3 HAZARD RISKS

Hazard risks refer to unpredictable events that often arise from natural disasters, accidents, or other external factors. There are pure risks, which are generally insurable. These risks can significantly disrupt supply chains.

A manufacturing facility located in an area prone to earthquakes. A major earthquake could damage the facility, disrupt production, and impact the entire supply chain.

Following are some of the examples of the hazard risks:

- Theft/Crime
- Fire or any damage to the property
- Business interruptions
- Disease, personal injuries, disability
- Liability

Categories of Hazard Risk

Hazard risk can be categorized into the following three categories:

1. **Personnel Risk:** Personnel risk refers to the uncertainty related to potential losses a firm may face due to various factors related to its employees, such as death, injury, health issues, disability, and loss of a key employee.
2. **Property Risk:** Property risk refers to the loss or damage to property or loss of wealth due to the damage to the property. For example, the loss of a manufacturing facility by an earthquake affects productivity.
3. **Liability Risk:** A liability risk refers to the financial responsibility that can lead an individual or business to be held responsible for specific types of losses. This could be an injury or loss of wealth that an entity causes. For example, a liability related to a faulty product damaging a consumer's health or injury.

How Hazard Risks Are Measured and Managed

Once a risk has been identified as a Hazard risk, the next step is to measure and manage it.

Frequency and severity are two key factors used to measure hazard risk. They help assess the likelihood of a hazard causing harm and the potential consequences of that harm.

- **Frequency** refers to how often a hazard event might occur. This could range from "rarely" to "likely to occur often."
- **Severity** refers to the seriousness of the potential harm caused by the hazard. This could range from a minor injury to a fatality.

By considering both frequency and severity, we can better understand the overall risk posed by a hazard. This allows us to prioritize risk management efforts and focus on hazards with the greatest potential to cause harm.

Hazard risks are managed using different techniques; however, all the techniques move around following two basic requirements.

- Prevent Losses.
- Reduce frequency and/or severity.

What is a Loss Exposure

Loss Exposure is the potential for loss that an individual or organization faces due to the frequency or severity. While identifying the risk, it is important to know the exposure of loss in any particular risk so that the appropriate corrective action is taken.

There are three circumstances where loss exposure arises when they intersect.

1. **Asset Exposed to Loss**: An asset that has a value and is exposed to loss, for example, tangible properties such as cash, property, investment, and intangibles such as patents and copyrights.
2. **Cause of loss**: An event that has caused a loss, like fire, thunderstorm, explosion, accident
3. **Financial consequences**: Financial consequences could be as simple as the loss of an asset damaged by fire, but they can be more complex when there is a loss of business while a building damaged in fire is restored. Some financial losses can be determined as soon as the loss occurs, but some take more time, like determining the liability.

Four types of Loss Exposures

1. **Property Loss Exposure**: The possibility of a financial loss due to damage, theft, or loss of use of property that someone has a financial interest in. This property can be broadly categorized into two types: tangible property, a property with a physical form, and intangible, a property with no physical form.
2. **Liability Loss Exposure**: This refers to a situation where an organization could become legally and financially responsible for injury, harm, or damage to another party. These exposures arise from the nature of an organization's work and where it is executed.
3. **Personnel Loss Exposure**: This refers to the potential risks associated with injury, disability, death, or departure of employees.
4. **Net Incomes Loss Exposure**: This refers to the possibility of experiencing a financial loss due to increased expenses or decreased revenue. Events like the loss of a major customer reducing revenue, supply chain disruption making it difficult to produce goods resulting in losing sales, damage to reputation impacting the company's reputation and leading to a loss of customers or natural disasters like floods, earthquakes, or fires disrupting operations and damage property, leading to lost income.

Table 2.3.1: Composition of Various Loss Exposure Categories

Loss Exposure Type	Asset Exposed to Loss	Cause of Loss	Financial Consequences of Loss
Property	Tangible, intangible, real, and personal property	Perils such as lightning, fire, flood, and so forth	Limited by the value of the property
Liability	Money in the form of, for example, lawsuit-related damages, settlement costs, and legal and court costs	The filing of a claim or suit seeking damages or some other legal remedy	Theoretically limitless, but essentially limited to the total wealth of the person or organization being sued
Personnel	The value that the key person adds to the organization	Death, disability, retirement, resignation, and so forth	Partial or total, as well as temporary or permanent. Depending on the circumstances and length of the departure
Net Income	Future stream of net income cash flow	Property, liability, or personnel loss; losses stemming from business risks	Vary based on the cause of loss; the worst-case scenario is a decrease in revenue to zero and a significant increase in expenses for a prolonged period.

Commercial Insurance Policies

Several commercial insurances are available for organizations as a part of the risk transfer technique for Hazard Risk. These insurances are developed through regulations and common usage.

Following are some of the insurances available (Elliott, 2018).

- Property Insurance
- Business Income Insurance
- Industrial All-Risk Insurance
- Builders' All Risk Insurance
- Equipment Breakdown Insurance
- Fidelity & Crime Insurance
- Surety Bonds
- General Liability Insurance
- Auto Insurance
- Workers Compensation & Employer Liability Insurance
- Professional Liability or Errors & Emissions Insurance
- Management Liability Insurance
- Doctors & Officers Liability Insurance
- Employment Practices Liability
- Fiduciary Liability
- Aircraft Insurance
- Ocean Marine Insurance
- Environmental Insurance

2.4 OPERATIONAL RISKS

Operational risks are associated with day-to-day business operations. These risks can stem from machinery breakdowns, IT system failures, labour disputes, or other internal factors.

A logistics company that relies on a fleet of delivery trucks. If one of the trucks breaks down unexpectedly, it could delay shipments and affect the overall supply chain efficiency.

Categories of Operational Risk

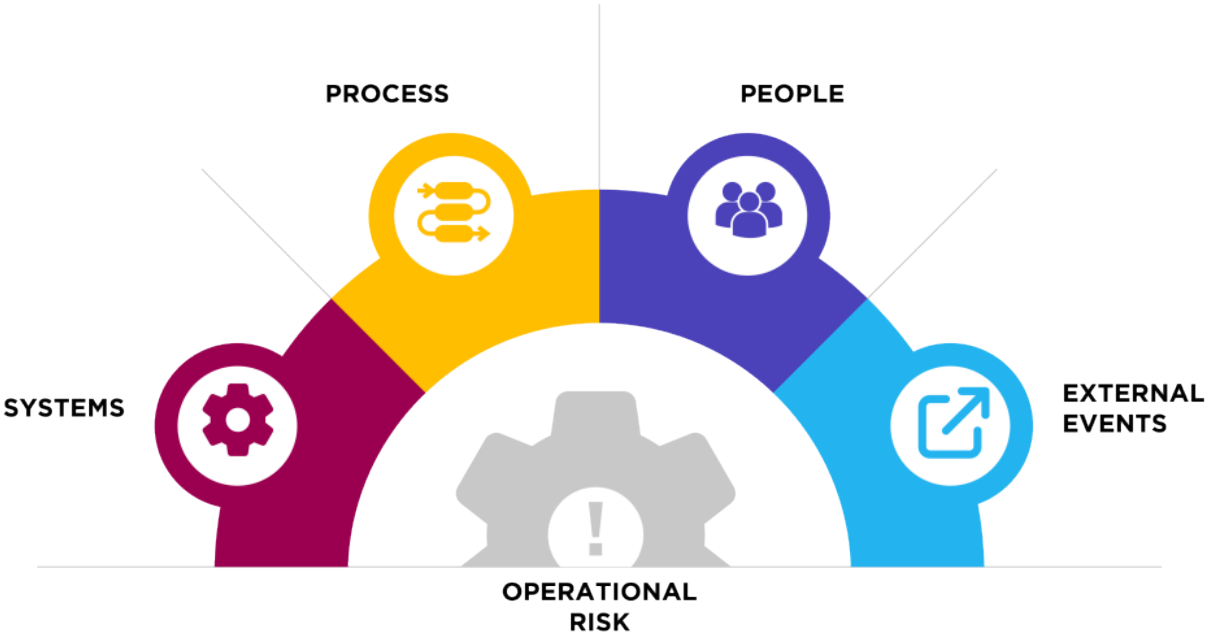

Figure 2.4.1: "Categories of Operational Risk" by Sanaz Habibi, CC BY-NC-SA 4.0

Image Description

A semi-circular diagram representing categories of operational risk, with segments for People (icon of a group of people in a purple segment), Processes (flowchart icon in a yellow segment), Systems (gear icon in a maroon segment), and External Events (arrow pointing outwards icon in a blue segment). At the center is a large gear

icon with an exclamation mark, representing the core of operational risk, with each segment connected to the center indicating their contribution to the overall operational risk.

- **People**: This refers to the risk of financial loss or other negative consequences arising from human error, misconduct, or a lack of skills or experience. Examples of people risk include employee fraud, negligence, turnover, and skills gaps.
- **Process**: This is the risk of loss arising from poorly designed or implemented business processes. Examples of process risk include errors in data entry, order fulfillment, or product development.
- **Systems**: This refers to the risk of loss resulting from failures or weaknesses in information technology systems, infrastructure, or other operational systems. Examples of systems risk include hardware or software failures, cyberattacks, and power outages.
- **External Events**: This is the risk of loss arising from events outside the organization's control, such as natural disasters, political unrest, or economic downturns.

Operations Risk Indicators

Operational risk indicators, also known as Key Risk Indicators (KRIs), are early warning systems used in risk management to identify potential operational risks before they cause problems. These metrics help assess the likelihood and impact of these risks (Elliott, 2018).

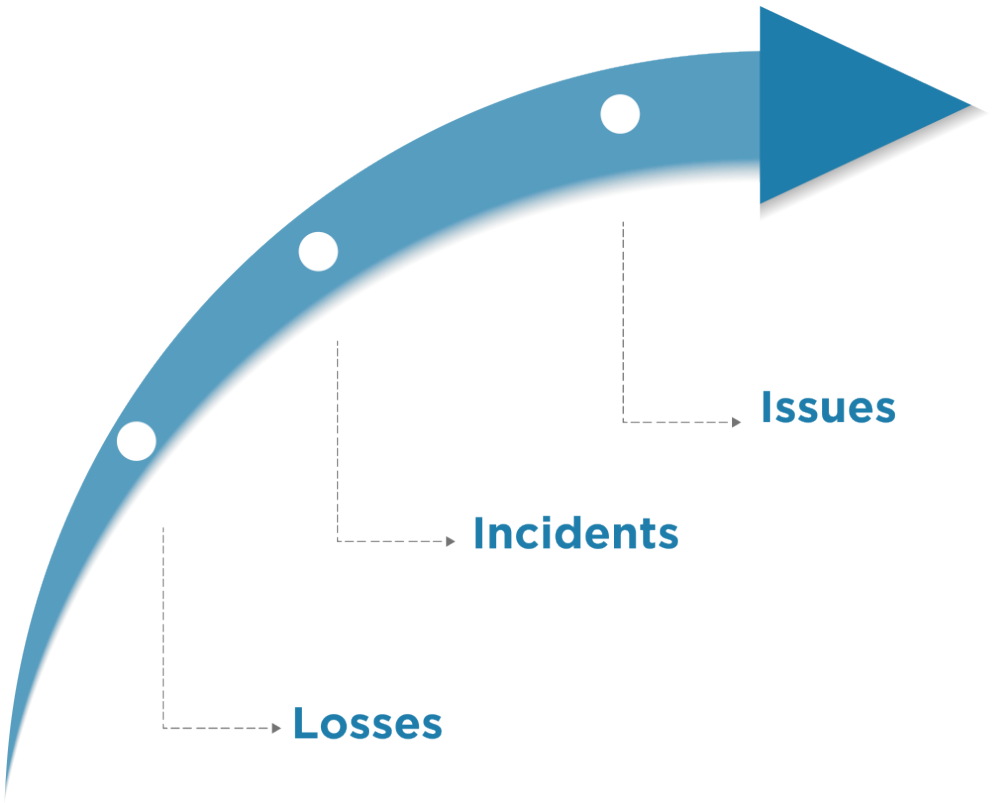

Figure 2.4.2: "Progression of Issues to Losses" by Sanaz Habibi, CC BY-NC-SA 4.0

Image Description

An arrow-shaped diagram showing the progression of issues to losses. The blue arrow curves upwards from the bottom left to the top right, with three white dots along its path. The first dot is labelled "Losses," with a dashed line pointing to the word. The second dot is labelled "Incidents," with a dashed line pointing to the word. The third dot is labelled "Issues," with a dashed line pointing to the word. The diagram illustrates the sequence from losses to incidents and finally to issues.

Key Risk Indicators are the metrics used to measure and define the potential loss. Employee turnover rate, customer complaint volume, and IT system breakdowns are some examples of KRIs. The following examples identify how KRIs identify the potential loss if not addressed.

- **Number of customer complaints**: Indicates the level of dissatisfaction with products or services.
- **Percentage of incomplete or inaccurate transactions**: Measures the quality of internal processes.
- **Employee turnover rates**: Reflects the stability or instability of the workforce.
- **Number of system downtime incidents**: Highlights technology-related risks.
- **Compliance violations**: Indicates adherence to regulatory requirements.

KRIs help organizations take action before issues are converted into incidents, eventually resulting in a loss to the organization.

2.5 FINANCIAL RISKS

Financial risks relate to changes in exchange rates, market risks, liquidity risks, or difficulties accessing capital. These risks can impact a company's ability to procure raw materials or pay suppliers on time.

There are three major types of financial risks: market, credit, and price.

Market risk

Market risk refers to the uncertainty surrounding the future value of an investment due to potential changes in the overall market conditions. Some of the financial risks are systematic, and some are nonsystematic.

Some of the Market risk categories are (Elliott, 2018):

- **Currency price risk**: risks associated with the change in currency exchange rate
- **Interest rate risk**: the risk that the asset's future value will decline due to the changes in the interest rates
- **Commodity price risk**: risk associated with the changes in the prices of commodities that are essential to the organization.
- **Equity price risk**: risk associated with the decrease in the price of the stock of the organization
- **Liquidity risk**: risk associated with the ability of the organization to raise cash or availability of cash reserves.

Credit Risk

Credit risk is the risk of loss that a lender faces when a borrower fails to meet their repayment obligations on a loan.

There are two types of credit risks: 'Firm-Specific' and 'Systemic credit risk', like the financial crisis 2008.

Price Risk

Price risk refers to the change in revenue or cost due to the increase or decrease in the price of products consumed.

Suppose a company imports raw materials from overseas. A sudden currency devaluation could increase the cost of these materials, affecting the supply chain's financial stability.

2.6 STRATEGIC RISKS

Strategic risks are from events like a recession, a financial crisis, or a pandemic like COVID-19 can threaten or provide opportunities to organizations.

These are outside the control of organizations and external to an organization. These are also from the speculative risk category, where the outcome could be positive or negative.

Type of Strategic Risks

There are three major types of Strategic Risk in the context of national or global conditions. The following are the three major Strategic Risks:

- Economic environment
- Demographics
- Political environment

Economic Environment

Under this strategic risk, there are several Key Risk Indicators that may help to identify the risk and take action:

- Gross Domestic Product (GDP)
- Inflations
- Financial crisis
- International trade flows and restrictions

Demographics

This refers to the characteristics of human populations. For example, the aging population and their expenses on health care, immigration, and younger populations in any specific area.

Political Environment

An action by one government to stop imports protecting local manufacturing or increase or decrease tariffs due to the political environment.

Effective supply chain & operations risk management entails recognizing and addressing risks across these four quadrants to guarantee the continuity and profitability of a business.

2.7 CHAPTER SUMMARY

Summary

Chapter 2 focuses on risk classifications and categories, emphasizing the importance of categorizing risks for better management and alignment with organizational objectives. It explains that risks can be classified into several types: pure and speculative risks, subjective and objective risks, and diversifiable and non-diversifiable risks. Additionally, it highlights the four main risk quadrants: hazard, operational, strategic, and financial risks. This classification helps organizations understand the specific nature, potential impact, and likelihood of risks, enabling them to allocate resources and develop targeted risk management strategies effectively.

The chapter further elaborates on the significance of understanding and managing different types of risks. It discusses pure risks, which involve only the possibility of loss, and speculative risks, which involve potential gains or losses. The document also distinguishes between subjective risks, influenced by personal beliefs and perceptions, and objective risks, based on measurable data. Diversifiable risks, which are firm-specific, can be mitigated through diversification, while non-diversifiable risks, like market risks, affect entire asset classes. The chapter underscores the need for tailored risk management approaches for each risk type, highlighting techniques such as avoidance, separation, duplication, diversification, and insurance. Effective risk management enhances organizational resilience, aligns risk mitigation efforts with goals, and ensures administrative efficiency.

OpenAI. (2024, May 24). *ChatGPT.* [Large language model]. https://chat.openai.com/chat

Prompt: *Please take the chapter content in this document attached and summarize the key concepts into no more than two paragraphs. Reviewed by authors.*

Key Terms

- **Asset Exposed to Loss**: An asset that has a value and is exposed to loss.
- **Avoidance**: It is a technique that involves ceasing or never undertaking an activity to eliminate the possibility of future gains or losses occurring from that activity.
- **Business Risk:** Arises from challenges specific to a firm's operations.
- **Cause of loss**: An event that has caused a loss, like fire, thunderstorm, explosion, or accident.
- **Commodity price risk**: risk associated with the changes in the prices of commodities that are essential to the organization.
- **Compliance violations**: Indicates adherence to regulatory requirements.
- **Credit risk** is the risk of loss that a lender faces when a borrower fails to meet their repayment obligations on a loan.
- **Currency price risk**: risks associated with the change in currency exchange rate.
- **Diversifiable risk** refers to firm-specific risks that impact individual stock prices rather than affecting the entire industry or sector in which the firm operates.
- **Diversification**: A technique spreading loss exposure across different assets, industries, projects, and companies, the overall risk can be reduced.
- **Duplication**: A technique to control risks by creating backups or spares of critical systems, data, or resources. It means not putting all your eggs in one basket.
- **Economic Factors:** Factors like inflation, recession, and geopolitical events affect all investments.
- **Employee turnover rates**: Reflects the stability or instability of the workforce.
- **Equity price risk**: risk associated with the decrease in the price of the stock of the organization.
- **External Events**: This is the risk of loss arising from events outside the organization's control, such as natural disasters, political unrest, or economic downturns.
- **Financial consequences**: Financial consequences could be as simple as the loss of an asset damaged by fire, but they can be more complex when there is a loss of business while a building damaged in fire is restored.
- **Financial Risk**: An internal risk related to the firm's capital structure and cash flow. A robust capital structure helps the firm weather turmoil.

- **Financial risks** relate to changes in exchange rates, market risks, liquidity risks, or difficulties accessing capital. These risks can impact a company's ability to procure raw materials or pay suppliers on time.
- **Frequency** refers to how often a hazard event might occur. This could range from "rarely" to "likely to occur often."
- **Hazard risks** refer to unpredictable events that often arise from natural disasters, accidents, or other external factors. There are pure risks, which are generally insurable. These risks can significantly disrupt supply chains.
- **Inflation Risk**: This risk results from the erosion of purchasing power caused by a general increase in the overall price level within the economy. Inflation can reduce the real value of investments.
- **Insurance**: A technique that transfers the potential risks or consequences by reducing the financial impact of unexpected events from insured to insurer. Risks with higher severity and low frequency are transferred to the insurance company.
- **Interest Rate Risk:** Changes in interest rates impact various assets uniformly.
- **Interest rate risk**: the risk that the asset's future value will decline due to the changes in the interest rates.
- **Interest Rate Risk**: This risk pertains to a security's future value due to changes in interest rates. When rates rise, bond prices tend to fall, affecting the value of fixed-income investments.
- **Key Risk Indicators** are the metrics used to measure and define the potential loss.
- **Liability Loss Exposure**: This refers to a situation where an organization could become legally and financially responsible for injury, harm, or damage to another party. These exposures arise from the nature of an organization's work and where it is executed.
- **Liability Risk:** A liability risk refers to the financial responsibility that can lead an individual or business to be held responsible for specific types of losses. This could be an injury or loss of wealth that an entity causes.
- **Liquidity risk**: risk associated with the ability of the organization to raise cash or availability of cash reserves.
- **Liquidity Risk**: This risk relates to the ease of selling an investment quickly and at a reasonable price. Illiquid assets may be challenging to convert into cash without significant loss.
- **Loss Exposure** is the potential for loss that an individual or organization faces due to the frequency or severity.
- **Management Risk**: The riskiest segment, influenced by leadership changes.

- **Market risk** refers to the uncertainty surrounding the future value of an investment due to potential changes in the overall market conditions.
- **Market Risk:** Inherent risk in the marketplace as a whole, affecting all investments.
- **Market Risk**: This risk arises from fluctuations in the prices of financial securities, including bonds and stocks. It reflects the potential for losses due to market movements.
- **Net Incomes Loss Exposure**: This refers to the possibility of experiencing a financial loss due to increased expenses or decreased revenue.
- **Non-diversifiable risk** affects an entire class of assets or liabilities and is independent of overall market conditions.
- **Number of customer complaints**: Indicates the level of dissatisfaction with products or services.
- **Number of system downtime incidents**: Highlights technology-related risks.
- **Objective risk** refers to the probability of an event occurring based on concrete data and facts. It is quantifiable, measurable, and independent of personal opinions or biases.
- **Operational risk indicators**, also known as Key Risk Indicators (KRIs), are early warning systems used in risk management to identify potential operational risks before they cause problems. These metrics help assess the likelihood and impact of these risks.
- **Operational risks** are associated with day-to-day business operations. These risks can stem from machinery breakdowns, IT system failures, labour disputes, or other internal factors.
- **People**: This refers to the risk of financial loss or other negative consequences arising from human error, misconduct, or a lack of skills or experience.
- **Percentage of incomplete or inaccurate transactions**: Measures the quality of internal processes.
- **Personnel Loss Exposure**: This refers to the potential risks associated with injury, disability, death, or departure of employees.
- **Personnel Risk:** Personnel risk refers to the uncertainty related to potential losses a firm may face due to various factors related to its employees, such as death, injury, health issues, disability, and loss of a key employee.
- **Prevention** by reducing the frequency of loss and Reduction by reducing the severity of losses.
- **Price risk** refers to the change in revenue or cost due to the increase or decrease in the price of products consumed.
- **Process**: This is the risk of loss arising from poorly designed or implemented business processes.

- **Property Loss Exposure**: The possibility of a financial loss due to damage, theft, or loss of use of property that someone has a financial interest in. This property can be broadly categorized into two types: tangible property, a property with a physical form, and intangible, a property with no physical form.
- **Property Risk:** Property risk refers to the loss or damage to property or loss of wealth due to the damage to the property.
- **Pure risk** is a category of risk that cannot be controlled and has two outcomes: complete loss or no loss at all, but no gain can be realized.
- **Separation**: A technique that involves spreading activities or assets across multiple locations to limit the overall severity of a potential loss. Separation can be applied to various aspects of a business, from physical assets like data centers to financial resources.
- **Severity** refers to the seriousness of the potential harm caused by the hazard. This could range from a minor injury to a fatality.
- **Speculative risk** refers to a category of risk where the outcome is uncertain and can result in either gains or losses.
- **Strategic risks** are from events like a recession, a financial crisis, or a pandemic like COVID-19 can threaten or provide opportunities to organizations.
- **Subjective risk** is influenced by personal beliefs, perceptions, and experiences. It is more individualized and can vary from person to person.
- **Systems**: This refers to the risk of loss resulting from failures or weaknesses in information technology systems, infrastructure, or other operational systems.

CHAPTER 3: RISK MANAGEMENT FRAMEWORK AND PROCESS

Chapter Overview

3.0 LEARNING OUTCOMES

Learning Objectives

At the end of this chapter, students will be able to:

- Explain the importance of a Risk Management Framework and Process
- Outline two key risk management standards: ISO 31000:2018 and COSO ERM Framework 2017
- Describe the elements of the generic risk management framework and process

3.1 IMPLEMENTING RISK MANAGEMENT

The undertaking by an organization to implement a risk management offering in a small organization or a multinational company is a daunting task. Individuals working in a small business will have hands on experience in the daily operations of the organization and will completely understand the processes, objectives, processes and goals related to the organization from the bottom up and the top down. In comparison, a large organization would require input from many individuals, departments, locations, management, senior management and shareholders to obtain the information required to fully understand the organization in its entirety. Irrespective of size and scale, all organizations require a coordinated approach to managing all the key business risks they face with the goal of obtaining favourable outcomes.

Some organizations can structure a risk management framework and process designed to manage all the key business risks they face based on the skill of individuals and designated risk management practitioners inside the organization. It is, however, recommended that an organization selects an internationally recognized standard that includes a framework and process that is best suited to that organization. The risk management framework is a foundation that supports the organization's risk management process and is the conduit that communicates risk information from the risk management process to the organization. The risk management process consists of activities that manage and control risks and their effects on the organization. The risk management framework supports the risk management process in the organization.

The advantages of using an internationally recognized risk management standard are that its standard approach can be applied to all organizations, its concepts are periodically reviewed to adjust to evolving risk, and it will be recognizable to risk management practitioners globally in the external environment.

Compliance with a risk management standard is not mandatory; its use by an organization is advisory. The two risk management standards that will be discussed in this chapter are the ISO 31000: 2018 and the COSO ERM 2017. It should be noted that both risk management standards are available as documents or in software form for ease of use by an organization.

A **standard** is a document often prepared by a recognized authority that provides guidelines, nomenclature, activities, principles, requirements and a basis to ensure consistency in practices that an organization undertakes. The use of a standard is not mandatory but the use of a standard is considered to be a tenet of best practices. In contrast, a code is mandatory, requiring compliance by an organization that, if not met, will result in consequences such as fines, suspension, shut-down or prison.

3.2 ISO 31000:2018

The International Organization for Standardization (ISO) developed and published an international standard for risk management in 2009 that has been updated into its present version, **ISO 31000:2018**. It is a generic risk management standard developed to address and manage risk in an organization of any size or complexity. The ISO 31000:2018 definition of risk is "the effect of uncertainty on objectives" (International Organization for Standardization, 2018), which is reflective of more modern thinking about risk. Uncertainty suggests that the outcome has the potential of having either positive or negative outcomes, an upside or a downside that reflects an enterprise approach. Therefore, this standard can be used by an organization to manage all its key business risks under the four major categories of hazard, operational, financial and strategic.

The ISO 31000:2018 standard is divided into five key sections:

Principles

There are eight key principles listed in the ISO 31000:2018 that the standard is built on that will contribute to the risk management strategy and protect the value of the organization:

1. Integrated risk management
2. Structured and comprehensive approach to risk management
3. Customized approach to the risk management framework and process
4. Involvement of all stakeholders
5. Ability to respond to change
6. Actions based on the best available data and information
7. Influence of human and cultural factors
8. Continued learning for improvement

Framework

ISO 31000:2018 provides guidance on how to establish a risk management framework that can be integrated into the organization's objectives and operations throughout the entire organization. The first step in establishing a successful risk management framework is to determine the context, followed by the introduction of a risk management policy for the organization. The context can be internal and/or external, with the purpose of describing the goals and objectives of the risk management offering, as well as the scope, responsibilities, and activities involved. The risk management policy is structured to guide the organization in the management of its risks. When all the internal/external risk management contexts have been contemplated, the risks that have been identified (including emerging risks) should be documented in a risk register.

Process

In addition to establishing the internal/external risk contexts, the organization must be able to follow a cycle of assessing, treating and monitoring risks. The ISO 31000:2018 definition of a risk assessment also consists of the identification and analysis of risks but also includes a third element of risk evaluation, which means applying risk criteria to determine the scale, significance and priority of the risk; in other words, the amount and type of risk that an organization can tolerate. ISO Guide 31073:2022 defines **risk criteria** as 'terms of reference against which the significance of a risk is evaluated.' The risk management process should reflect an enterprise approach by listing all the risks that have the potential to benefit or adversely affect the organization.

Risk Assessment

The first step in the risk assessment process is placing importance on identifying as many risks as possible with an emphasis on risks that influence the organization's objectives. The second step is analyzing the identified risks by examining the potential likelihood of each risk and the consequences. Quantitative or qualitative techniques can be used to analyze the risks that have been identified. Often, both techniques are required to conduct an analysis of the risks. The third step involves evaluating the risks by applying risk criteria to the levels of the risks to evaluate their significance and priority. The level of risk considers the combined effects of the likelihood and impact of the risk on the organization. On a risk map, the levels of risk for likelihood could be rare, unlikely, moderate, likely or almost certain. For impact or consequences, the levels of risk could be negligible, low, medium, very high or extreme. Responses to risks or risk treatments will be based on the level of risk.

Risk Treatment

Risk treatment is the implementation of actions and techniques for responding to both hazard and speculative risks by avoiding risks, modifying risks, retaining risks or transferring risks. Organizations will often combine risk treatments when responding to risks. Risks that are determined to produce positive outcomes should be embraced by the organization.

Risk Monitoring and Review

Risk management processes are generally cyclical in nature and the internal and external environments should be reviewed with necessary adjustments made. The organization's risk register is a useful tool that can be used to conduct this activity.

3.3 COSO ENTERPRISE RISK MANAGEMENT (ERM) FRAMEWORK

COSO (Committee of Sponsoring Organizations of the Treadway Committee). The COSO standard, like the ISO 31000 standard previously discussed, is not a mandatory requirement by an organization seeking to build a risk management offering. The COSO 2017 definition of risk has moved away from its more traditional roots by stating that risk is "the possibility that events will occur and affect the achievement of strategy on business objectives." When comparing it to the ISO 31000:2018 definition of risk, both definitions lean towards the uncertainty of risk and its effect on objectives with the goal of implementing an effective risk management offering in an organization. The effects could have an upside or a downside on the objectives of the organization.

Traditionally, the COSO ERM Framework was almost exclusively used by the financial sector due to its focus on financial reporting, audit, and compliance. The COSO ERM Framework, which was introduced in 2017, uses an intertwining double helix in the form of a ribbon-like rainbow instead of a cube known as the COSO ERM cube.

Figure 3.3.1: "Enterprise Risk Management" in *Enterprise Risk Management: Integrating with Strategy and Performance*, © 2017 Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used with permission. (See Acceptable Use of COSO Materials [PDF] for permission details).

Image Description

A double helix shape made up of 5 colours representing one side: governance & culture and information, communication, & reporting. On the other side, strategy & objective-setting, performance, and review & revision. In between the loops of the helix are mission, vision, & core values, strategy development, business objective formulation, implementation & performance, and enhanced value.

The update was deemed necessary to address the changing business landscapes and failures and to integrate an organization's risks with its strategies. There are five components for successful enterprise risk management that can be applied to an organization's mission and core values:

1. **Governance and Culture**: oversight from the top down.
2. **Strategy and Objective Setting**: activities related to related to risk appetite and performance
3. **Performance**: risk assessment and risk responses to address risks that could adversely affect the organization's performance.
4. **Review and Revision**: review the performance of ERM in the organization and make changes where necessary.
5. **Information, Communication and Reporting**: communicating the effect of ERM on the organization using information obtained from inside and outside the organization.

There are 20 principles across the five components stated above that have a relationship with each of the components. The COSO ERM Framework is connected to the organization by the components and the principles in the 2017 model. The interrelated components and principles in the form of a double helix are the DNA of a COSO ERM Framework, allowing an organization to manage risks and drive performance while maximizing value.

Table 3.3.1: "20 principles of the COSO ERM Framework" in *Enterprise Risk Management: Integrating with Strategy and Performance*, © 2017 Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used with permission. (See Acceptable Use of COSO Materials [PDF] for permission details).

Governance & Culture	Strategy & Objective-Setting	Performance	Review & Revision	Information, Communication, & Reporting
1. Exercises Board Risk Oversight 2. Establishes Operating Structures 3. Defines Desired Culture 4. Demonstrates Commitment to Core Values 5. Attracts, Develops, and Retains Capable Individuals	6. Analyzes Business Context 7. Defines Risk Appetite 8. Evaluates Alternative Strategies 9. Formulates Business Objectives	10. Identifies Risk 11. Assesses Severity of Risk 12. Prioritizes Risks 13. Implements Risk Responses 14. Develops Portfolio View	15. Assesses Substantial Change 16. Reviews Risk and Performance 17. Pursues Improvement in Enterprise Risk Management	18. Leverages Information and Technology 19. Communicates Risk Information 20. Reports on Risk, Culture, and Performance

3.4 ENTERPRISE RISK MANAGEMENT FRAMEWORK AND PROCESS

Although the ISO 31000:2018 or the COSO ERM Framework can be used by any organization, the ISO 31000:2018 contains a generic risk management framework and process that many organizations feel is easier to implement. This will be used as the model in this course.

The four components of the generic risk management framework supporting the risk management process are:

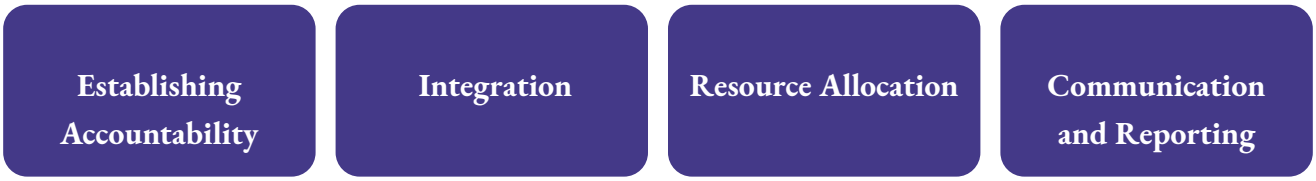

Figure 3.4.1: The four components of the generic risk management framework supporting the risk management process.

Establishing Accountability

The first element of the risk management framework is to establish accountability within the ranks of the organization's senior management. A risk management architecture and structure should be implemented to support management's commitment to a risk management culture.

Integration

The second element of the risk management framework is to align risk management with the organization's objectives with the goal of integrating the risk management process into the organization's processes.

Resource Allocation

The third element of the risk management framework is to receive a commitment from management to provide the necessary resources to implement the risk management process throughout the organization. Management must be prepared to dedicate financial, personnel and training resources to support the implementation of a risk management offering.

Communication and Reporting

The fourth and final element of the risk management framework is the communication of the risk management process across the organization and to stakeholders. Detailed reports containing information on both known and emerging risks should be completed, prepared, and reviewed. Known risks are risks that an organization has knowledge about or that have previously affected the organization. Emerging risks are risks that are not known to an organization, resulting from cycles, technology, global events, or changes to existing processes.

3.5 ENTERPRISE-WIDE RISK MANAGEMENT PROCESS

The implementation of an **Enterprise-Wide Risk Management Process** is an approach that allows an organization to manage all the risks that have potential upside and downside effects on the organization.

The Enterprise-Wide Risk Management Process is cyclical and addresses all the risks that have the potential for positive or negative effects on an organization.

The five steps of the Enterprise Wide Risk Management Process are listed in sequence:

Figure 3.5.1: The five steps of the Enterprise Wide Risk Management Process.

Scan the Environment

The first step in the process is to look at the internal and external environments that the organization exists in to see where risk can adversely affect the organization or create opportunities. The information gained from this important first step can be used to make decisions as to how the risk management process is aligned with

the organization's objectives. If the objective of the organization is fire safety, then the risk management process should be aligned with this objective by preventing fires and reducing their impact.

There should be an understanding between risk management and others in the organization as to the meaning and alignment of risk criteria. Risk criteria can be defined as the causes of risk and effects of risk, metrics to measure the effects of risk, timeframe, methods to determine levels of risk, and approaches to addressing combinations of risk.

Scanning the environment could also include looking at other organizations working in the same sector and their management of risk. For example, a police force that is establishing a formal risk management offering would be wise to communicate with other police forces to learn about risks and opportunities that could also affect them.

Identify Risks

Risk identification is the second step in the Enterprise-Wide Risk Management Process. It involves collecting a list of key and emerging risks that could have an effect on the organization's objectives. In an enterprise approach, it is foreseeable that one risk could very well extend into other risk quadrants. For example, an organization's carelessness with respect to environmental stewardship would normally be classified as a hazard risk since there could be harm to property, personnel, or liability. The publicity resulting from the environmental event could also influence the organization's reputation by involving one or more of the other three risk categories (operational, financial, strategic).

Analyze Risks

Risk analysis is the third step in the process. Defined risk criteria can be used to determine the source, cause, likelihood (frequency, probability) and consequences (impact, severity) of the risks that have been identified. Risk analysis can be qualitative, quantitative, or a combination of both. If the previous environmental example under Identify Risks is used, the harm caused by the environmental event can be quantified or measured. The reputational risk, however, might be more difficult to measure and would likely be expressed qualitatively.

Treat Risks

A risk assessment involves the steps of identifying and analyzing risks in the organization, followed by treating risk, which is the fourth step in the process. **Risk treatment** involves strategies, controls and techniques that are implemented to respond to an organization's risks. It should be noted that more than one technique is often required to address a risk. For example, if a potential fire loss (total level of risk) to a key distribution

centre that is not sprinkled would drastically affect profits (risk criteria), then the organization should respond by installing a standard sprinkle system to minimize the impact. The financial impact of a fire on the organization would be reduced by purchasing guaranteed cost insurance at the distribution centre. Although there is a real upside to installing a sprinkler system in a building, there is also the downside created by the accidental escape of water from the sprinkler system or someone shutting off the water to the sprinkler system. This is an example of how addressing one risk can create another risk! The risk response to this newly created risk would be to install a water shut alarm designed to notify personnel that the water has been shut off to the sprinkler system and to install low-pressure and water flow alarms that will notify personnel that water is flowing through the sprinkler piping.

The Five Risk Responses Used to Treat Risks

1. Avoid the risk
2. Modify the likelihood and/or impact of the risk
3. Transfer the risk
4. Retain the risk
5. Exploit the risk

Monitor and Assure

The final step in the Enterprise-Wide Risk Management Process is to review and monitor results by improving risk assessment, determining the effectiveness of controls, analyzing the successes and failures of events, noting changes inside and outside of the organization and identifying emerging risks.

To maintain a high standard of risk management, the cyclical nature of the Enterprise-Wide Risk Management Process would require that the five-step process be continued in response to the modern risk environment.

3.6 CHAPTER SUMMARY

Summary

Chapter 3 covers the essentials of risk management frameworks and processes, highlighting the importance of structured approaches to managing business risks for organizations of any size. It introduces two key risk management standards, ISO 31000:2018 and the COSO ERM Framework 2017. Both standards offer guidelines for establishing a risk management framework and processes that integrate with an organization's overall objectives. ISO 31000:2018 defines risk as the effect of uncertainty on objectives and encompasses principles, frameworks, and processes to manage risks effectively. The COSO ERM Framework redefines risk management by linking it to strategy and performance, using a model with five components: governance and culture, strategy and objective setting, performance, review and revision, and information communication and reporting.

The chapter outlines the steps of the risk management process, starting with scanning the environment to identify potential risks, analyzing these risks, and then treating them through various strategies such as avoidance, modification, transfer, retention, or exploitation. Monitoring and review ensure the process remains dynamic and responsive to new risks. The chapter emphasizes the value of adopting recognized standards like ISO 31000:2018 and COSO ERM to ensure consistency, improve risk management practices, and enhance organizational resilience against potential threats.

OpenAI. (2024, May 29). *ChatGPT.* [Large language model]. https://chat.openai.com/chat

Prompt: *Please take the chapter content in this document attached and summarize the key concepts into no more than two paragraphs. Reviewed by authors.*

Key Terms

- **Enterprise-Wide Risk Management Process** is an approach that allows an organization to manage all the risks that have potential upside and downside effects on the organization.
- **Governance and Culture**: oversight from the top down.
- **Information, Communication, and Reporting**: communicating the effect of ERM on the organization using information obtained from inside and outside of the organization.
- **ISO 31000:2018**. It is a generic risk management standard developed to address and manage risk in an organization of any size or complexity.
- **Performance**: risk assessment and risk responses to address risks that could adversely affect the organization's performance.
- **Review and Revision**: Review the performance of ERM in the organization and make changes where necessary.
- **Risk criteria** are defined by ISO Guide 31073:2022 as 'terms of reference against which the significance of a risk is evaluated.'
- **Risk treatment** involves strategies, controls and techniques that are implemented to respond to an organization's risks.
- **Risk treatment** is the implementation of actions and techniques for responding to both hazard and speculative risks by avoiding risks, modifying risks, retaining risks or transferring risks.
- **Standard** is a document often prepared by a recognized authority that provides guidelines, nomenclature, activities, principles, requirements and a basis to ensure consistency in practices that an organization undertakes.
- **Strategy and Objective Setting**: activities related to related to risk appetite and performance.

CHAPTER 4: IDENTIFYING RISKS

Chapter Overview

4.0 LEARNING OUTCOMES

Learning Objectives

At the end of this chapter, students will be able to:

- Identify and describe the types of risks that can positively and negatively affect an organization.
- Describe the features of established risk identification strategies that can be used by organizations.
- Create a Risk Register and connect it to a Risk Map.

4.1 RISK IDENTIFICATION

After Scanning the Environment, the second step in the generic risk management process is to identify all the potential risks that could positively or negatively affect an organization's objectives. **Risk identification** is defined by the International Organization for Standardization (ISO) as the "process of finding, recognizing and describing risks" (International Organization for Standardization, 2022).

Risks that have the effects of uncertainty on an organization can be internal or external to an organization. Traditionally, risks have been put into silos meaning that organizations isolate their risks within departments, business units, sectors or locations and address their risks at that level in the absence of sharing information with others in the organization. **Enterprise Risk Management** allows an organization to holistically manage all its key risks as well as opportunities that might exist. An organization practicing holistic risk management is taking a broad and integrated approach to managing its risks by 'wrapping its arms around all of its risks and allowing them to communicate with each other.' **Holistic risk management** allows the organization to see how potential risks and opportunities fit together across the four classifications of hazard, operational, financial and strategic risks (Elliott, 2018). Risks should also be identified holistically by an organization, as one risk will very likely influence the emergence of a second or even more risks within an organization. For example, a supply chain operating across North America would have a heavy reliance on information technology to coordinate its activities. If a fire occurred at a distribution centre, causing an interruption in data transmission, it could have a cascading effect on the organization's overall ability to function efficiently. In this case, a fire, which is a hazard risk, would have a direct effect on the organization's ability to distribute products, resulting in an operational risk. If there was inadequate communication within the organization regarding the situation, the adverse effects of the situation could be much greater.

When an organization conducts a risk assessment, it should identify all its risks before analyzing and responding to them using risk treatment techniques. The types of risks that should be identified are:

- **Known risks:** risks that the organization knows about or that have previously affected the organization.
- **Emerging risks:** risks that are not known to the organization.

- **Inherent risks:** risks that have not been managed or treated.
- **Residual risks:** the risk that remains after the risk has been managed or treated.

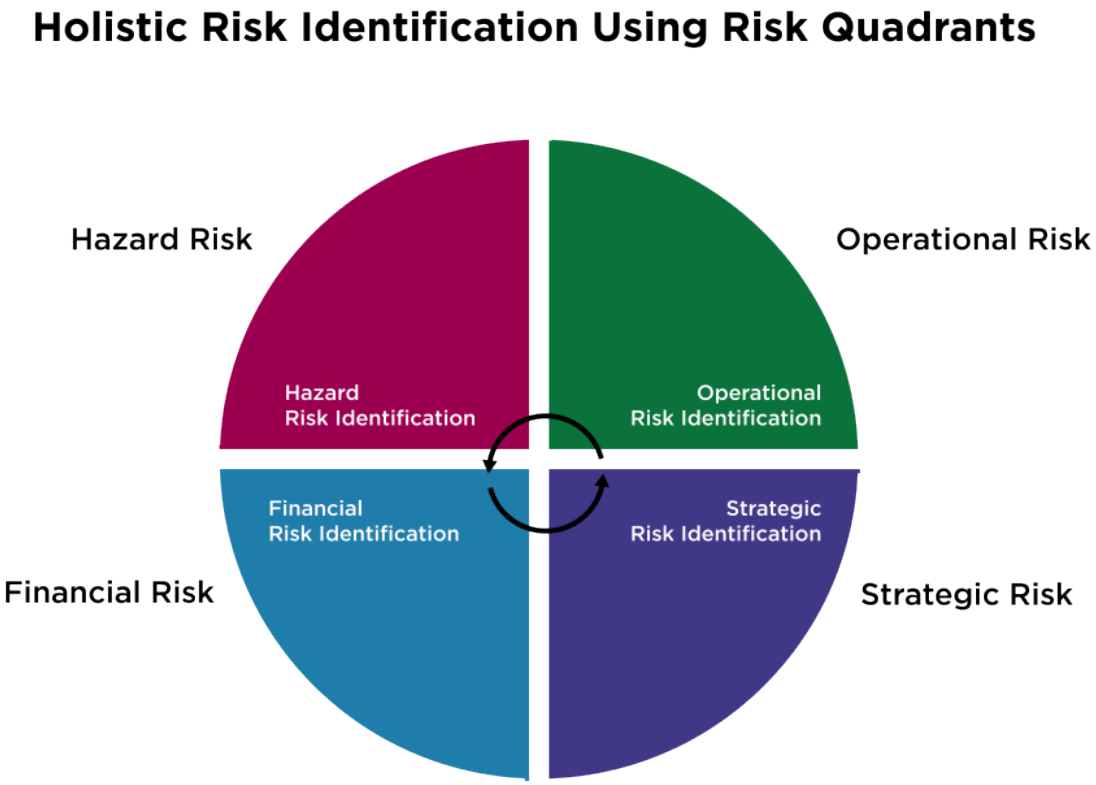

Figure 4.1.1: "Holistic Risk Identification Using Risk Quadrants" by Sanaz Habibi, CC BY-NC-SA 4.0. *Click to enlarge*

Image Description

A circular diagram, divided into four quadrants, each representing a different type of risk identification. The top left quadrant is maroon and labelled "Hazard Risk Identification." The top right quadrant is green and labeled "Operational Risk Identification." The bottom right quadrant is purple and labeled "Strategic Risk Identification." The bottom left quadrant is blue and labeled "Financial Risk Identification." An arrow in the center points clockwise, indicating the continuous process of holistic risk identification across all quadrants.

There are two holistic approaches to identifying risks available to an organization: a top-down or bottom-up approach. When a **top-down approach** is used, the senior management in the organization makes decisions on the risks that can have a positive or negative effect on the organization. The advantage of this approach

is that senior management will have access to all relevant risk information in the organization from a high-level perspective. While this is an advantage, it is also a disadvantage because there might not be a true grasp of all the organization's activities from that level, and there would also be a dependency on receiving accurate information from inside the organization. A **bottom-up approach** has the advantage of providing an abundance of information from personnel working within and throughout the organization. The disadvantages created would stem from not having access to all relevant information at that level and compiling the information to achieve a holistic perspective of the risks in the organization. The best overall approach to risk identification would be one that combines a top-down and a bottom-up approach.

4.2 RISK IDENTIFICATION STRATEGIES

There are many approaches and strategies that an organization can use to identify the potential adverse effects and opportunities that its risks present. When identifying risks, the best approach is an integrated approach, which is consistent with holistic risk management. A holistic approach to risk identification would involve individuals from senior management, middle management, risk management and personnel from all departments and sectors of the organization. In other words, it is a team approach to risk identification.

The following risk identification strategies should be performed by teams or groups that are familiar with the organization:

Brainstorming

Identifying risks in an informal and open discussion where all suggestions are welcomed as good suggestions based on the knowledge and experience of those in attendance. At the conclusion of the session, all the risks that have been identified should be analyzed and evaluated.

Workshops

Identifying risks in a formal setting by collaborating and hearing from others with the purpose of achieving a result. It is recommended that internal and external stakeholders be present at the workshop. It is advisable to have a facilitator who is familiar with leading risk management to guide the discussion, manage time and keep the participants on task. A facilitator can be an employee of the organization, but it is not uncommon to bring in a facilitator from outside of the organization for a more diverse perspective.

SWOT

Identifying risks by analyzing Strengths, Weaknesses, Opportunities, and Threats that exist in the organization. SWOT is commonly used by organizations to make decisions about risk during workshops or brainstorming sessions.

Documents

Identifying risks by examining documents that are relevant to the organization. Documents containing information on surveys that have been conducted, compliance reviews, insurance policies in force and no longer in force, financial statements, contracts, and projects should be reviewed to understand where risks exist in the organization, where risks are transferred and where there are opportunities.

Root Cause Analysis

Identifying risks by understanding the factors that caused an event to adversely affect the organization and controls or strategies that can be implemented to minimize the potential of a re-occurrence. The root causes of negative events that have previously affected the organization's risks and have the potential to cause future harm can be identified.

Physical Risk inspections

Identifying risks by having persons with skill and experience in risk assessment visit sites to determine if physical hazards exist that could adversely affect the organization. A visit by a qualified risk inspector is key in identifying risks that exist at a site that otherwise might not be known to the organization. The risk inspector will also consult with front-line employees and managers at the location to gather or confirm information that might not be apparent during the inspection.

Experts

Identifying risks using the opinions of subject experts. The Delphi technique brings together a panel of experts to answer questions pertaining to the organization and its risks. Each panel member is separated from the other panel members, and the answers to the questions are gathered anonymously. After each round of questions, a facilitator reviews the replies and presents the responses to all panel members. The same question is then asked again, and each panel member is given the opportunity to re-evaluate their previous response to the question before answering for a second time.

Risk Register

Identifying risks and inserting them into a table. A **risk register** is a risk management tool that identifies all the risks in an organization across individual scenarios, processes, sectors and locations. It is a useful tool that an organization can use to assess and prioritize its risks. For example, forest fires in Western Canada

lead to catastrophic losses. In this case, risks resulting from forest fires should be identified across the four risk classifications of hazard risks, operational risks, financial risks and strategic risks (See Table 4.2.1). The likelihood and consequences of each risk should be listed separately and calculated to determine the level of risk for each of the risk categories. The consequences can be expressed as dollar amounts. A risk register showing all the risks collected from the individual risk registers in the organization can be combined into a single organizational risk register that shows all the identified risks in one place.

Risk Register

Table 4.2.1 Risk Register

Risk Event/ Description	Risk Owner	Likelihood	Impact	SCORE	Improvement Action	Due Date/By When

Legends:

Likelihood	Score
	1
	2
	3
	4
	5

Impact	Score
	1
	2
	3
	4
	5

- *Risk Event/Description:* A description of the risks under each of the four risk categories: hazard, operational, financial, and strategic. It is more common to list risks with negative outcomes as opposed to positive outcomes under this heading. It is customary to build a risk register showing the inherent risks faced by an organization, followed by a second risk register that shows the residual, target or optimum risks that exist after the risks have been treated.
- *Risk Owner:* The Risk Owner is the entity that will make decisions about the risk and /or reports on the risk.
- *Likelihood:* The likelihood of an event occurring is expressed as a number between 1 and 5. It is associated with the frequency of an event occurring typically within the next 12 months. A likelihood of 5 would indicate that an event is extremely likely to occur, whereas a likelihood of 1 is indicative of an event that is extremely unlikely to occur.
- *Impact:* The impact of an event is expressed as a number between 1 and 5. It is associated with the consequences or severity of an event. An impact of 5 would indicate that the event would have a significant effect on an organization, whereas an impact of 1 would be indicative of an event that would have a minimal effect on an organization. The impact can also be expressed in ranges of dollar amounts.
- *Score:* The score for the risk is calculated as follows: likelihood score × impact score. The calculated score will quantitatively show the level of risk that the organization is exposed to. Scores can be displayed as a matrix on a risk map to visually show what risks fall inside or outside of the organization's risk appetite.
- *Improvement Action:* Actions that are already in place and/or plans that could contribute to improving risks faced by the organization. It is not necessary to identify specific risk responses or treatments at this point.
- *Due Date/By When:* The date showing when existing plans were put into place or the proposed date that plans to address risk are to be implemented by the organization.

Risk Map

Identifying risks by transferring them from the risk register and graphically depicting them on a heat map. Risks are plotted using their likelihood and impact scores. The risk map positions likelihood on a scale along the x-axis against impact or consequences on a scale along the y-axis (Table 4.2.2). The level of risk is calculated by adding the likelihood score to the impact of consequences score. The heat map is colourized into green, yellow and red sectors. A likelihood score of 5 and an impact or consequences score of 5 would place a risk in the top right-hand corner of the risk map in a red-coloured sector. This would be a risk that would not be acceptable to an organization under normal circumstances as it would very likely fall outside of the organization's risk appetite. Identified risks in this sector should be addressed by stopping the activity that is causing this level of risk or by taking steps to reduce the likelihood or impact/consequences of the risk. In comparison, a risk with a likelihood score of 1 and an impact or consequences score of 1 would place the risk in the green sector of the risk map. Risks in the green sector are normally tolerated by the organization without any further action required as they would fall within the organization's appetite for risk. An organization can create a variation of the basic risk map that traces an inherent risk (red sector) where there has been no attempt to respond to the likelihood or impact consequences of the risk through to the risk that has been left over after a risk response (residual risk) in the yellow sector. If the organization is not satisfied with the level of risk after the initial risk response, then further risk responses may be required to shift the risk into the green sector, where it would be considered as a target or optimum risk that falls within the organization's risk appetite. Risks that are identified on the risk map as being outside of the scope of the organization's risk appetite must be addressed. Risk responses are decisions that will be based on the outcome of a risk assessment, the identification and analysis of the organization's risks.

Table 4.2.2: Basic Risk Map. See the description below for an accessible description.

Impact							
	5						Major Risk
	4						
	3						Moderate Risk
	2						
	1						Minor Risk
		1	2	3	4	5	
		Likelihood					

Table Description

A table with numbers from 1-5 going up for Impact and 1-5 from left to right along the bottom for Likelihood.

The top corner (5/5) is labelled Major Risk in red. The mid-way row is labelled Moderate Risk in yellow, and the bottom is labelled Minor Risk in green.

4.3 CHAPTER SUMMARY

Summary

Chapter 4: Risk Identification explores the critical process of identifying potential risks that could impact an organization, either positively or negatively. The chapter outlines that after scanning the environment, risk identification is the next crucial step in risk management, defined by the ISO as finding, recognizing, and describing risks. It emphasizes the importance of a holistic approach to risk management, where risks are managed across the organization rather than isolated within individual departments. This approach, known as Enterprise Risk Management (ERM), integrates hazard, operational, financial, and strategic risks, allowing organizations to understand how different risks interconnect and influence each other. For example, a fire at a distribution center could disrupt IT systems, causing cascading operational risks.

The chapter details various types of risks: known, emerging, inherent, and residual. It also explains two primary approaches to risk identification—top-down and bottom-up—each with its advantages and disadvantages. Effective risk identification strategies involve a team approach, including brainstorming, workshops, SWOT analysis, document reviews, root cause analysis, physical inspections, and expert opinions (e.g., Delphi technique). Additionally, the chapter introduces tools such as the risk register and risk map to organize and visualize risks, emphasizing the need for organizations to assess, prioritize, and respond to risks based on their likelihood and impact. These tools help in creating a comprehensive risk management framework, guiding organizations in maintaining risks within their risk appetite and addressing those that exceed acceptable levels.

OpenAI. (2024, July 2). *ChatGPT.* [Large language model]. https://chat.openai.com/chat

Prompt: *Please take the chapter content in this document attached and summarize the key concepts into no more than two paragraphs. Reviewed by authors.*

Key Terms

- **Bottom-up approach** has the advantage of providing an abundance of information from personnel working within and throughout the organization.
- **Emerging risks:** risks that are not known to the organization.
- **Enterprise Risk Management** allows an organization to holistically manage all its key risks as well as opportunities that might exist.
- **Holistic risk management** allows the organization to see how potential risks and opportunities fit together across the four classifications of hazard, operational, financial and strategic risks.
- **Inherent risks:** risks that have not been managed or treated.
- **Known risks:** risks that the organization knows about or that have previously affected the organization.
- **Residual risks:** the risk that remains after the risk has been managed or treated.
- **Risk identification** is defined by the International Organization for Standardization (ISO) as the "process of finding, recognizing and describing risks."
- **Risk register** is a risk management tool that identifies all the risks in an organization across individual scenarios, processes, sectors and locations.
- **Top-down approach** is when the senior management in the organization makes decisions on the risks that can have a positive or negative effect on the organization.

CHAPTER 5: RISK ANALYSIS

Chapter Overview

5.0 LEARNING OUTCOMES

Learning Objectives

At the end of this chapter, students will be able to:

- Describe the importance of risk assessment
- Summarize the most common risk analysis techniques
- Identify quantitative and qualitative risk analysis techniques
- List traditional risk analysis techniques
- Explain root cause analysis

5.1 WHAT IS RISK ASSESSMENT

Risk Assessment is the process of identifying, analyzing and evaluating risk. Risk assessment must be systematic, iterative and collaborative, using the stakeholders' knowledge. It should be based on the most recent information and supported by further research as required.

1. **Risk Identification**. This is the process of finding, recognizing, and describing potential risks that can support or threaten a project's achievement of its objectives (ISO, 2018). The project team should use a wide range of techniques to identify risks which affect one or more objectives.
2. **Risk Analysis**. This is a comprehensive analysis of risk, based on its characteristics (ISO, 2018). This involves considering risks, sources, consequences, likelihood, triggers, contingencies, controls and control effectiveness. A key consideration is risk exposure, which refers to the risk likelihood and consequence levels. A risk can have numerous causes and consequences and affect multiple objectives or goals.
3. **Risk Evaluation**. This process is used to support decision-making. It involves comparing the results of the risk analysis process to the pre-defined risk criteria, which outlines when further action is required (ISO, 2018). This can lead to a decision to transfer, avoid, treat/mitigate, approve, or reject.(Reaiche et al., 2022).

Figure 5.1.1: The five steps of the Enterprise Wide Risk Management Process.

Importance of Risk Assessment

Risk assessment is the foundation of a strong Enterprise Risk Management (ERM) program. It's the first step in understanding the potential threats an organization faces. Here's why risk assessment is so crucial:

- *Identify threats:* Risk assessment helps uncover potential issues, both internal (e.g., process breakdowns) and external (e.g., economic shifts).
- *Prioritize effectively:* Risk assessment helps categorize threats based on likelihood and impact, allowing resources to be focused on the most critical issues.
- *Informed decision-making*: With a clear understanding of risks, one can make better choices about resource allocation, strategic direction, and risk mitigation strategies.
- *Proactive approach*: Identifying risks early can avoid them altogether or lessen their impact. This proactive approach can save an organization time, money, and reputation.
- *Regulatory compliance*: Many industries have regulations requiring organizations to have a risk management plan. A strong risk assessment is a key component of demonstrating compliance.

Risk assessment is the cornerstone of a successful ERM program. It provides the information required to make informed decisions, protect the organization, and achieve goals.

Risk Assessment Approaches

There are two approaches for assessing risks: top-down and bottom-up. Both approaches are strategies for conducting risk assessments, but they differ in where the assessment process starts and who is involved. Apart from the starting point, they have different focuses, advantages, and disadvantages. Risks associated with strategies can be assessed more effectively when approached through a top-down approach, whereas, for hazard and operational risk, a bottom-up approach may give better results.

Top-Down Approach

This approach starts with senior management or executives identifying and assessing risks that could impact the organization's overall strategic objectives and goals. This approach focuses on high-level, enterprise-wide risks such as strategic, financial, operational, and reputational risks.

The **top-down approach** ensures that risk management is aligned with the organization's strategic direction and priorities. It provides a comprehensive view of risks that could significantly impact the entire enterprise (Howell, 2024).

Bottom-up Approach

The **bottom-up approach** involves identifying and assessing risks at the operational or functional levels of the organization, such as individual projects, processes, departments, or business units. This approach relies on input from employees closest to the day-to-day operations, who have first-hand knowledge of potential risks in their respective areas. For example, project, process, compliance, and health and safety risks.

The bottom-up approach ensures that risk management is grounded in the realities of the organization's operations and captures risks that may not be visible at the higher levels (Howell, 2024).

Combining Top-Down and Bottom-Up Approaches

Most organizations recognize the importance of using top-down and bottom-up approaches in risk management practices. The top-down approach provides a strategic perspective, while the bottom-up approach offers a granular, operational view. By combining these approaches, organizations can comprehensively understand risks at all levels and develop effective risk mitigation strategies. The integration of top-down and bottom-up approaches can be facilitated through establishing a risk management culture that encourages collaboration and information sharing across all levels.

By adopting a holistic approach that incorporates both top-down and bottom-up perspectives, organizations

can effectively identify, assess, and manage risks, ultimately enhancing their ability to achieve their strategic objectives while minimizing potential negative impacts (Howell, 2024).

5.2 RISK ANALYSIS

The main objective of risk analysis is to equip decision-makers/organizations with enough information using different techniques and tools to make informed decisions on the risks identified, from setting up a priority to suitable risk management approaches.

Risk Analysis Approaches

Risk Analysis evaluates the likelihood and Impact (consequence) of each potential risk and prioritizes these risks, generally determined as:

Risk = Likelihood × Consequence

When risks have been identified, they need to be evaluated, either qualitatively or quantitatively, to determine their level of influence and consequence on the organization. This will ensure that appropriate steps can be planned to mitigate or treat them.

There are several ways to assess a potential risk's likelihood and impact (consequences), mainly divided into qualitative and quantitative analyses.

Quantitative Risk Analysis: This approach uses mathematical models and simulations to assign numerical values to risk. An objective approach that uses numerical data and statistical methods to assess and prioritize risks.

Qualitative Risk Analysis: It relies on a person's subjective judgment to build a theoretical risk model for a given scenario and subjective assessments to evaluate risks. It aims to predict the likelihood and impact of risks.

Level of Risks and Assessing Controls

Risks are illustrated in the 'Risk Matrix,' which shows their current level of risk. When analyzing risks, there are three key levels are considered: inherent risk, current/residual risk, and target risk. These levels provide a comprehensive view of the risk landscape and aid in effective risk management.

Inherent Risk

Inherent risk represents the level of risk before any controls or mitigating actions are implemented. It is the risk that exists in the absence of any countermeasures or safeguards. Assessing inherent risk helps organizations understand the magnitude of potential threats or vulnerabilities if left unaddressed.

Current/Residual Risk

Current risk, also known as residual risk, is the level of risk that remains after considering the existing controls and mitigation measures currently in place. It reflects the risk exposure that the organization is currently accepting or managing with its current risk management practices and control environment.

Target Risk

Target risk represents the desired or acceptable level of risk that an organization aims to achieve or maintain. It is the risk level that aligns with the organization's risk appetite and tolerance levels. Target risk serves as a benchmark or goal for risk management efforts, guiding the implementation of additional controls or mitigation strategies.

Analyzing these three levels together provides a comprehensive understanding of the risk landscape and enables informed decision-making. Whereas we do understand controls that may bring down the inherent risk to current/residual to the target level of risk. (Figure 5.2.1)

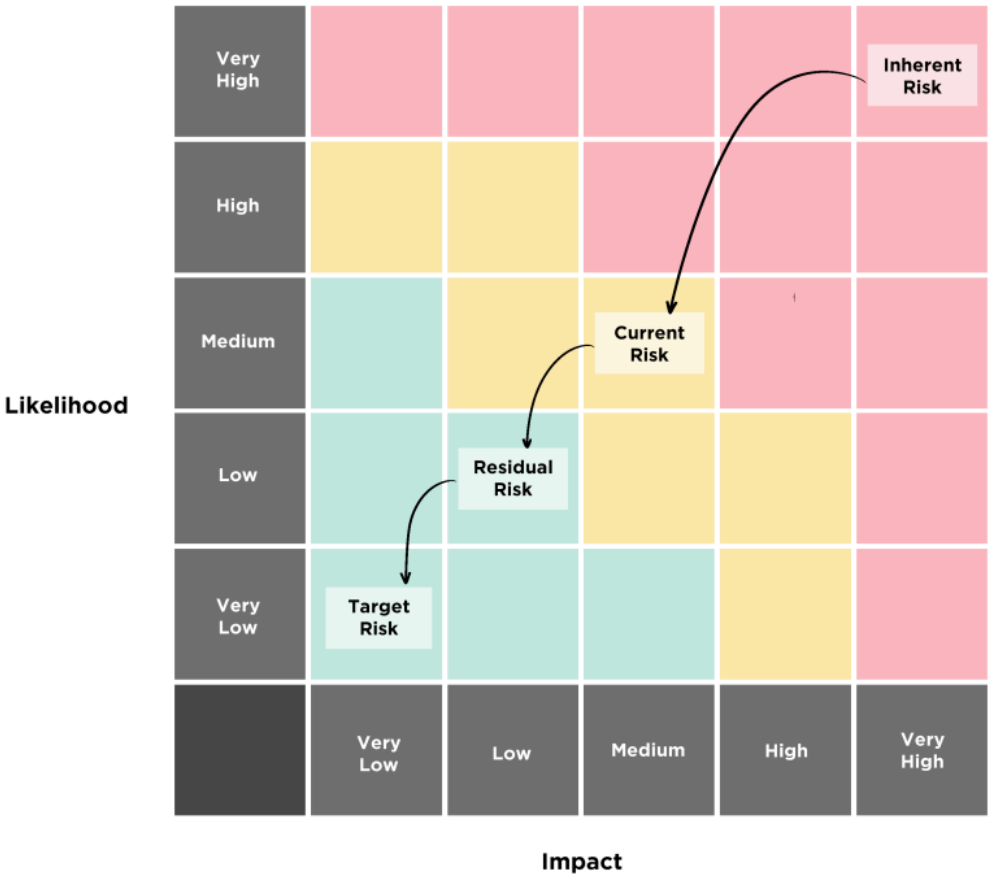

Figure 5.2.1: "Risk Matrix" by Sanaz Habibi, CC BY-NC-SA 4.0

Image Description

A matrix grid with Likelihood on the vertical and Impact on the horizontal. Segments are Very Low, Low, Medium, High, & Very High.

Squares noted as Likelihood-Impact.

Squares Very Low-Very High, Low-Very High, Medium-Very High, Medium-High, High-Medium, High-High, High-Very High, Very High-Very Low, Very High-Low, Very High-Medium, Very High-High, Very-High-Very High coloured red.

Squares Very Low-High, Low-Medium, Low-High, Medium-Low, Medium-Medium, High-Very Low, & High, Low coloured yellow.

Squares Very Low-Very Low, Very Low-Low, Very Low-Medium, Low-Very Low, Low-Low, Medium-Very Low coloured green.

Very High-Very High noted as Inherent Risk.

Medium-Medium noted as Current Risk.

Low-Low noted as Residual Risk.

Very Low-Very Low noted as Target Risk.

5.3 RISK ANALYSIS TECHNIQUES

Net Present Value (NPV)

Present Value

Risk managers will be faced with situations where they will need to know the current or present value of money that will be received or paid out in the future. For example, how much money must be invested today to generate funds that are sufficient to pay a sprinkler system at a specific time in the future.

Money that is invested at a given interest rate will increase in value over a given period. For this reason, its present value will be less than its future value. The future value of a sum of money that is to be received is dependent on the rate of return and the number of periods over which it would receive that rate of return.

Simply put, the present value is today's value of money that is to be received in the future. Discounting is the process that is used to calculate present values.

A dollar today is worth more than a dollar tomorrow!

The formula to calculate present value is as follows:

$$PV = \frac{FV_n}{(1+r)^n}$$

n = Number of periods

r = Rate of return

FV_n = Future value of money that must be discounted

Example

At the end of one year, $11,500 needs to be in a savings account that pays 3 percent interest compounded annually. Using the present value table, determine how much must be deposited in the account today to have $11,500 in one year.

Solution

$$PV = \frac{FV_n}{(1+r)^n}$$

$$PV = \frac{\$11,500}{(1+0.03)^1}$$

$$PV = \frac{\$11,500}{1.03}$$

$$PV = \$11,165$$

$11,165 must be deposited in the account today to have $11,500 in the account in one year.

Net Present Value

Net present value is the difference between the present value of all future cash inflows, including the salvage value of assets, and the present value of cash outflows over a period.

For example, a risk manager may want to know whether investing in an initiative today, which is a cash outflow, will save money on future costs, which are cash inflows based on saving expenses.

The Net Present Value Equation is expressed as:

$$NPV = -C_o + \frac{C_t}{(1+r)^t} + \ldots + \frac{C_n}{(1+r)^n}$$

C_o = Cash flow at beginning of project
C_t = Payment at period t for t = 1, through $t = n$
r = Discount rate
n = Number of periods

Net present value (NPV) is the difference between the present value of cash inflows and the present value of cash outflows.

NPV = PV (sum of the benefits) – ***PV*** (initial costs)

An investment should not be made when the Net Present Value (NPV) is negative. In contrast, a positive NPV would be indicative of an investment that should be made.

Example

A risk manager overseeing a chain of fitness clubs is deciding if an investment of $50,000 on a 2-year preventive maintenance program for the equipment in the clubs is a good idea. The fitness clubs require a return on investment of 6% and expect to save $15,000 on maintenance costs at the end of the first year and $20,000 on maintenance costs at the end of the second year.

Solution

$$NPV = -C_o + \frac{C_t}{(1+r)^t} + \ldots + \frac{C_n}{(1+r)^n}$$

$$NPV = -\$50,000 + \frac{\$15,000}{(1+0.06)^1} + \frac{\$20,000}{(1+0.06)^2}$$

$$NPV = -\$50,000 + \$14,150 + \$17,800$$

$$NPV = -\$18,050$$

Since the *NPV* is negative the investment in the preventive maintenance program should not be made

---

Probability Analysis

Probability analysis involves quantifying uncertainties associated with various events or scenarios. By assigning probabilities to different outcomes, risk analysts can assess the likelihood of specific events occurring and their potential impact on a system, process, or project.

Several methods/concepts can be used to calculate probability, such as the law of large numbers, theoretical probability, empirical probability, and probability distributions (Hillson & Hulett, 2004).

However, there are two main ways to do this: the empirical approach and the theoretical approach.

The **Empirical Approach** uses real-world data and past experiences. It looks at what has happened before to guess what might happen in the future. This method works well when we have lots of information about past events. It's like learning from history to predict the future (Halton, 2024).

On the other hand, the **Theoretical approach** uses math and models to calculate probabilities. It doesn't need past data. Instead, it uses logical reasoning to figure out what might happen. This method is useful when we're dealing with new situations or when we don't have much historical information.

Both approaches have their strengths and weaknesses. The empirical approach is great when we have lots of past data, but it might not work well for new or quickly changing situations. The theoretical approach can handle new scenarios, but it might need complex math and could be wrong if its basic assumptions are incorrect (Halton, 2024).

Let's examine how each approach would determine the probability of getting heads when flipping a fair coin.

Example

Empirical Approach

In this approach, we would actually flip a coin multiple times and record the results. Let's say we flip a coin 100 times and get the following results:

- Heads: 52 times
- Tails: 48 times

Using the empirical approach, we would calculate the probability of getting heads as:

Probability of Heads = Number of Heads ÷ Total Number of Flips
= 52 ÷ 100 = 0.52 or 52%

This probability is based on actual observed data. If we increased the number of flips to 1000 or 10,000, we would expect the result to get closer to 50%.

Theoretical Approach

In the theoretical approach, we would analyze the coin and the flipping process without actually flipping the coin. We know that a fair coin has two sides: heads and tails. Assuming the coin is perfectly balanced and the flip is fair, we can deduce that:

- There are two possible outcomes (heads or tails)
- Each outcome is equally likely

Using probability theory, we can calculate:

Probability of Heads = Number of favourable outcomes ÷ Total number of possible outcomes
= 1 ÷ 2 = 0.5 or 50%

This theoretical probability is based on logical reasoning and the assumption of a fair coin and fair flip without needing to actually perform any coin flips.

Comparison

The theoretical approach gives us the exact 50% probability we expect from a fair coin. The empirical approach gave us 52%, which is close to but not exactly 50%. This difference illustrates a

key point: empirical results can vary due to random chance, especially with smaller sample sizes. As we increase the number of flips in the empirical approach, we would expect the result to converge toward the theoretical 50% probability (Halton, 2024).

In real life, risk managers often use both approaches together. This helps them get a fuller picture of possible risks. They might use empirical data where it's available and theoretical models where it's not.

Regression Analysis

Regression analysis is a statistical technique employed in risk assessment to identify relationships between variables and ultimately predict the potential severity of loss events. It is one of the most widely used associative forecasting methods, which involves constructing a mathematical equation that relates the dependent variable to one or more independent variables. This statistical technique estimates the relationships between variables. It encompasses a diverse set of methods for modelling and analyzing the interplay between a dependent variable (the variable being forecast) and one or more independent variables (factors believed to influence the dependent variable). Regression analysis is particularly valuable for understanding how changes in independent variables impact the average value of the dependent variable while holding all other independent variables constant.

The coefficients of the independent variables in the regression equation represent the magnitude and direction of their impact on the dependent variable.

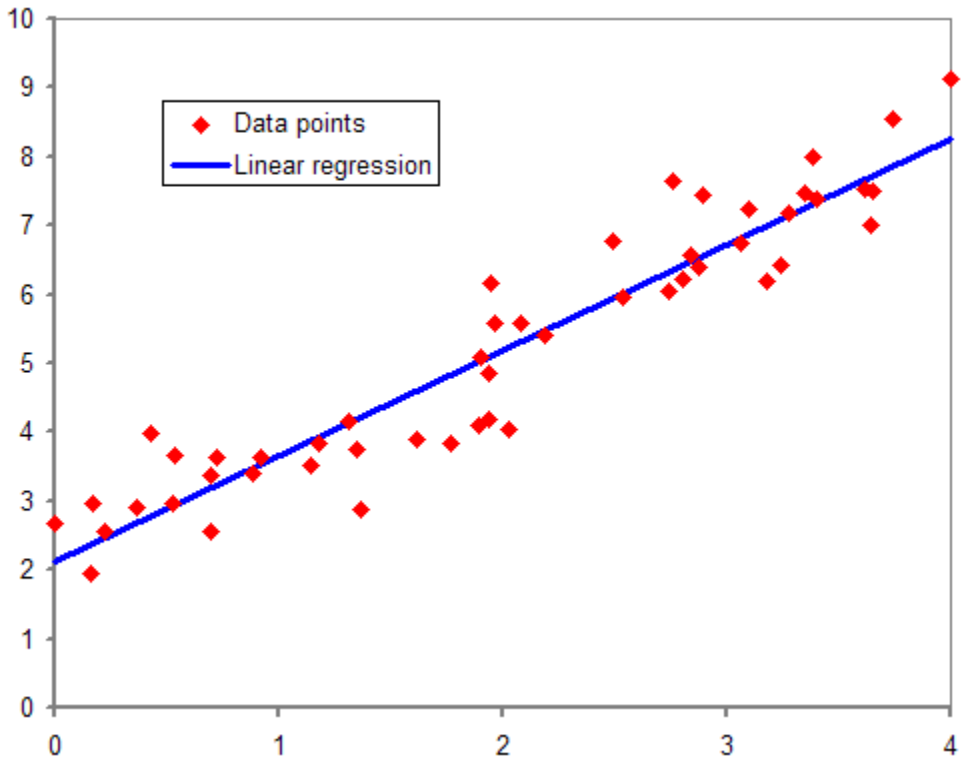

Figure 5.3.1: "Example of regression analysis." by Amatulic **public domain**

Image Description

The image is a scatter plot depicting data points and a linear regression line. The x-axis ranges from 0 to 4. The y-axis ranges from 0 to 10. The red diamonds represent the data points. The blue line represents the linear regression line, showing the best-fit line through the data points.
The data points follow an upward trend, indicating a positive correlation between the variables. The linear regression line slopes upward from left to right, suggesting a strong linear relationship. The legend in the plot identifies the red diamonds as "Data points" and the blue line as "Linear regression."

Regression analysis provides several benefits in risk assessment, including:

- Quantifying the influence of multiple risk factors simultaneously
- Identifying the most significant risk drivers
- Developing predictive risk models for forecasting purposes
- Supporting risk-based decision-making through quantitative risk estimates

Regression models' accuracy depends on data quality, assumptions' validity, and the appropriate selection of

techniques. Residual analysis, model diagnostics, and expert judgment are often used to evaluate and refine regression models in risk assessment applications (Edwards, 2024).

Loss Exposures

Loss exposures refer to situations or circumstances that may lead to financial losses for an individual, organization, or entity. These exposures can arise from various sources, such as property damage, liability claims, or other risks. Analyzing loss exposures is a critical step in risk management, as it helps identify potential risks and develop strategies to mitigate them.

Dimensions of Loss Exposures

When analyzing loss exposures, risk management professionals consider four key dimensions:

1. Loss Frequency is the number of losses during a specific period.
2. Loss Severity is the seriousness of a specific occurrence.
3. Total Dollar Losses is the total dollar amount of losses incurred across all occurrences during a specific period.
4. Timing refers to the points at which losses occur and when loss payments are made. Importance of Analyzing Loss Severity

Analyzing loss severity helps to understand the potential financial impact of a loss event. By assessing severity, they can prioritize risks and allocate resources effectively. For instance, a high-severity risk may require more attention and preventive measures than a low-severity risk.

Approaches for Jointly Analyzing Loss Frequency and Severity

The **Prouty Approach** is a qualitative technique used in risk assessment to determine how to treat different risks based on their potential frequency (likelihood) and severity (impact) of loss.

This approach is typically depicted using a risk matrix that maps the probability of a loss occurring (frequency)

on one axis against its potential consequence (severity) on the other axis. Risks are then plotted on this matrix and treated according to which zone they fall into.

(Onischuk, 2023)

The Prouty Approach

		Loss Frequency			
		Almost Nil	**Slight**	**Moderate**	**Definite**
Loss Severity	**Severe**	Transfer	Reduce/Prevent	Reduce/Prevent	Avoid
	Significant	Retain	Transfer	Reduce/Prevent	Avoid
	Slight	Retain	Transfer	Prevent	Prevent

Events Consequences Analysis

Decision Tree Analysis

Decision trees provide a graphical framework for depicting a decision-maker's available choices (actions), potential outcomes (events), and interdependencies between these. They excel in analyzing situations involving a sequence of interrelated decisions.

Following the tree's construction, the analysis proceeds from right to left, aiming to identify the optimal decision strategy, which translates to a sequence of decisions that maximizes utility. This analysis necessitates three key elements:

- *Decision Criterion:* The benchmark used to assess the desirability of outcomes, often expressed in terms of profit, cost, or a risk-adjusted measure.
- *Event Probabilities:* The likelihood assigned to each potential outcome is crucial for calculating expected values.
- *Outcome Values:* The monetary consequence (revenue or cost) of each decision alternative and chance event.

Example: New Product Launch

Consider a firm contemplating launching a new product versus continuing its existing offering. Launching the new product entails uncertain outcomes contingent upon market demand. High demand translates to a projected profit of $140, while low demand translates to $80. The firm estimates high and low demand probabilities to be 0.7 and 0.3, respectively. Maintaining the existing product guarantees a profit of $110. These estimated profits are depicted at the terminal nodes of the chance branches. Probabilities of high and low demand for the new product are indicated below the corresponding branches emanating from the chance node.

Expected values are calculated by averaging the profits weighted by their respective probabilities. For instance, the expected value at chance node (2) is calculated as (0.7×$140) + (0.3×$80) = $122, which is then inscribed above node (2). Arriving at the decision node (1), we select the alternative with the superior expected value. Since max ($122, $110) = $122, launching the new product is the more profitable course of action.

Procedure

1. List the possible alternatives (actions/decisions).
2. Identify the possible outcomes.
3. List the payoff or profit or reward.
4. Select one of the decision theory models.
5. Apply the model and make your decision (Borrelli, 2015).

Event Tree Analysis

Event tree analysis (ETA) is a forward-looking, inductive technique employed in risk assessment. It systematically explores the potential consequences of a single initiating event, branching out to depict various

sequences of successes and failures that can culminate in different accident scenarios. This approach facilitates the identification of critical pathways that contribute most significantly to system failure.

Key Advantages of Event Tree Analysis

- *Comprehensive Coverage:* ETAs provide a structured framework for analyzing the temporal progression of events, encompassing the interplay between system functionalities, protective safeguards, operator responses, and potential accident outcomes.
- *Probabilistic Assessment:* By assigning probabilities to each branch within the event tree, analysts can quantify the likelihood of various accident scenarios, enabling a more informed risk evaluation.
- *Identification of Critical Pathways:* ETAs pinpoint the sequence of events with the highest probability of leading to system failure, guiding efforts towards targeted risk mitigation strategies.

Applications and Effectiveness

While broadly applicable to diverse risk assessment scenarios, ETAs are particularly well-suited for analyzing complex systems equipped with multiple safety barriers. Their strength lies in systematically dissecting the potential consequences of an initiating event, revealing the interplay

between system behaviour, safeguard effectiveness, and human intervention. This facilitates the identification of critical vulnerabilities and the development of effective risk mitigation strategies.

Overall, event tree analysis is a valuable tool within the probabilistic risk assessment framework, offering a structured and systematic approach to identifying and evaluating potential accident scenarios (Borrelli, 2015).

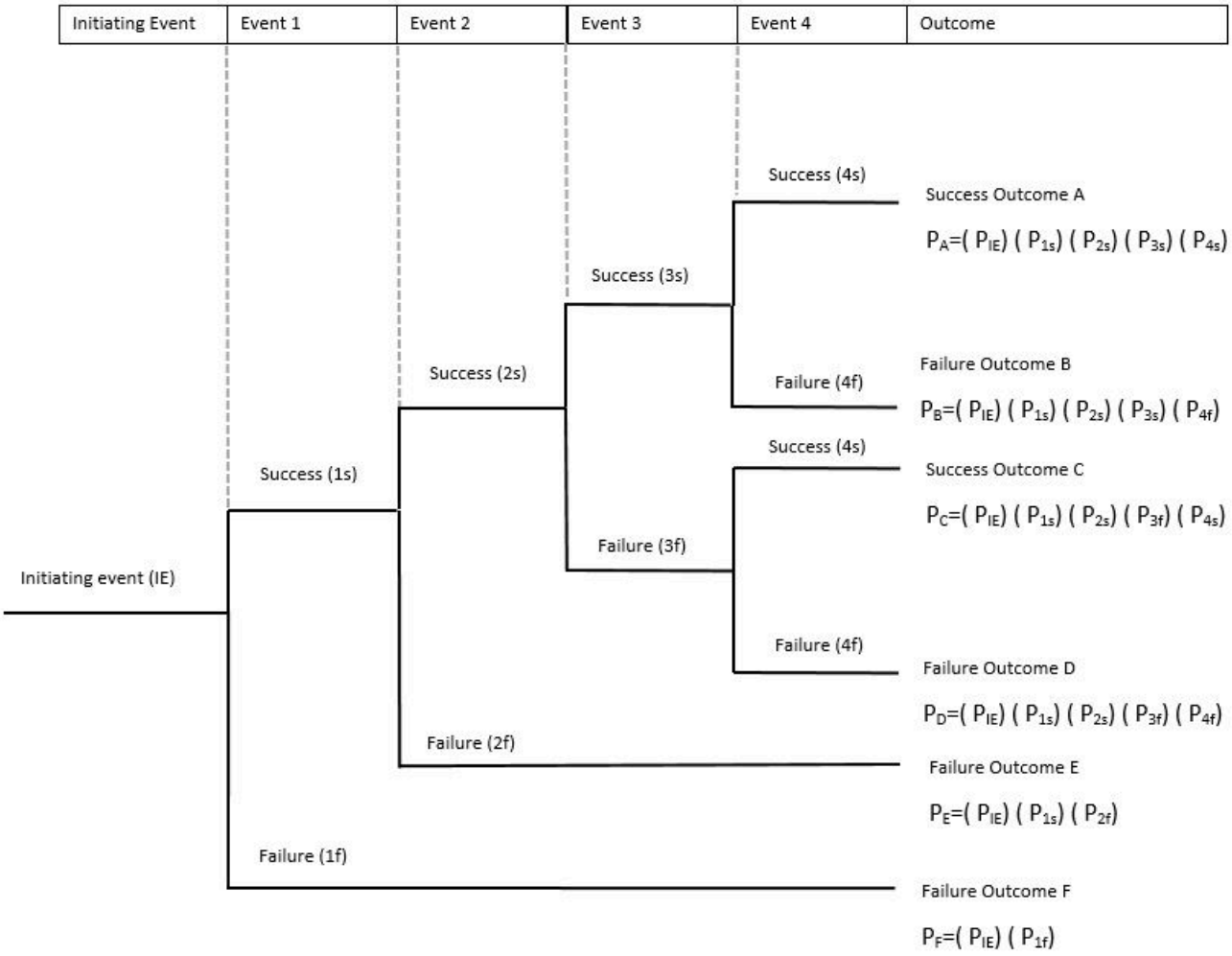

Figure 5.3.1: "Event Tree Diagram" by 570SJR, CC BY-SA 3.0.

Image Description

It starts with an "Initiating Event (IE)" at the bottom, which branches into two possible events labelled "Event 1" with outcomes "Success (1s)" and "Failure (1f)." Each of these outcomes leads to further events, numbered 2 to 4, each also having success and failure branches. The final column lists the overall outcome as either "Success Outcome (S)" or "Failure Outcome (F)," with associated probabilities P(S|E) and P(F|E) for success and failure given event E, respectively.

Success Outcome A: $P_A=(P_{IE})(P_{1s})(P_{2s})(P_{3s})(P_{4s})$

Failure Outcome B: $P_B=(P_{IE})(P_{1s})(P_{2s})(P_{3s})(P_{4f})$

Success Outcome C: $P_C=(P_{IE})(P_{1s})(P_{2s})(P_{3f})(P_{4s})$

Failure Outcome D: $P_D=(P_{IE})(P_{1s})(P_{2s})(P_{3f})(P_{4f})$

Failure Outcome E: $P_E=(P_{IE})(P_{1s})(P_{2f})$

Failure Outcome F: $P_F=(P_{IE})(P_{1f})(P_{2f})$

Steps

1. Define the system.
2. Identify the accident scenarios.
3. Identify the initiating events.
4. Identify intermediate events.
5. Build the event tree diagram.
6. Obtain event failure probabilities.
7. Identify the outcome risk.
8. Evaluate the outcome risk.
9. Recommend corrective action.
10. Document the entire process.

Business Impact & Strategic Analysis

Fault Tree Analysis – FTA

Fault tree analysis (FTA) is a deductive, top-down approach to system reliability and safety analysis. Pioneered by Bell Laboratories, FTA systematically decomposes an undesired top-level event (failure) into its constituent basic events. Figure 5.3.2 is an example of a Fault-Tree analysis that goes from the system failure or consequences and follows the sequence of events backward to determine the system failure. The fish-tailed shape symbols are designated '***or gates***,' meaning that only one event below them is required to occur to cause the event. The dome-shaped symbols are designated '***and gates***,' meaning that an event can occur only if all events below them occur in sequence. For example, for the top event shown in the figure to occur, one of the events identified under the 'or gates' as 1, 2 or 6 must occur first. In comparison, for the top event in the figure to occur, all of the events identified under the 'and gates' as 3, 4, 5 or 7 and 8 must occur.

This methodology facilitates the identification of all possible combinations of hardware failures, software malfunctions, and human errors that could lead to the undesired outcome (Borrelli, 2015).

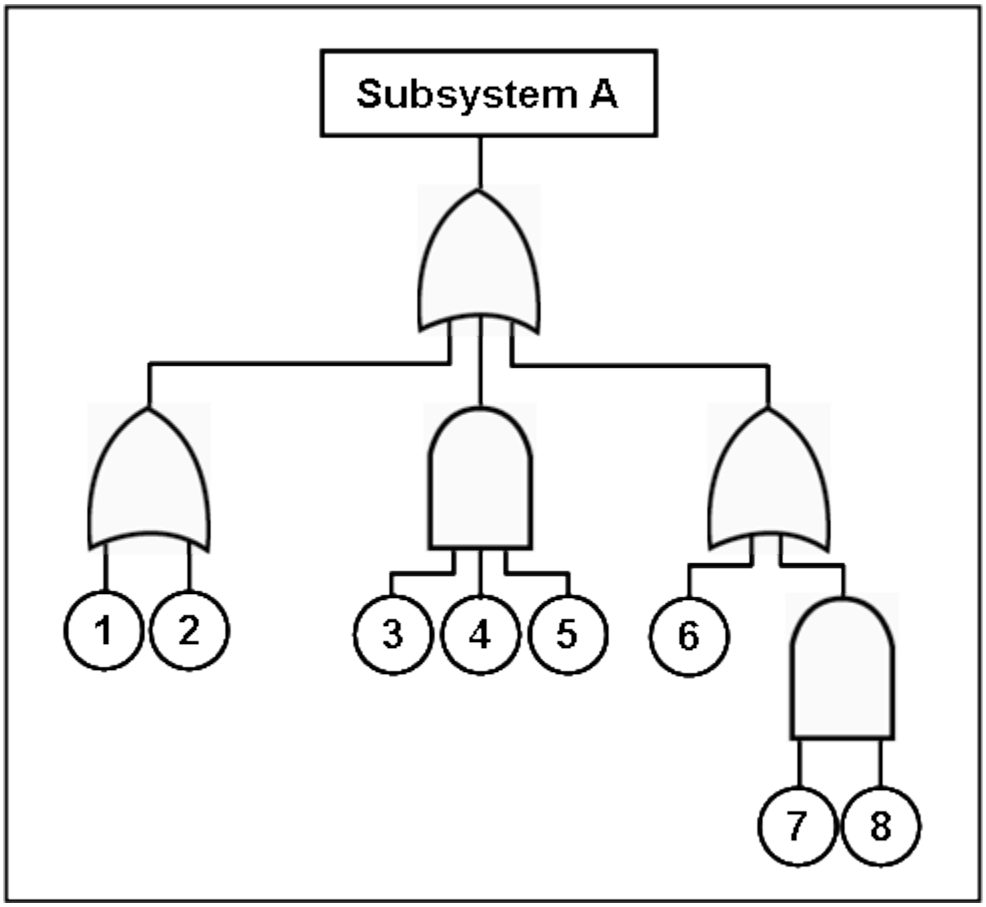

Figure 5.3.2: "Fault Tree" by U.S Federal Government, Public domain.

Image Description

The diagram starts with "Subsystem A" at the top, followed by an "OR" gate directly below it. Below the "OR" gate, there are three symbols arranged horizontally from left to right: an "OR" gate, an "AND" gate, and another "OR" gate. The first "OR" gate has two base events numbered 1 and 2. The second "AND" gate has three base events numbered 3, 4, and 5. The third "OR" gate has one base event numbered 6 and an "AND" gate with two base events numbered 7 and 8.

Methodology

- Define undesired events.
- Resolved into immediate causes.
- Continue resolution until basic events are identified.

- Construct a fault tree to demonstrate the logical relationships.

Business Continuity Planning

Business Continuity Planning (BCP) is an organization's comprehensive process to identify potential threats and develop strategies to ensure the continuity of critical business operations and services during disruptions or disasters. In risk assessment, BCP is crucial in mitigating risks and minimizing their impact on the organization.

BCP involves several key steps that are closely tied to risk assessment:

- *Risk Identification*: The first step is identifying potential risks that could disrupt business operations. This includes risks from natural disasters (e.g., earthquakes, floods, hurricanes), technological failures (e.g., cyber-attacks, system outages), human-caused events (e.g., terrorism, civil unrest), and other sources.
- *Risk Analysis:* Once risks are identified, organizations conduct a thorough analysis to understand the likelihood of occurrence and the potential impact on critical business functions, assets, and resources. This analysis helps prioritize risks based on their severity and probability.
- *Business Impact Analysis (BIA):* A BIA is performed to determine the potential consequences of disruptions on the organization's operations, processes, and resources. It identifies critical business functions, dependencies, and recovery time objectives, providing insights into risks' potential financial and operational impacts.
- *Risk Mitigation Strategies*: Based on the risk analysis and BIA, organizations develop strategies to mitigate or minimize the identified risks. These strategies may include preventive measures, contingency plans, recovery procedures, and continuity plans to ensure the continuation of critical business functions during and after a disruptive event.
- *Plan Development*: A comprehensive BCP is developed, documenting the strategies, procedures, and resources required to respond to and recover from disruptions. The plan outlines roles, responsibilities, communication protocols, resource allocation, and testing and maintenance procedures.
- *Testing and Maintenance*: Regular testing and exercising of the BCP are essential to validate its effectiveness and identify areas for improvement. The plan should be reviewed and updated periodically to reflect changes in the organization's operations, risks, and regulatory requirements.

By integrating risk assessment into the BCP process, organizations can proactively identify and mitigate

potential risks, minimize the impact of disruptions, and ensure the continuity of critical business operations, ultimately enhancing their resilience and competitiveness (Setiawan et al., 2017).

SWOT Analysis

SWOT stands for Strengths, Weaknesses, Opportunities, and Threats. It was explained in Chapter 4 as an effective risk identification strategy, but it should be noted that it is also effective in analyzing risks. In risk analysis, SWOT analysis helps identify and categorize potential risks and risk factors into these four categories:

1. *Strengths*: Internal factors or capabilities that can help mitigate risks or enhance the ability to manage risks effectively. These could include skilled personnel, robust processes, financial resources, environment, or competitive advantages.
2. *Weaknesses*: Internal vulnerabilities or deficiencies that can increase the likelihood or impact of risks. Examples include lack of expertise, outdated technology, limited resources, or inefficient processes.
3. *Opportunities*: External factors or situations that, if capitalized upon, can help reduce risks or create new opportunities for risk mitigation. These could include favourable market conditions, new technologies, strategic partnerships, or regulatory changes.
4. *Threats*: External factors or events that can pose risks or challenges to the project or organization. Examples include competition, economic downturns, political instability, natural disasters, or changes in customer preferences.

The SWOT Analysis Process in Risk Analysis Typically Involves The Following Steps

1. *Identify Risks*: Conduct a brainstorming session or use other risk identification techniques to list potential risks that could impact the project or organization.
2. *Categorize Risks*: Classify the identified risks into the four SWOT categories (Strengths, Weaknesses, Opportunities, and Threats) based on their nature and source (internal or external).
3. *Analyze Interactions*: Examine how the identified strengths, weaknesses, opportunities, and threats interact and influence the overall risk landscape. For example, strengths can help mitigate weaknesses or threats, while opportunities can be leveraged to address weaknesses or capitalize on strengths.
4. *Develop Risk Strategies*: Based on the SWOT analysis, develop risk response strategies

that leverage strengths, address weaknesses, exploit opportunities, and mitigate threats. These strategies may include risk avoidance, mitigation, transfer, or acceptance.

5. *Monitor and Review*: Monitor the SWOT factors and update the risk analysis as the project or organizational environment changes. Adjust risk strategies accordingly.

By conducting a SWOT analysis in risk analysis, organizations can comprehensively understand their internal and external risk factors, identify potential risk interactions, and develop effective risk management strategies tailored to their specific strengths, weaknesses, opportunities, and threats (Hall, 2024).

Cause and Effect Analysis

Fishbone Diagram

The **Fishbone Diagram,** or Ishikawa Diagram, is an analytical tool that investigates the causes of an event. It provides a systematic way to explore and visualize the root causes contributing to a specific effect or undesirable outcome.

Fishbone Diagram is a powerful tool that helps organizations identify and analyze the potential causes of risks or failures in a project or process. The diagram resembles a fish skeleton, with the "effect" or problem represented by the fish's head and the potential causes branching off like bones from the backbone (Oktaviani et al., 2021).

The Main Steps Involved in Fishbone Diagram

- Define the Effect or Problem
- Identify Main Cause Categories
- Brainstorm Potential Causes
- Analyze and Prioritize Causes

- Develop Countermeasures
- Monitor and Review

A critical component of the Fishbone Diagram is the 5-Whys Analysis. The **5-Why Analysis** is a structured problem-solving technique used in risk assessment to identify the root causes of potential risks or undesirable events. It involves repeatedly asking the question "Why?" to peel back layers of symptoms and uncover the underlying root causes.

The 5-Why Analysis is instrumental during risk assessment's risk identification and analysis phases. Systematically exploring the causal relationships behind a potential risk event helps organizations gain a deeper understanding of the root causes and develop effective mitigation strategies.

The Main Steps Involved in The 5-Why Analysis in A Risk Assessment Context

- Define the Risk Event
- Ask "Why?" and Record the Answer
- Repeat the "Why?" Question
- Identify Root Causes
- Develop Countermeasures
- Monitor and Review

Future State Analysis

Scenario Analysis

Scenario analysis is a technique used in risk analysis to evaluate and quantify the potential impacts of uncertainties and risks on desired outcomes or objectives.

It involves creating and analyzing multiple plausible scenarios or future states of the world, each defined by a unique set of assumptions, trends, and events. It helps decision-makers understand how different factors and uncertainties could interact and influence outcomes.

The Following Steps Are Usually Taken in This Technique For Risk Analysis

1. Identify Key Uncertainties
2. Develop Scenarios
3. Assess Impacts
4. Quantify Risks
5. Analyze and Communicate

Scenario analysis is used in various situations for risk analysis, including:

1. Financial Risk Assessment for banks and financial institutions.
2. Climate Change Risk for insurance companies and environmental agencies employ scenario analysis to understand the potential impacts of climate change, such as extreme weather events, sea-level rise, and regulatory changes.
3. Supply Chain Risk for manufacturers and logistics companies analyzes scenarios related to supplier disruptions, natural disasters, or geopolitical events.
4. Pandemic Preparedness for healthcare organizations and public health agencies uses scenario analysis to plan for potential disease outbreaks and assess hospital capacity.
5. Strategic Planning for businesses to leverage scenario analysis to evaluate the risks and opportunities associated with different strategic decisions.

By considering multiple scenarios and quantifying their impacts, scenario analysis provides a structured approach to risk assessment, enabling organizations to make informed decisions, develop risk mitigation strategies, and enhance resilience in the face of uncertainty (Hayes, 2023; Airmic, 2016).

Monte-Carlo Analysis

Monte Carlo analysis is a technique used in risk analysis to quantify the potential impact of uncertainty on a project or decision. It simulates various possible scenarios by considering the randomness or variability of different factors.

Monte Carlo Analysis provides a more comprehensive risk picture than traditional point estimates (best-case, worst-case scenarios). It also helps to identify potential risks that might not have been considered before, allowing better decision-making by understanding the probabilities of various outcomes (Stammers, 2024; Agarwal, 2024).

Human Reliability Analysis

Human Reliability and Error Analysis

Human reliability plays a critical role in the resilience of complex systems, given the potential consequences of human errors or oversights. Whether operating a nuclear reactor, flying an aircraft, driving a car, or managing an industrial plant, understanding human reliability is essential.

Various methods can be employed to analyze human reliability. These include hierarchical task analysis, focusing on critical activities that could lead to hazardous events. The process begins by identifying individual tasks and steps within an activity, highlighting potential errors associated with specific steps, and using prompts to identify error mechanisms (such as skipping a step, performing the right action on the wrong object, or transposing digits).

Once potential error sources are identified, actions are developed to minimize their impact and enhance human performance reliability.

Key steps include evaluating necessary information, identifying pre- and post-task states, understanding information transmission, classifying tasks adequately, recognizing interconnections among staff and actions, and screening critical actions. Additionally, practice-oriented methods help estimate failure probabilities.

Finally, constructing a quantitative fault/event tree—incorporating both component failures and human action failures—allows us to perform dominance analyses, further improving system reliability (Borrelli, 2015).

Failure Modes and Effects Analysis

Failure Modes and Effects Analysis (FMEA) is a foundational technique for quantifying potential risks associated with a system's design. It fosters a systematic approach to analyzing how components or the entire

system might fail and the resultant consequences of such failures, and ultimately, guides design revisions to minimize risk. Notably, risk mitigation can be achieved by reducing the occurrence of failures, mitigating their consequences, or, ideally, both. The difference between a fault-tree analysis and failure mode and effects analysis is that fault-tree analysis goes from consequences to causes. In contrast, failure mode and effects analysis go from causes to consequences.

From an engineering design perspective, FMEA empowers the implementation of robust risk mitigation strategies. This can involve incorporating multiple failure barriers, a concept often called defence-in-depth. Additionally, FMEA can inform the system's strategic use of redundancy and diversity to enhance fault tolerance (Borrelli, 2015).

FMEA Procedure

1. Construct a detailed flow chart of the process.
2. Determine how each step could possibly fail.
3. Determine the "effects" of each possible failure.
4. Assign a Severity Rating for each effect.
5. Assign an Occurrence Rating for each failure.
6. Calculate and prioritize a Risk Priority Number (RPN) for each failure.
7. Review the process and conduct a root cause analysis.
8. Take action to eliminate or reduce the Risk Priority Number.
9. Recalculate the resulting RPN as the failure modes are reduced or eliminated.

5.4 CHAPTER SUMMARY

Summary

Chapter 5 focuses on Risk Analysis, highlighting the systematic process of identifying, analyzing, and evaluating risks. The chapter emphasizes the importance of risk assessment as the cornerstone of Enterprise Risk Management (ERM). It details how risk assessment involves identifying threats, prioritizing them based on likelihood and impact, and making informed decisions to mitigate these risks. This proactive approach not only helps in regulatory compliance but also in protecting an organization's assets and reputation. The chapter further explores the two primary approaches for risk assessment: top-down, which focuses on strategic risks identified by senior management, and bottom-up, which addresses operational risks identified by employees at various levels. Combining these approaches provides a comprehensive understanding of risks across the organization.

The chapter also delves into various risk analysis techniques. Quantitative methods involve mathematical models and statistical methods to assign numerical values to risks, while qualitative methods rely on subjective judgment to evaluate risks. Tools such as the Risk Matrix help illustrate the levels of risk—ranging from inherent to residual and target risks. Additionally, the chapter covers advanced techniques like Net Present Value (NPV), probability analysis, regression analysis, and scenario analysis, which are crucial for making informed risk management decisions. Human reliability and error analysis, along with methodologies like Failure Modes and Effects Analysis (FMEA), are also discussed, providing a thorough approach to identifying and mitigating risks in complex systems.

OpenAI. (2024, July 2). *ChatGPT.* [Large language model]. https://chat.openai.com/chat

Prompt: *Please take the chapter content in this document attached and summarize the key concepts into no more than two paragraphs. Reviewed by authors.*

Key Terms

- **5-Why Analysis** is a structured problem-solving technique used in risk assessment to identify the root causes of potential risks or undesirable events.
- **Bottom-up Approach** involves identifying and assessing risks at the operational or functional levels of the organization, such as individual projects, processes, departments, or business units.
- **Business Continuity Planning (BCP)** is an organization's comprehensive process to identify potential threats and develop strategies to ensure the continuity of critical business operations and services during disruptions or disasters.
- **Current risk**, also known as residual risk, is the level of risk that remains after considering the existing controls and mitigation measures currently in place.
- **Decision Criterion**: The benchmark used to assess the desirability of outcomes, often expressed in terms of profit, cost, or a risk-adjusted measure.
- **Decision Trees** provide a graphical framework for depicting a decision-maker's available choices (actions), potential outcomes (events), and interdependencies between these.
- **Empirical Approach** uses real-world data and past experiences. It looks at what has happened before to guess what might happen in the future.
- **Event Probabilities**: The likelihood assigned to each potential outcome is crucial for calculating expected values.
- **Event tree analysis (ETA)** is a forward-looking, inductive technique employed in risk assessment. It systematically explores the potential consequences of a single initiating event, branching out to depict various sequences of successes and failures that can culminate in different accident scenarios.
- **Failure Modes and Effects Analysis (FMEA)** is a foundational technique for quantifying potential risks associated with a system's design.
- **Fault tree analysis (FTA)** is a deductive, top-down approach to system reliability and

safety analysis. Pioneered by Bell Laboratories, FTA systematically decomposes an undesired top-level event (failure) into its constituent basic events.

- **Fishbone Diagram,** or Ishikawa Diagram, is a structured technique used in risk assessment to identify potential causes of a problem or risk event. It provides a systematic way to explore and visualize the root causes contributing to a specific effect or undesirable outcome. Also known as Cause and Effect Analysis.
- **HAZOP (Hazard and Operability)** analysis is a risk assessment technique to identify potential hazards and operability problems in a system or process.
- **Human Reliability** plays a critical role in the resilience of complex systems, given the potential consequences of human errors or oversights.
- **Inherent risk** represents the level of risk before any controls or mitigating actions are implemented.
- **Loss Exposures** refer to situations or circumstances that may lead to financial losses for an individual, organization, or entity.
- **Monte Carlo analysis** is a technique used in risk analysis to quantify the potential impact of uncertainty on a project or decision. It simulates various possible scenarios by considering the randomness or variability of different factors.
- **Net present value** is the difference between the present value of all future cash inflows including the salvage value of assets and the present value of cash outflows over a period.
- **Opportunities**: External factors or situations that, if capitalized upon, can help reduce risks or create new opportunities for risk mitigation.
- **Outcome Values**: The monetary consequence (revenue or cost) of each decision alternative and chance event.
- **Probability Analysis** involves quantifying uncertainties associated with various events or scenarios.
- **Prouty Approach** is a qualitative technique used in risk assessment to determine how to treat different risks based on their potential frequency (likelihood) and severity (impact) of loss.
- **Qualitative Risk Analysis:** It relies on a person's subjective judgment to build a theoretical risk model for a given scenario and subjective assessments to evaluate risks. It aims to predict the likelihood and impact of risks.
- **Quantitative Risk Analysis:** This approach uses mathematical models and simulations to assign numerical values to risk. An objective approach that uses numerical data and statistical methods to assess and prioritize risks.
- **Regression Analysis** is a statistical technique employed in risk assessment to identify

relationships between variables and ultimately predict the potential severity of loss events.

- **Risk Analysis**. This is a comprehensive analysis of risk, based on its characteristics (ISO, 2018).
- **Risk Assessment** is the process of identifying, analyzing and evaluating risk. Risk assessment must be systematic, iterative and collaborative, using the stakeholders' knowledge.
- **Risk Evaluation**. This process is used to support decision-making. It involves comparing the results of the risk analysis process to the pre-defined risk criteria, which outlines when further action is required (ISO 2018).
- **Risk Identification**. This is the process of finding, recognizing, and describing potential risks that can support or threaten a project's achievement of its objectives (ISO, 2018).
- **Scenario Analysis** is a technique used in risk analysis to evaluate and quantify the potential impacts of uncertainties and risks on desired outcomes or objectives.
- **Strengths**: Internal factors or capabilities that can help mitigate risks or enhance the ability to manage risks effectively.
- **SWOT** stands for Strengths, Weaknesses, Opportunities, and Threats.
- **Target risk** represents the desired or acceptable level of risk that an organization aims to achieve or maintain.
- **Theoretical approach** uses math and models to calculate probabilities. It doesn't need past data. Instead, it uses logical reasoning to figure out what might happen.
- **Threats**: External factors or events that can pose risks or challenges to the project or organization.
- **Top-down Approach** ensures that risk management is aligned with the organization's strategic direction and priorities. It provides a comprehensive view of risks that could significantly impact the entire enterprise (Howell, 2024).
- **TVM** dictates that future cash flows are worth less than present ones due to the potential for investment and earning a return.
- **Weaknesses**: Internal vulnerabilities or deficiencies that can increase the likelihood or impact of risks.

CHAPTER 6: RISK RESPONSE AND RISK TREATMENT

Chapter Overview

6.0 LEARNING OUTCOMES

Learning Objectives

At the end of this chapter, students will be able to:

- Apply Risk Treatment Techniques for risks described under the Enterprise Risk Management Process
- Execute risk control techniques in response to Hazard of Pure Risks and accidental losses used by traditional risk management practitioners

6.1 INTRODUCTION TO RISK RESPONSE AND RISK TREATMENT

After an organization has scanned the environment, identified its risks and analyzed its risks, it must decide on courses of action that must be taken to address the risks that have the potential to affect the organization in either a positive or negative way. The way in which an organization manages its risks is referred to as risk response and risk treatment; it is where the 'rubber hits the road !' with respect to addressing risks.

Risk Response

Risk Response is a broad term that is used to describe the approaches that an organization will use to manage its risks. It is a plan to manage risks derived from information that is received after conducting a risk assessment. As we have learned, the ISO 31000:2018 definition of a risk assessment consists of the identification of risks, the analysis of risks and the evaluation of risks. Note that generic definitions of a risk assessment consist of risk identification and risk analysis and do not include the third step of risk evaluation. An organization can identify and analyze its risks using the strategies that are outlined in Chapter 4 and Chapter 5, respectively.

Risk Register & Risk Map

An excellent way to develop a risk response is using a risk register and map. When a risk map is built from a risk register, the organization's risks are clearly shown in the form of a Risk Matrix. Risks that can potentially affect the organization are placed into quadrants based on the likelihood of the risk occurring and the impact that it has on the organization. This information can be used to develop a risk profile and to evaluate the risks by applying risk criteria to determine the scale and significance of the risks. A risk profile will help an organization understand its risks and the threats that they pose to the organization.

Risk Appetite

Actions taken by the organization to address risks are based on the information contained in the risk profile that is in alignment with the organization's risk appetite. **Risk appetite** is the amount of risk that an organization is willing to retain, tolerate or seek in pursuit of its objectives. Organizations that actively take on risks even in the absence of controls have a high-risk tolerance and are described as being **Risk aggressive**.

In comparison, organizations that are reluctant or unwilling to take on risks have a low-risk tolerance and are described as being **Risk adverse**. There is an upside and a downside to each approach; for example, a risk adverse organization could miss opportunities to move forward with its objectives by not taking on risks. In contrast, a risk aggressive organization is prepared to pursue its objectives by taking on risks in the absence of controls or restrictions, which could either lead to significant gains or losses for the organization. Organizations will often use the concept of risk versus reward as a measurement when taking on risk by positioning risk appetite and tolerance against potential gains or losses.

Risk treatment

Risk treatment describes the specific actions and decisions that an organization will use to modify the upside and the downside of the risks that have been identified and analyzed by the organization. The terms risk treatment and risk control are often used interchangeably as they both modify the likelihood and impact of risks that could advantageously or adversely affect an organization. The subtle difference is that risk treatments are recommended or proposed actions to reduce the likelihood or impact of risks. In contrast, Risk Controls consist of actions that have been taken by the organization to modify the likelihood and impact of risks with the goal of making losses more predictable.

6.2 RISK TREATMENT TECHNIQUES FOR THE ENTERPRISE-WIDE RISK MANAGEMENT PROCESS

The Enterprise-wide risk management process is a five-step process that holistically addresses the upside and the downside of the risks faced by an organization across four risk categories:

- Hazard Risk
- Operational Risk
- Financial Risk
- Strategic Risk

Organizations have the option to choose the language that will be used not only to describe the way that its risks are categorized but also to describe the techniques that are used to treat them. For hazard risks, which are pure risks, the risk treatment should focus on modifying the potential for only negative outcomes. Risk treatments for speculative risks must focus on modifying the outcomes of both positive and negative outcomes. Risk treatment is a continuous process, and the techniques selected to modify risks at one time might no longer be viable in the future. This is particularly true in cases involving emerging risks created by introducing new technologies, changes in existing processes and risks that have developed or evolved beyond their known context.

Risk Control & Risk Financing

When an organization is faced with treating its risks, there are two main options available to the organization. The first option is to use Risk Control to avoid activities that have the potential to cause future losses or to take corrective actions to modify the likelihood and/or impact of risk. The second option is to use Risk Financing techniques to generate funds to pay for loss events. Organizations will often implement elements of both options in combination to create an effective risk treatment package.

Risk Control...Risk Financing or both!

There are five accepted risk treatment techniques that can be used to address the categories of risk included in enterprise risk management:

- Risk Avoidance
- Modifying the likelihood and/or impact of the risk
- Risk Transfer
- Risk Retention
- Risk Exploitation

Risk Avoidance

Risk avoidance is a risk treatment technique that terminates risk by stopping or never undertaking the activity or activities that have the potential to cause a risk to occur. This technique reduces the probability of the loss to zero except in cases where the activity was previously conducted and a decision was made by management not to continue with the activity. When risk avoidance is implemented by an organization as a risk treatment, additional risk treatment techniques are often not required.

The obvious upside to risk avoidance is that the chance loss is removed because the activity is no longer conducted by the organization. The downside is that the organization will lose any benefits or gains that the activity could have provided.

Examples

- An individual who does not drive a car cannot cause an automobile accident because the

activity of driving is avoided.

- When a manufacturer of furniture decides to stop producing its line of baby furniture and cribs due to the potential of product liability actions, the probability of future losses caused by baby furniture is reduced to zero because this activity is avoided. The organization could still face losses from baby furniture and cribs that were manufactured prior to the cessation of their production.
- A fabrication shop that manufactures agricultural equipment spray paints finished products before sending them out to customers. A decision was made by management to contract out spray painting operations due to the complexities and costs of complying with environmental regulations. This example of risk avoidance has a downside because the organization will have the inconvenience and additional expense of transporting the equipment to an offsite facility and paying the contractor for spray painting services, which could lead to a loss of competitive advantage due to a possible price increase. The organization will also face a loss of revenue as it will no longer be including the price of spray painting in its invoices.
- An auto body shop that uses a solvent-based painting system reduces levels of volatile organic compounds by changing to an aqueous or water-based technology. By substituting solvent-based paints with water-based paints, the auto body shop is avoiding the use of more hazardous materials and the requirements to store, dispense and apply them.

Modifying the Likelihood and/or Impact of the Risk

Modifying the likelihood of a risk is a risk treatment technique that involves measures to decrease or change the probability or frequency of the positive or negative effects of a risk through corrective actions or controls. These are steps that are taken by the organization before an event occurs. Likelihood can be measured quantitatively or qualitatively. For example, quantitative analysis could determine that the probability or frequency of a delivery vehicle being involved in an accident is 18%. The qualitative analysis would be based on the experience of the fleet manager and could describe the probability or frequency of an accident as being extremely low, low, moderate, high, or very high.

The other component of this risk treatment technique is modifying the impact of the risk. These are steps that are taken by the organization to reduce the consequences or impact of an event after it has occurred and affected the organization. As with likelihood, impact can be measured using quantitative and qualitative analysis. Quantitative analysis involving the magnitude or size of an event as the result of risk can be measured by calculating the probability of the risk occurring and the consequences or severity associated with the risk.

Qualitative analysis could describe the impact, severity or consequences of the risk by assigning levels such as minimal, moderate or severe ratings.

Often, the approach when using this risk treatment technique is to either modify the likelihood of the risk or to modify the impact of the risk. It is not uncommon to use both elements of this risk treatment technique when responding to a risk.

Examples

- The impact of a fire on a distribution centre would be modified by installing an automatic sprinkler system inside of the premises. Although the sprinkler system will not affect the frequency of a fire, it would lessen its effects by controlling or suppressing the fire once it has started, thereby reducing the consequences. In this case, the risk response will modify the impact of the risk.
- Installing high-security locks on doors and bars on the interior surfaces of windows will modify the frequency of break-and-enter occurrences by intruders. This is an example of modifying the likelihood of the risk.
- A retail operation considering expansion in Canada could take steps to modify the likelihood and impact of this initiative to ensure a positive outcome and to prepare for any negative effects that could arise. The organization is deliberately pursuing this speculative risk with the intention of achieving growth and profits, but there could be a downside associated with taking this opportunity. The negative aspect of this risk would be the need for more profitability achieved by the new location. Additionally, not pursuing this opportunity risk could result in the organization falling behind its competitors and losing market share in that region.
- Organizations can modify the frequency and impact of risks involving commodities by using financial instruments. For example, airlines require fuel to operate aircraft. Aviation fuel is a commodity that is subject to volatility in its price per litre because of many factors. A futures contract is a financial instrument that can be used to lessen the impact caused by an increase in the price of aviation fuel. If an airline agrees to purchase fuel from a supplier for a set price over the next three years to protect itself from the variability of fuel prices, it is using a futures contract to modify the impact of the risk. If fuel prices rise and the airline is locked in at a lower price per litre, it will have a positive outcome and a competitive advantage over its

competitors. A negative outcome will be realized if prices decrease and the airline is locked in at a higher price.

Risk Transfer

Risk transfer is a risk treatment technique that is used to shift the financial responsibilities of future losses to another party. Risk transfer is one of two risk financing techniques that can be used to provide assets and resources to an organization. The second risk financing technique is Risk Retention, which will be discussed after the risk transfer. In almost all cases, risk transfer is applicable to pure risks, which are hazard risks.

An organization can transfer risk using any of the following methods:

- **Guaranteed cost insurance** is a primary risk transfer mechanism involving insurance contracts that provide coverage for insurable perils. A known cost in the form of a premium is paid to the insurance company with the promise that the insurance company will place the organization or individual back into the same financial position that it was in prior to the loss in compliance with the principle of indemnity.
- **Non-insurance contracts** transfer the financial consequences of an event or future event based on a relationship with a party other than an insurance company by contractual agreement. The relationship will involve an agreement where one party agrees to assume the financial responsibilities of a second party for losses that incur as per the terms of the contract. A hold-harmless or indemnity agreement is an example of a non-insurance contract where one party (indemnitor) agrees to assume the financial consequences caused by the liability of another party (indemnitee).
- **Derivatives** are financial contracts that derive their value from another asset. Forward contracts, future contracts, options and swaps are all examples of derivatives. Derivatives can be used to transfer financial risk by offsetting the consequences of financial risk using a technique called hedging. Hedging does not mean that financial instruments will not experience a decrease in value but what it does do is to offset the losses from one investment and balance them against the gains from another investment with the intention of mitigating the adverse effects of financial risk.

Examples

- Fire is a hazard risk that has a low likelihood and a high severity on a risk map placing it in the top left corner of the risk map. Risks that lay in this quadrant are ideally situated to be insured. An organization that wants to minimize the financial impact or consequences resulting from a fire that could occur in the future could purchase guaranteed cost insurance. The purchase of guaranteed cost insurance will reduce the financial uncertainty associated with a potential fire loss by indemnifying the policyholder should the peril of fire occur.
- The management of a chain of retail furniture stores contracts a furniture manufacturer to provide chairs to be sold in their stores. The management of the retail furniture store requests that the manufacturer sign a hold-harmless agreement holding the retailer harmless as a part of the contract. If this agreement is signed, then the manufacturer of the chairs would assume the financial responsibility for any liability that results from their chairs. A customer purchasing a chair that causes an injury could bring legal action against the retailer and the manufacturer. If the manufacturer signs a hold harmless agreement with the retailer, then the financial consequences of the retailer's liability will be transferred to the manufacturer.
- A Canadian-based company engages in a forward contract with a financial institution to purchase U.S. dollars at a future date but at the current exchange rate. The Canadian company will be protected from financial losses if the U.S. dollar increases in value at a future date. The downside is that if the exchange rate decreases, the Canadian-based company will be obligated to purchase U.S. dollars at the exchange rate that was agreed upon.

Risk Retention

Risk Retention is a risk treatment technique where the organization retains the financial responsibilities of future losses. This risk treatment can be the most or least preferred risk financing technique selected by an organization, depending on many factors. Organizations often choose to practice risk retention because it is the most economical way to finance risk when compared to the cost of guaranteed cost insurance. The property and casualty insurance industry is cyclical in nature; during a **soft market**, there is an abundance of insurance markets available, and rates are low. In contrast, a **hard market** results in higher insurance rates and a reduced capacity or availability of insurance. Organizations may decide to purchase guaranteed cost insurance to transfer financial risk during a soft market cycle and to retain financial risk during a hard market cycle. It

should also be understood that the activities or claims experience of some organizations might fall outside of the appetites of insurance companies, resulting in risks that are uninsurable. In this case, risk retention is the only option.

Self-insurance is a practice that involves setting funds aside to cover the consequences of retained losses. It is a technique that is selected by an organization to reduce its cost of risk when the organization can predict its future losses with a degree of accuracy. Losses that are predicted to be high frequency and low severity are ideal risks to self-insure, as risk control techniques can be implemented to decrease their frequency. Although there are many advantages associated with self-insurance, such as improved cash flows, focus on loss control, cost savings, flexibility and control over claims, there are disadvantages, such as the uncertainty of large losses, lack of resources, and administration requirements. An organization that is self-insuring can actively retain the financial consequences of its predicted losses by ensuring that funds are available in advance. In contrast, some organizations practice in-active or informal risk retention and do not have funds set aside to cover the financial consequences of losses that could affect the organization.

A **hybrid risk financing plan** incorporates the elements of both risk transfer and risk retention as funds are available from both inside and outside of the organization. A deductible is a specified amount of money that an organization is required to pay towards a loss that an insurance company does not pay. Deductibles are used to lower insurance costs and to minimize nuisance claims involving small losses.

Example

If a total loss occurs on a property that is insured for $1 million dollars with a $50 thousand-dollar deductible, then the loss would be paid as follows:

- Amount paid by the insured is $50 thousand dollars
- Amount paid by the insurer is $950 thousand dollars

The organization retains $50 thousand dollars of the loss and transfers $950 thousand dollars of the loss to the insurance company.

A **captive insurance company** is a hybrid risk financing plan that is a subsidiary of a parent company that is not an insurance company. The primary reason that an organization will form a captive insurance company is to insure the parent companies' risk and the risk of its affiliates with the intention of reducing the cost

of risk. Captive insurance companies are alternatives to self-insurance; they are licenced insurance companies that must meet the requirements of the domicile in which they are located. A captive insurance company can be located anywhere in the world, but some domiciles are captive-friendly domiciles that offer favourable regulatory requirements, tax implications, stability, capital and solvency requirements. It should be noted that a captive is a legitimate insurance company that issues policies and collects premiums from its parent company. It could also take on insurance risks outside of its parent company.

A captive insurance plan will retain the first layer of losses where there is a high frequency and low severity by issuing a policy to the parent company and transfer losses with a higher severity to an insurance company or by purchasing reinsurance through the captive.

Reinsurance is a transaction that transfers the financial consequences of insurance risk from a primary insurance company (in this case, the captive) to another insurance company known as a reinsurer.

Examples

- An organization seeking to lower its cost of insurance plans to assume the financial consequences of its risks decides to self-insure by putting money into a fund to pay for high frequency/low severity losses that it predicts will occur in the future. The organization is practicing risk financing using retention.
- A hard insurance market has resulted in higher insurance rates for an organization. The organization decides to investigate the possibility of forming a captive insurance company or self-insuring to reduce the organization's cost of risk. The fact that captive insurance companies have elements of retention and transfer is more appealing to the organization than self-insurance, which only has the element of retention. After evaluating the domicile where the captive will be located, the organization selects the risks that the captive will be retaining and the risks that it will transfer through a reinsurance arrangement.

Risk Exploitation

Risk Exploitation is a risk treatment technique that involves actions or activities that are taken to ensure that the benefits from an opportunity are maximized by the organization. While there is a risk to an organization when it pursues an opportunity, there is also a risk to an organization when it does not pursue an opportunity.

The risk treatment of exploit can be applied to risks that have an upside and a downside, but it is more commonly used with events that have positive outcomes. Organizations that conduct activities to exploit risk are taking steps to eliminate the uncertainty associated with events to ensure that a positive result occurs in order to meet objectives. An organization can take steps to measure the probability and impact of risk events to achieve a positive outcome, whereas with uncertainty, future events are not known, and the organization would have doubts about what the outcome would be.

Example

If a retail operation has a fire that destroys its facility, then a competitor could offer that retailer's customers a discount to encourage them to visit their location. This is an example of risk exploitation as actions have been taken by offering a discount to ensure the expansion of the customer base by modifying the likelihood of a positive outcome.

Risk Control for Hazard Risks

The five accepted risk treatment techniques applicable to enterprise risk management that have been explained above are:

- Risk Avoidance
- Modifying the likelihood and/or impact of the risk
- Risk Transfer
- Risk Retention
- Risk Exploitation

These risk treatment techniques can be used to respond to risks across the four risk categories of Hazard Risk, Operational Risk, Financial Risk and Strategic Risk.

Hazard risks are pure risks that have a chance of loss; no loss but no gains can be realized; there are only negative outcomes. Insurance companies deal with the negative outcomes of pure or hazard risks resulting from accidental losses; speculative risks are not to be considered insurable. Hazard risks are defined by their capacity to cause harm to people, property or legal liability.

There are six risk control techniques exclusive to hazard risks which were the sole focus of traditional risk management practitioners. These techniques are very specific to hazard risks and were not intended for use with speculative risks, in other words, risks with positive or negative outcomes.

Avoidance

Avoidance is a risk control technique that terminates risk by stopping or never undertaking the activity or activities that have the potential to cause a risk to occur. It is identical in meaning to risk avoidance, which was described earlier as a risk treatment for the upside and downside of risk under enterprise risk management. It is not practical to terminate some activities to avoid the downside of risk, but when a risk is avoided, the probability of loss is zero unless the activity was previously undertaken by the organization prior to being terminated.

Loss Prevention

Loss prevention is a risk control technique that is similar in its intent to modify the likelihood of the risk, which was described as a risk treatment for risks included under enterprise risk management. Loss prevention measures are implemented prior to the occurrence of a negative event with the intention of reducing the likelihood, frequency or probability of the event. Loss prevention differs from avoidance because it does not terminate or eliminate the chance of loss. Risk control techniques associated with loss prevention do not affect the impact or severity of a risk because they are pre-loss measures intended to prevent the occurrence of an event before it starts.

Loss Reduction

Loss reduction is a risk control technique that is similar in its intent to modify the impact of the risk, which was described as a risk treatment for risks included under enterprise risk management. Loss reduction measures are implemented after the occurrence of a negative event with the intention of reducing the impact, severity or consequences of the event. Loss reduction measures can be identified as being either pre-loss measures, post-loss measures or both. Pre-loss measures, as stated earlier, are steps that are taken to reduce the frequency of a loss, but they can also be taken to reduce the severity of a loss. An example of a pre-loss measure for the peril of fire is to construct buildings with fire-resistant materials that do not contribute fuel to the fire. Post-loss measures focus on the negative event after it has occurred and are normally associated with emergency procedures or recovery from the event. An example of a post-loss measure for the peril of fire would be the operation of an automatic sprinkler system that responds to a fire that has started inside the building.

Separation

Separation is a risk control technique that spreads assets or activities over several locations to reduce the severity, impact or consequences of a negative event at one location, affecting only that location and not the entire organization. An example would be an organization shipping products from two distribution centres located in different geographical locations in Canada. If a fire causes a total loss at one location, then the company could still distribute products from the second location. The second location must have the capacity and resources to operate independently across a region formally served by two distribution centres to prevent an interruption in service.

Duplication

Duplication is a risk control technique that keeps alternate assets in reserve to reduce the severity, impact and consequences caused by the loss of an organization's primary assets. The duplicate assets are used to maintain continuity of operations in the event of a loss to the primary assets. Duplication is often not practical as it can be costly to an organization because the duplicate assets are sitting in reserve and are not used unless called upon. The main difference between separation and duplication is that all the assets associated with separation are in regular use, whereas the assets associated with duplication are not used and are held in reserve.

6.3 CHAPTER SUMMARY

Summary

In Chapter 6 the focus is on how organizations address identified risks through strategic actions and decisions. The chapter begins by defining risk response as the approaches an organization uses to manage risks, which involves a risk assessment process consisting of identification, analysis, and evaluation. Tools such as risk registers and maps help visualize risks based on their likelihood and impact, aiding in developing a risk profile that aligns with the organization's risk appetite—the level of risk an organization is willing to tolerate or pursue in achieving its objectives.

Risk treatment, often interchangeable with risk control, encompasses various techniques to manage risks. These include risk avoidance, modifying the likelihood or impact of risks, risk transfer, risk retention, and risk exploitation. Risk avoidance involves stopping activities that generate risk, while modifying likelihood or impact entails preventive measures or controls. Risk transfer shifts financial responsibilities to another party through insurance or contracts. Risk retention keeps financial responsibilities within the organization, often through self-insurance. Risk exploitation aims to maximize benefits from opportunities. Additionally, risk control techniques for hazard risks—pure risks leading only to negative outcomes—are detailed, including avoidance, loss prevention, loss reduction, separation, and duplication. These strategies ensure a comprehensive approach to managing both the upside and downside of risks across various categories.

OpenAI. (2024, July 29). *ChatGPT.* [Large language model]. https://chat.openai.com/chat

Prompt: *Please take the chapter content in this document attached and summarize the key concepts into no more than two paragraphs. Reviewed by authors.*

Key Terms

- **Avoidance** is a risk control technique that terminates risk by stopping or never undertaking the activity or activities that have the potential to cause a risk to occur.
- **Captive insurance company** is a hybrid risk financing plan that is a subsidiary of a parent company that is not an insurance company.
- **Derivatives** are financial contracts that derive their value from another asset.
- **Duplication** is a risk control technique that keeps alternate assets in reserve to reduce the severity, impact and consequences caused by the loss of an organization's primary assets.
- **Guaranteed cost insurance** is a primary risk transfer mechanism involving insurance contracts that provide coverage for insurable perils.
- **Hard market:** a hard market results in higher insurance rates and a reduced capacity or availability of insurance.
- **Hazard risks** are pure risks that have a chance of loss; no loss but no gains can be realized; there are only negative outcomes.
- **Hybrid risk financing plan** incorporates the elements of both risk transfer and risk retention as funds are available from both inside and outside of the organization.
- **Loss prevention** is a risk control technique that is similar in its intent to modify the likelihood of the risk, which was described as a risk treatment for risks included under enterprise risk management.
- **Loss reduction** is a risk control technique that is similar in its intent to modify the impact of the risk, which was described as a risk treatment for risks included under enterprise risk management.
- **Modifying the likelihood of a risk** is a risk treatment technique that involves measures to decrease or change the probability or frequency of the positive or negative effects of a risk through corrective actions or controls.
- **Non-insurance contracts** transfer the financial consequences of an event or future event based on a relationship with a party other than an insurance company by contractual agreement.
- **Reinsurance** is a transaction that transfers the financial consequences of insurance risk from a primary insurance company (in this case, the captive) to another insurance company known as a reinsurer.

- **Risk adverse** is when organizations are reluctant or unwilling to take on risks, indicating a low-risk tolerance.
- **Risk aggressive** is when organizations actively take on risks even in the absence of controls, indicating a high-risk tolerance.
- **Risk appetite** is the amount of risk that an organization is willing to retain, tolerate or seek in pursuit of its objectives.
- **Risk avoidance** is a risk treatment technique that terminates risk by stopping or never undertaking the activity or activities that have the potential to cause a risk to occur.
- **Risk Exploitation** is a risk treatment technique that involves actions or activities that are taken to ensure that the benefits from an opportunity are maximized by the organization.
- **Risk Response** is a broad term that is used to describe the approaches that an organization will use to manage its risks. It is a plan to manage risks derived from information that is received after conducting a risk assessment.
- **Risk Retention** is a risk treatment technique where the organization retains the financial responsibilities of future losses.
- **Risk transfer** is a risk treatment technique that is used to shift the financial responsibilities of future losses to another party.
- **Risk treatment** describes the specific actions and decisions that an organization will use to modify the upside and the downside of the risks that have been identified and analyzed by the organization.
- **Self-insurance** is a practice that involves setting funds aside to cover the consequences of retained losses. It is a technique that is selected by an organization to reduce its cost of risk when the organization can predict its future losses with a degree of accuracy.
- **Separation** is a risk control technique that spreads assets or activities over several locations to reduce the severity, impact or consequences of a negative event at one location, affecting only that location and not the entire organization.
- **Soft market:** during a soft market, there is an abundance of insurance markets available, and rates are low.

CHAPTER 7: RISK MONITORING

Chapter Overview

7.0 LEARNING OUTCOMES

Learning Objectives

At the end of this chapter, students will be able to:

- Identify and explain three key responsibilities of the board in risk management, including setting the risk appetite, overseeing risk policies, and fostering a risk-aware culture.
- Describe the primary functions of a Board Risk Committee and outline the processes for monitoring key and emerging risks within an organization.
- Evaluate the role of a Chief Risk Officer by listing at least five key responsibilities, such as leading risk management efforts and overseeing technology and cybersecurity risks.
- Assess the contribution of internal audit to risk management by explaining how it provides independent assurance on the effectiveness of risk processes and controls.
- Analyze the COSO Internal Control Framework by detailing its five components and explaining their relevance to risk management.
- Discuss the role of internal audit in risk monitoring by identifying at least three ways it supports risk management activities, such as providing independent assurance and evaluating control activities.
- Create an effective risk report by outlining the key components, including risk identification, assessment, and the use of visual elements like dashboards and heat maps.

7.1 ROLE OF THE BOARD IN RISK MANAGEMENT

> Potential profit often corresponds to the potential risk.... Stockholders' investment interests will be advanced if corporate directors and managers honestly assess risk and reward, cost and benefit – Hon. E. Norman Veasey (former Chief Justice of the Delaware Supreme Court) (Waller Lansden Dortch & Davis, 2005)

The board of directors plays a crucial role in risk management by providing oversight and strategic guidance. While not directly involved in day-to-day risk management activities, the board is responsible for ensuring that the organization has effective risk management systems and processes in place. The board's primary functions in risk management include setting the company's risk appetite, overseeing the development and implementation of risk management policies and procedures, monitoring significant risks facing the organization, and fostering a risk-aware culture throughout the company. By fulfilling these responsibilities, the board helps to safeguard the organization's assets, reputation, and long-term sustainability.

From the COSO ERM framework, some of the key responsibilities and functions of the board this context are described below:

Figure 7.1.1: "COSO ERM Framework" in *Enterprise Risk Management: Integrating with Strategy and Performance*, © 2017 Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used with permission. (See Acceptable Use of COSO Materials [PDF] for permission details).

Image Description

A double helix shape of different colours representing the various components: Governance & Culture with Information, Communication, & Reporting on one side and Strategy & Objective Setting, Performance, and Review & Revision on the other. Interspersed through the double helix shape are Mission, Vision, & Core Values, Strategy Development, Business objective Formulation, Implementation & Performance, and Enhanced Value

Oversight and Governance

Risk Oversight

The board's oversight role involves:

- Regularly reviewing the organization's risk profile and risk management strategies
- Challenging management's assumptions about risks
- Ensuring that risk management is integrated into strategic planning and decision-making processes
- Verifying that appropriate resources are allocated to risk management activities

Policy Development

In developing risk management policies, the board should:

- Establish clear guidelines for risk identification, assessment, and mitigation
- Define the organization's risk appetite and tolerance levels
- Ensure policies are adaptable to changing business environments
- Regularly review and update policies to reflect new risks and best practices

Risk Culture

To foster a risk-aware culture, the board can:

- Lead by example in prioritizing risk management
- Encourage open communication about risks at all levels of the organization
- Integrate risk considerations into performance evaluations and incentive structures
- Promote training and education programs on risk management

Monitoring and Reporting

Continuous Assessment

This involves:

- Implementing a systematic approach to identifying and assessing risks
- Regularly reviewing the effectiveness of risk mitigation strategies
- Ensuring that risk assessments are forward-looking and consider emerging risks
- Conducting periodic independent reviews of the risk management framework

Key Risk Indicators (KRIs)

The board should:

- Work with management to identify relevant KRIs for different risk categories
- Ensure KRIs are aligned with the organization's strategic objectives
- Set appropriate thresholds for KRIs that trigger escalation or action
- Regularly review the relevance and effectiveness of chosen KRIs

Risk Reporting

- Effective risk reporting to the board includes:
- Establishing a clear reporting structure and frequency
- Ensuring reports provide a comprehensive view of the organization's risk profile
- Including both quantitative metrics and qualitative assessments
- Highlighting significant changes in risk exposure and emerging risks

Committee Involvement

Audit and Risk Committees

These committees should:

- Conduct deep dives into specific risk areas
- Review the adequacy of internal controls and risk management processes
- Oversee the internal audit function and its risk-based audit plans
- Engage with external auditors to understand their risk assessments

Coordination Among Committees

To ensure comprehensive risk coverage:

- Establish clear charters defining each committee's risk responsibilities
- Hold joint committee meetings to discuss overlapping risk areas
- Ensure regular information sharing between committees

- Provide periodic updates to the full board on committee-level risk discussions

Strategic Risk Management

Strategic Risks

The board's involvement includes:

- Dedicating time in board meetings to discuss strategic risks
- Challenging management's strategic assumptions and risk assessments
- Considering scenario planning and stress testing for major strategic decisions
- Ensuring alignment between risk management and strategic planning processes

Cyber Risks

Given the critical nature of cyber risks, the board should:

- Ensure regular briefings on the organization's cybersecurity posture
- Oversee investments in cybersecurity infrastructure and talent
- Review incident response and business continuity plans
- Stay informed about evolving cyber threats and regulatory requirements

Accountability and Transparency

Accountability

To ensure accountability, the board should:

- Clearly define risk management responsibilities for executives and management
- Include risk management objectives in performance evaluations
- Ensure there are consequences for non-compliance with risk policies
- Regularly assess the effectiveness of the risk management function

Transparency

To promote transparency, the board can:

- Oversee the development of comprehensive risk disclosures in financial reports
- Ensure clear communication of risk management practices to stakeholders
- Encourage management to be forthcoming about significant risks and mitigation efforts
- Support engagement with regulators, investors, and other stakeholders on risk-related matters

The board's role in risk monitoring and reporting is to provide oversight, develop policies, foster a risk-aware culture, ensure continuous risk assessment, and maintain accountability and transparency. By fulfilling these responsibilities, the board helps safeguard the organization against potential risks and supports its long-term success. The board can significantly enhance its risk monitoring and reporting effectiveness, ultimately contributing to the organization's resilience and long-term success. (Krishnamoorthy, n.d.; Barlow, 2016; Waller Lansden Dortch & Davis, 2005; Institute of Risk Management, n.d.)

Figure 7.1.2: "Risk Management Organization" by Sanaz Habibi, CC BY-NC-SA 4.0

Image Description

The image depicts an organizational chart for risk management within a company. The hierarchy and connections are as follows:

1. **Board** (pink circle at the top): Connected to all committees and executive officers.
2. **Committees and Executive Officers**:
    1. **Risk Committee** (green circle): Connected to the Chief Risk Officer (CRO).
    2. **Chief Executive Officer (CEO)** (blue circle): Connected to the Chief Risk Officer (CRO) and Chief Financial Officer (CFO).
    3. **Audit Committee** (purple circle): Connected to the Chief Risk Officer (CRO).
    4. **Finance Committee** (yellow circle): Connected to the Chief Financial Officer (CFO).
3. **Chief Officers**:
    1. **Chief Risk Officer** (CRO) (purple circle): Connected to Risk Management and Internal Audit.
    2. **Chief Financial Officer** (CFO) (green circle): Connected to Financial.
4. **Functional Units**:

1. **Risk Management (pink circle)**: Connected to the Chief Risk Officer (CRO).
2. **Internal Audit (purple circle):** Connected to the Chief Risk Officer (CRO).
3. **Financial (yellow circle)**: Connected to the Chief Financial Officer (CFO).

The chart uses colour-coded circles to represent different roles and their connections, indicating lines of reporting and oversight within the organization.

7.2 BOARD RISK COMMITTEE

The **Board Risk Committee** is a specialized group within the board of directors focused on overseeing an organization's risk management practices. Typically comprising 3-5 members with risk management expertise, this committee enhances the board's ability to manage risk effectively.

The committee's primary responsibilities include overseeing the enterprise risk management framework, approving risk policies, monitoring key and emerging risks, and ensuring adequate risk reporting to the full board. It meets regularly, often quarterly, with additional sessions as needed, including private meetings with key executives like the Chief Risk Officer.

Working closely with management while maintaining independence, the committee provides crucial oversight and challenges risk assessments. Its scope covers a wide range of risks, from strategic and financial to operational and emerging threats like cybersecurity.

The Board Risk Committee adds significant value by allowing in-depth risk discussions and demonstrating strong risk governance to stakeholders. However, it doesn't replace the full board's ultimate responsibility for risk oversight and may not be necessary for smaller organizations.

Operating under a clear charter, the committee regularly reviews its effectiveness and engages in ongoing risk management education. These efforts play a vital role in strengthening the organization's risk governance and supporting the board's fiduciary duties, ultimately contributing to the organization's resilience and long-term success.

7.3 ROLE OF CHIEF RISK OFFICER

The **Chief Risk Officer (CRO)** is a senior executive responsible for overseeing an organization's enterprise-wide risk management. Key aspects of the CRO's role include:

- Leading risk management efforts across the organization
- Integrating risk considerations into strategic planning
- Developing and implementing risk policies and procedures
- Ensuring compliance with relevant laws and regulations
- Fostering a risk-aware culture throughout the organization
- Providing regular risk assessments to the board and executive management
- Managing crises and mitigating their impact
- Overseeing technology and cybersecurity risks
- Collaborating with other executives for comprehensive risk management
- Staying informed about emerging risks and best practices (Horvath, 2024; Strawser, 2023)

The CRO's role has become increasingly important due to complex business environments, regulatory requirements, and the need for proactive risk management. Their work is crucial in helping organizations navigate uncertainties and protect their assets, reputation, and long-term viability.

7.4 ROLE OF INTERNAL AUDIT

Internal Audit plays a crucial role in an organization's risk management framework by providing independent and objective assurance on the effectiveness of risk management processes. It evaluates the design and implementation of the risk management framework, identifies emerging risks and control issues, and offers recommendations for improvement.

Internal Audits help foster a risk-aware culture by promoting risk management principles and educating staff. It coordinates with other risk and control functions to ensure comprehensive risk coverage and avoids duplication of efforts.

Regular reporting to the Audit Committee and board keeps key stakeholders informed about significant risk exposures and control issues. Additionally, internal audits provide valuable advisory services to management on risk-related matters while maintaining objectivity.

Internal Audit enhances risk management by offering independent assurance, identifying risks, recommending improvements, and fostering a risk-aware culture, ultimately contributing to the organization's resilience and success.

Adapted from "The Role of Internal Audit in Risk Management" by Arturo Navarro under Fair Dealing for Educational Purposes (Canada).

7.5 INTERNAL CONTROLS FROM A RISK MANAGEMENT PERSPECTIVE

Internal controls are processes and measures an organization implements to provide reasonable assurance regarding achieving operations, reporting, and compliance objectives. From a Risk management perspective, these are processes and measures implemented by an organization to:

- Provide reasonable assurance that the organization's objectives will be achieved
- Mitigate risks to acceptable levels
- Ensure effectiveness and efficiency of operations
- Promote reliability of financial reporting
- Ensure compliance with applicable laws and regulations

COSO's Internal Control Framework

COSO's Internal Control-Integrated Framework identifies five interrelated components of internal control:

Figure 7.5.1: "COSO's five components of Internal Control" by Sanaz Habibi, CC BY-NC-SA 4.0

Image Description

The image presents COSO's Five Components of Internal Controls in a circular arrangement, visually conveying their interconnectedness within the internal control framework. Each component is represented by a coloured segment with an icon and label: Control Environment (pink segment with a lightbulb icon), Risk Assessment (yellow segment with a clock icon), Information and Communication (green segment with an information icon), Control Activities (blue segment with a gear icon), and Monitoring (purple segment with a target icon). At the center of the circle, a grey circle contains the text "COSO's Five Components of Internal Controls," emphasizing the core elements that comprise the internal control system.

Control Environment

- Sets the tone of the organization, influencing the control consciousness of its people

- Includes integrity, ethical values, management's philosophy and operating style
- Encompasses organizational structure, assignment of authority and responsibility
- Involves human resource policies and practices
- Provides the foundation for all other components of internal control

Risk Assessment

- Involves identifying and analyzing relevant risks to achieving objectives
- Forms a basis for determining how risks should be managed
- Includes setting objectives at different levels (entity-wide and activity-level)
- Encompasses internal and external factors that could impact objectives
- Considers the potential for fraud in assessing risks
- Identifies and assesses changes that could significantly impact the internal control system

Control Activities

- Policies and procedures that help ensure management directives are carried out
- Occur throughout the organization, at all levels and in all functions
- Include a range of activities such as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties
- Can be preventive or detective in nature
- Include general controls and application controls over technology

Information and Communication

- Pertinent information must be identified, captured, and communicated in a form and timeframe that enables people to carry out their responsibilities.
- Information systems produce reports containing operational, financial, and compliance-related information.
- Deals with internal and external communications
- Provides the information needed to carry out day-to-day controls
- Enables personnel to understand their own role in the internal control system, as well as how individual activities relate to the work of others

Monitoring

- Assesses the quality of internal control performance over time

- Includes ongoing monitoring activities built into normal, recurring operating activities
- Involves separate evaluations, the scope and frequency of which depend on risk assessment and effectiveness of ongoing monitoring procedures
- Communicates deficiencies to those responsible for taking corrective action and to management and the board as appropriate
- Considers feedback from both internal and external sources, including audits and regulatory reviews

From a risk management monitoring perspective, these components work together as an integrated system. They provide a framework for organizations to develop and maintain effective internal controls that address significant risks. The monitoring component, in particular, is crucial in ensuring that the internal control system remains effective over time and adapts to changes in the organization's risk profile and operating environment (Leland, 2023; COSO, 2013).

7.6 ROLE OF INTERNAL AUDIT IN RISK MONITORING

Internal audit is an activity that evaluates a company's internal controls, including corporate governance and accounting processes, as well as risk monitoring. These audits ensure compliance with laws and regulations, maintain accurate financial reporting, and identify areas for improvement (Tuovila, 2024).

Internal Audit system supports Risk Monitoring in the following areas (The Institute of Internal Auditors, n.d.):

- *Independent Assurance:* Internal Audit provides independent and objective assurance on the effectiveness of risk management processes and internal control systems. This helps organizations assess whether their risk-monitoring activities are adequate and effective.
- *Risk Assessment:* Internal Audit conducts risk assessments to identify and analyze risks that could affect the achievement of organizational objectives. This supports ongoing risk monitoring efforts by highlighting areas of concern.
- *Evaluation of Control Activities:* Internal Audit reviews and evaluates control activities implemented to mitigate risks, ensuring they function as intended and effectively address identified risks.
- *Monitoring of Risk Management Processes:* Internal Audit assesses the quality and effectiveness of risk management processes over time, helping to ensure that risk monitoring activities remain relevant and effective.
- *Reporting on Risk Issues:* Internal Audit provides periodic reports to the Audit Committee and senior management on significant risk exposures and control issues, supporting ongoing risk monitoring efforts.
- *Recommendations for Improvement:* Internal Audit offers recommendations to improve risk management practices and internal controls, enhancing the organization's ability to monitor and manage risks effectively.
- *Advisory Role:* Internal Audit can act as a consultant or advisor on risk-related matters, providing insights and expertise to support risk monitoring activities.

- *Promoting Risk Awareness:* Internal Audit helps foster a risk-aware culture throughout the organization, which supports more effective risk monitoring at all levels.
- *Compliance Assurance:* Internal Audit assesses compliance with laws, regulations, and internal policies, an important aspect of risk monitoring.
- *Continuous Monitoring Support:* Internal Audit can help implement and assess the effectiveness of continuous monitoring processes for key risks and controls.

By fulfilling these roles, Internal Audit supports Risk Monitoring by providing an independent perspective, enhancing the effectiveness of risk management processes, and offering valuable insights to improve the organization's ability to identify, assess, and manage risks continuously.

7.7 RISK REPORTING

Risk reporting is a critical process in organizational risk management, serving as the primary means of communicating vital risk-related information to key stakeholders, particularly senior management and the board of directors. This process involves systematically collecting, analyzing, and presenting data about an organization's risk landscape, enabling informed decision-making and effective risk oversight.

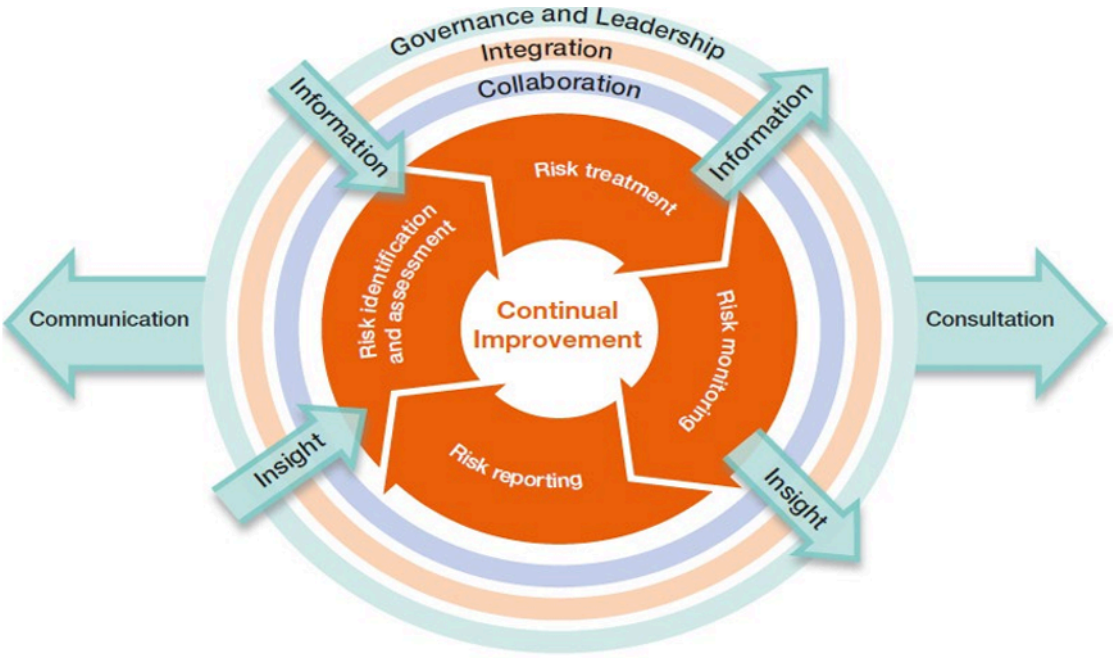

Figure 7.7.1: Risk Reporting as a key component of Risk Management. Orange Book: Management of risk – Principles and Concepts, UK Government, Open Government Licence.

Image Description

A series of circles and arrows with Continual Improvement in the centre. In the first circle, Risk treatment, Risk monitoring, Risk reporting, and Risk identification and assessment. There are two arrows pointing in called lnsight and Information, and two pointing out labelled Insight and Information. The next three circles (inside to outside) are Collaboration, Integration, Governance and Leadership. An arrow from the outside circle pointing left is Communication and an arrow pointing right is labelled Consultation.

- *Contents:* Risk reporting aims to provide a clear, comprehensive picture of the organization's significant risks. This includes identifying key risks, assessing their potential impact and likelihood, and detailing the status of risk mitigation efforts. Effective risk reports highlight emerging risks and trends, ensuring that leadership remains aware of evolving threats and opportunities.
- *Format:* Risk reporting may combine visual elements like risk dashboards or heat maps with more detailed narrative reports. This approach allows for quick comprehension of the overall risk profile while providing depth where needed. The reporting frequency typically follows a regular schedule, often quarterly, supplemented by ad-hoc reports for significant risk events or changes in the risk landscape.
- *Internal Audit Role:* It plays a crucial role in this process, offering independent assurance on the effectiveness of risk management processes and providing valuable insights on risk trends. Their involvement enhances the credibility and objectivity of risk reporting, supporting the board and senior management in their oversight responsibilities.
- *Best Practices:* Best practices in risk reporting emphasize clarity, conciseness, and relevance. Reports should focus on the most significant risks, provide context and analysis beyond raw data, and include recommendations for risk mitigation where appropriate. This approach ensures that risk information is not only comprehensive but also actionable.

Effective risk reporting is fundamental to fostering a risk-aware culture throughout the organization. Providing a clear view of the risk landscape enables leadership to make informed decisions, allocate resources effectively, and navigate the complex, ever-changing business environment with greater confidence and resilience (Financial Reporting Council, 2014; PWC, 2011; UK Government, 2023).

7.8 CHAPTER SUMMARY

Summary

Chapter 7 emphasizes the critical role of risk monitoring within an organization, focusing on the board of directors' responsibilities and the various elements that ensure effective risk management. The board plays a pivotal role by setting the risk appetite, overseeing the implementation of risk policies, and fostering a risk-aware culture. This includes regularly reviewing risk profiles, challenging management's risk assumptions, and ensuring risk management is integrated into strategic planning. The development of clear guidelines for risk identification and mitigation, alongside fostering open communication and training programs, are highlighted as essential for cultivating a robust risk culture.

The chapter further discusses the importance of continuous risk assessment and the use of Key Risk Indicators (KRIs) to monitor significant risks. Effective risk reporting is emphasized, requiring comprehensive and clear communication of the organization's risk profile to the board and stakeholders. The roles of specialized committees, such as the Board Risk Committee, Chief Risk Officer (CRO), and Internal Audit, are detailed, highlighting their contributions to risk monitoring, policy development, and assurance of compliance with risk management processes. The COSO Internal Control Framework's five components—control environment, risk assessment, control activities, information and communication, and monitoring—are explained as the foundation for effective internal controls, ensuring ongoing effectiveness and adaptation to changing risks.

OpenAI. (2024, June 28). *ChatGPT.* [Large language model]. https://chat.openai.com/chat

Prompt: *Please take the chapter content in this document attached and summarize the key concepts into no more than two paragraphs. Reviewed by authors.*

Key Terms

- **Board Risk Committee** is a specialized group within the board of directors focused on overseeing an organization's risk management practices.
- **Chief Risk Officer (CRO)** is a senior executive responsible for overseeing an organization's enterprise-wide risk management.
- **Internal audit** is an activity that evaluates a company's internal controls, including corporate governance and accounting processes, as well as risk monitoring.
- **Internal controls** are processes and measures an organization implements to provide reasonable assurance regarding achieving operations, reporting, and compliance objectives.
- **Risk reporting** is a critical process in organizational risk management, serving as the primary means of communicating vital risk-related information to key stakeholders, particularly senior management and the board of directors.

CHAPTER 8: RISK MANAGEMENT IN SUPPLY CHAIN AND OPERATIONS MANAGEMENT

Chapter Overview

8.0 LEARNING OUTCOMES

Learning Objectives

At the end of this chapter, students will be able to:

- Evaluate the processes involved in supply chain management and supply chain risk management, and explain how effective risk management can enhance operational efficiency and resilience.
- Identify and categorize various risks that affect supply chain operations, including demand variations, natural disasters, global events, supplier risks, and cybersecurity threats.
- Develop and implement a systematic framework for identifying, analyzing, treating, and monitoring supply chain risks.
- Assess and apply various supply chain risk management strategies, such as multisourcing, nearshoring, stress testing, building buffers, and improving cybersecurity.

8.1 SUPPLY CHAIN MANAGEMENT AND SUPPLY CHAIN RISK MANAGEMENT

Supply chain management includes all activities that turn raw materials into finished goods and put them into customers' hands. This can include sourcing, design, production, warehousing, shipping, and distribution. SCM aims to improve efficiency, quality, productivity, and customer satisfaction. (SAP, n.d.; Inbound Logistics, 2023)

Successful global supply chains listen closely. They track market trends and gather customer feedback to understand what products people want, when, and how they want them delivered. From sourcing materials to research and development, manufacturing, and final delivery, smart companies use this customer data to streamline their entire supply chain. It's all about making things faster, cheaper, and better.

Imagine a supply chain as a series of links. Each link, or partner, needs to work together seamlessly. This means having a well-coordinated system where information flows freely.

Video: "What is Supply Chain Management (SCM) and Why is it Important?" by Eye on Tech [2:00] is licensed under the Standard YouTube License. *Transcript and closed captions available on YouTube.*

COVID-19 was a stark wake-up call, highlighting the inherent vulnerabilities within some of the most critical global supply chains. Businesses across the globe swiftly recognized the pressing need for modernization. The focus shifted towards implementing agile and resilient supply chain management processes, possessing the flexibility to adapt to unforeseen circumstances without succumbing to disruptions.

Leading companies are currently engaged in a rigorous self-evaluation process. They are scrutinizing their SCM operations and the underlying technological infrastructure, constantly seeking avenues for improvement. This proactive approach centers on a core question: how can we optimize efficiency, profitability, and, most importantly, future-proof our businesses in the ever-evolving global marketplace?

Supply Chain Risk Management

To mitigate these risks, organizations implement robust Supply Chain Risk Management (SCRM) strategies. SCRM serves as a proactive approach to building resilience and ensuring business continuity in the face of uncertainty.

Supply chain risk management (SCRM) is the process of finding and addressing potential vulnerabilities in a company's supply chain. SCRM aims to minimize the impact of these risks on a company's operations, reputation and financial performance (McGrath & Jonker, 2023).

By adopting SCRM strategies, companies can:

1. Anticipate and minimize potential disruptions
2. Optimize cost structures
3. Enhance product and service quality
4. Improve customer satisfaction levels

Furthermore, effective SCRM facilitates regulatory compliance, safeguards brand equity, and promotes sustainable business practices.

8.2 RISKS THAT AFFECT SUPPLY CHAIN OPERATIONS

Supply chain operations are inherently complex and susceptible to various risks that can disrupt the flow of goods and services. Understanding these risks is crucial for developing strategies to mitigate them and ensure business continuity. The primary risks affecting supply chain operations can be categorized into several key areas; some are internal to organizations, and some are external.

Variations in Demand

In today's dynamic market environment, consumer demand is changing at an unprecedented pace, driven by evolving needs, preferences, and an ever-expanding array of options. This volatility in demand presents significant challenges for supply chain management as accurately predicting consumer behaviour becomes increasingly complex. For postgraduate students studying risk management, understanding the implications of demand fluctuations and developing strategies to address them is essential.

The impact of demand fluctuations: Accurate demand forecasting is critical for maintaining profitability and operational efficiency. Misjudging demand can lead to either excess inventory, which ties up capital and increases storage costs, or stockouts, which result in lost sales and diminished customer satisfaction. Both scenarios can have a detrimental impact on a company's bottom line and market reputation (McGrath & Jonker, 2024).

Natural Disasters

Natural disasters have increasingly become a significant threat to global supply chains, causing widespread disruptions and economic losses. Events such as earthquakes, hurricanes, floods, and wildfires can severely impact the flow of goods and services, leading to delays, increased costs, and shortages. The frequency and intensity of these disasters have been rising, partly driven by climate change, which exacerbates extreme weather conditions.

For instance, the Texas freeze in February 2021 caused the worst involuntary energy blackout in U.S. history, leading to the closure of major semiconductor plants and exacerbating a global semiconductor shortage. Similarly, heavy rainfall and snowmelt in Europe disrupted shipping on the Rhine River, a critical commercial

waterway, affecting both inbound raw materials and outbound product deliveries. In China, severe flooding in July 2021 forced the closure of a Nissan plant, highlighting the vulnerability of manufacturing hubs to natural disasters (Leslie, 2022).

The economic impact of these disruptions is substantial. The cost of addressing damage caused by natural disasters has risen from approximately $50 billion per year in the 1980s to around $200 billion per year in the last decade (Al Kazimi & Mackenzie, 2016). This trend underscores the need for robust risk management and contingency planning in supply chain operations. Effective risk management processes involve creating contingency plans to mitigate the effects of these events.

Recent data shows a concerning upward trend in the frequency and severity of natural disasters. The number of billion-dollar weather and climate disasters in the United States has increased dramatically. In 2023, there were 28 such events, surpassing the previous record of 22 in 2020. These disasters resulted in a total cost of at least $92.9 billion (USAFacts Team, 2024).

These statistics underscore the growing importance of robust risk management and contingency planning in supply chain operations. As the frequency and intensity of natural disasters continue to rise, businesses must adapt their strategies to ensure resilience in the face of these increasing global events.

Global Events

Global events, particularly political and economic developments, have become increasingly significant factors affecting supply chains and global trade. These events can range from geopolitical instability and wars to trade disputes, strikes, and fluctuations in currency values and fuel prices. The impact of such events on global markets and supply chains necessitates robust risk management processes and contingency planning.

Geopolitical tensions and conflicts have emerged as key determinants of global economic performance. The ongoing war in Ukraine and the conflict between Israel and Hamas in the Middle East, compounded by Houthi missile attacks in the Red Sea, have significantly disrupted trade flows and caused supply chain problems even in third-party countries. These events have led to higher inflation, lower growth, and significant welfare losses globally (Kaya, 2024).

Trade disputes and protectionist policies have also become more prevalent. For instance, the tariff war between the United States and China in 2018 led to a series of retaliatory measures, affecting global trade patterns and supply chains. Such disputes can lead to increased restrictions, disrupt trade flows, and cause supply chain problems that extend beyond the directly involved countries (S&P Global, n.d.).

Currency fluctuations pose another significant risk to global trade. The value of currencies can be affected by various factors, including political events and economic policies. For example, the 2022 French presidential

elections correlated with a substantial drop in the Euro's value, demonstrating how political events can influence currency dynamics.

Supplier Risk in Supply Chains

Supplier risk is a critical concern in the complex landscape of global supply chains. Healthy supply chains depend on robust supplier partnerships, but weaknesses in these relationships can introduce significant instability and vulnerability.

Key forms of supplier risk include:

1. *Financial Instability:* Suppliers facing financial difficulties may struggle to maintain production levels or fulfill orders, potentially leading to sudden supply disruptions.
2. *Capacity Constraints:* Limitations in a supplier's ability to scale production can result in delays and unfulfilled orders, impacting the buying company's operations.
3. *Quality Issues:* Inconsistent or subpar quality from suppliers can lead to product recalls, brand damage, and increased costs.
4. *Geopolitical Factors:* Suppliers in politically unstable regions may face disruptions due to conflicts or trade restrictions, interrupting supply flows.
5. *Natural Disasters:* Suppliers in disaster-prone areas risk prolonged production stoppages and severe supply chain disruptions.
6. *Compliance and Ethical Concerns:* Non-compliance with regulations or ethical standards by suppliers can expose the buying company to legal risks and reputational damage.
7. *Technological Obsolescence:* Suppliers lagging in technological advancements may fail to meet changing product specifications or quality standards.
8. *Single-Source Dependency:* Relying on a single supplier for critical components creates significant vulnerability, with any issues potentially causing immediate and severe impacts.

The consequences of these risks include production delays, increased costs, lost revenue, and damage to brand reputation. The interconnected nature of modern supply chains means that problems with even a single supplier can have cascading effects throughout the entire network. Understanding and addressing supplier risk is crucial for ensuring the resilience and sustainability of supply chains in an uncertain global environment (Lobdell, 2023; Vicente, 2023; Marotta, n.d.).

Cybersecurity Threats in Supply Chains

Modern supply chains heavily rely on digital systems and communication technologies for managing orders, inventory, and distribution. This digital integration, while efficient, exposes supply chains to significant cybersecurity risks.

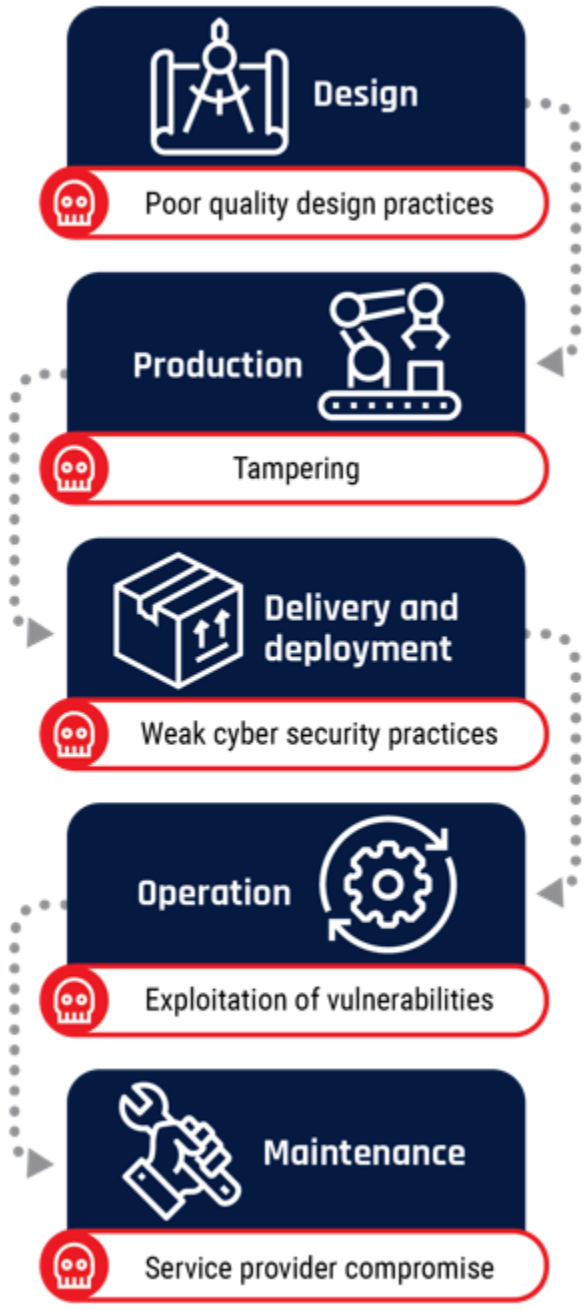

Figure 8.2.1: "Supply Chain vulnerabilities" by Canadian Centre for Cyber Security used under the Crown Copyright – NonCommercial Reproduction Licence (Canada). The Government of Canada is not affiliated with nor endorses the reproduction of its official documents here.

Image Description

The five areas are:

1. Design – poor quality design choices
2. Production – tampering
3. Delivery and Deployment – weak cyber security practices
4. Operation – exploitation of vulnerabilities
5. Maintenance – service provider compromise

Key cybersecurity threats include:

1. Ransomware and Malware Attacks can halt production and delay distribution, causing operational disruptions and financial losses.
2. Data Breaches: Unauthorized access to sensitive supply chain data can expose proprietary information or customer data, leading to reputational damage and legal consequences.
3. Disruption of Logistics: Cyberattacks can target transportation and logistics networks, causing delays in the distribution of goods.
4. Critical Infrastructure Damage: Attacks on key infrastructure components can lead to widespread supply chain disruptions.
5. Intellectual Property Theft: Cybercriminals may steal valuable IP, causing competitive disadvantages.
6. Counterfeit Products: Cyberattacks can facilitate the creation and distribution of counterfeit goods, undermining brand integrity.
7. Financial Fraud: Supply chains are vulnerable to cyber-enabled financial fraud, resulting in monetary losses.

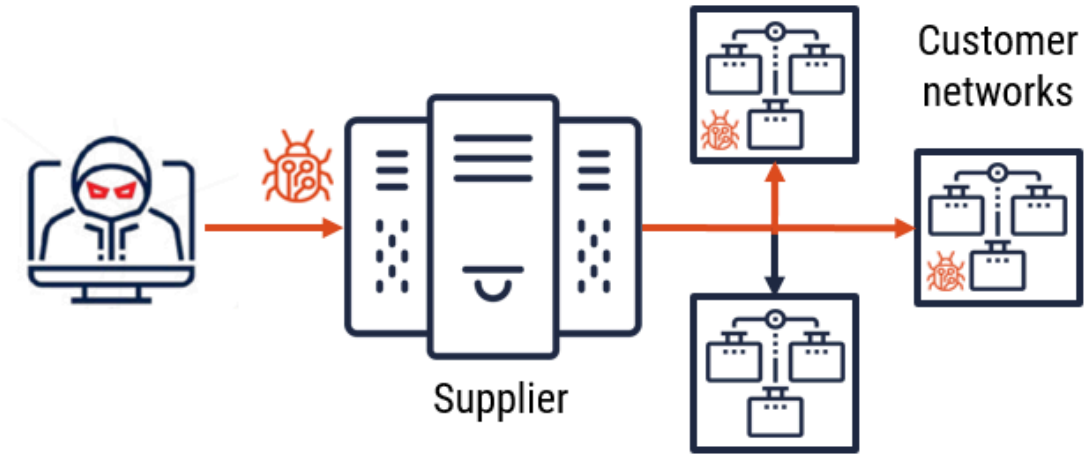

Figure 8.2.2: "Threat Movement through the supply chain" by Canadian Centre for Cyber Security used under the Crown Copyright – NonCommercial Reproduction Licence (Canada). The Government of Canada is not affiliated with nor endorses the reproduction of its official documents here.

The interconnected nature of modern supply chains means that a cyberattack on one part can have cascading effects throughout the entire network. As organizations strengthen their own cybersecurity, vulnerabilities within the supply chain become critical weak points. Understanding and addressing these cybersecurity risks is crucial for maintaining the resilience and integrity of supply chains in the digital age (Canadian Centre for Cyber Security, 2023; Kost, 2023).

Ethical and Social Responsibilities

Supply chain visibility is crucial for identifying unethical practices related to human rights, labour violations, and environmental impact. Suppliers deviating from international standards or a company's values can have significant consequences for all parties involved.

Key ethical concerns include:

1. *Human Rights Violations:* Issues like child labour and unsafe working conditions.

2. *Labour Violations:* Unfair practices such as underpayment and excessive working hours.
3. *Environmental Impact:* Harmful practices like improper waste disposal and excessive emissions.

These unethical practices can lead to:

- Reputational damage
- Legal consequences
- Financial losses

Companies must prioritize ethical considerations to mitigate risks and uphold their social responsibilities, maintaining the integrity of their supply chains and protecting their reputation in an increasingly conscious marketplace (Gordon, 2023; Sedex, 2024).

Outsourcing of Operations

Outsourcing operations is a strategic approach in supply chain management that allows companies to leverage external expertise, reduce costs, and focus on core competencies. However, this strategy also introduces significant risks that must be carefully managed to ensure supply chain resilience and reliability.

Key Risks Associated with Outsourcing

- *Supplier Reliability:* Outsourcing depends on the reliability of external suppliers. Any weaknesses in a supplier's financial stability, capacity, or quality control can lead to disruptions. For example, if a key supplier faces financial difficulties, it may fail to deliver critical components on time, halting production lines.
- *Geopolitical and Economic Instability:* Suppliers in politically or economically unstable regions pose risks. Changes in trade policies, tariffs, or political unrest can disrupt supply chains. For instance, trade tensions between the U.S. and China have increased tariffs and uncertainties for companies relying on Chinese suppliers.
- *Quality Control Issues:* Maintaining consistent quality standards can be challenging when

operations are outsourced. Variations in quality can lead to product recalls, increased costs, and damage to brand reputation. For example, a toy manufacturer outsourcing production may face recalls if the supplier uses substandard materials.

- *Intellectual Property Risks:* Outsourcing can expose companies to theft of intellectual property (IP). Suppliers may misuse proprietary information, leading to competitive disadvantages. For instance, a tech company outsourcing software development may risk its code being copied or leaked.
- *Compliance and Ethical Concerns:* Ensuring outsourced operations comply with regulatory standards and ethical practices is crucial. Violations can lead to legal penalties and reputational damage. For example, a fashion brand outsourcing production to a factory with poor labour practices may face backlash and legal action.
- *Communication and Coordination Challenges:* Effective communication and coordination with outsourced partners are essential. Miscommunication can lead to delays, errors, and inefficiencies. For instance, a delay in communication about a design change can result in the production of incorrect products.

Outsourcing operations can offer significant benefits but also introduces various risks that must be managed proactively. Companies must conduct thorough risk assessments, establish robust monitoring mechanisms, and maintain strong relationships with suppliers to mitigate these risks (Schnellbächer et al., 2023; Mbiam, 2023).

8.3 MANAGEMENT OF SUPPLY CHAIN RISKS

Effective Supply Chain Risk Management hinges on a systematic framework that proactively identifies, analyzes, treats, and continuously monitors potential disruptions within the supply chain.

1. *Identification:* Companies must proactively identify potential vulnerabilities impacting their supply chain's integrity. This process involves conducting comprehensive risk assessments that consider both internal and external factors, such as supplier locations, transportation routes, political stability, and weather patterns.
2. *Analysis:* After identifying potential risks, companies need to evaluate their likelihood and potential impact on the supply chain. This analysis can be conducted using various quantitative and qualitative methodologies, including risk scoring, scenario analysis, and expert judgment. These tools help compare historical data with current metrics and risk factors to forecast potential outcomes.
3. *Treatment:* Based on the risk analysis, companies develop strategies to address identified vulnerabilities, prioritizing the most significant issues. Risk mitigation strategies may include diversifying suppliers, improving inventory management, enhancing communication channels, investing in technology, and developing robust contingency plans.
4. *Monitoring:* Supply chain risk management is an ongoing process that requires continuous vigilance. Companies must regularly monitor supply chain operations and review risk management policies and procedures. This involves tracking key performance indicators, conducting audits, fostering strong supplier relationships, and engaging stakeholders. The ultimate goal is to minimize risk exposure and ensure informed decision-making throughout the supply chain.

By implementing this framework, companies can enhance their supply chain resilience and better navigate potential disruptions in an increasingly complex global marketplace (McGrath & Jonker, 2024).

8.4 SUPPLY CHAIN RISK MANAGEMENT STRATEGIES

There are several strategies to address or prepare for risks associated with supply chain management; however, while following the abovementioned process, organizations can formulate the right or appropriate strategy.

Video: "How Companies Are Overhauling Supply Chains to Ease Bottlenecks | WSJ" by The Wall Street Journal [5:15] is licensed under the Standard YouTube License. *Transcript and closed captions available on YouTube.*

Following are some of the strategies:

Multisourcing

Consider not relying on a single supplier. Multisourcing offers a robust shield against disruptions. Categorize suppliers not just by cost but also by their potential impact on operations in the event of an issue. This allows for a multifaceted approach to risk mitigation. Explore establishing relationships with additional suppliers in different geographic locations, or consider partnering with suppliers with diversified production facilities.

Nearshoring

Nearshoring involves strategically locating suppliers and distributors closer to your core operations or final product destinations. This approach can significantly reduce cycle times for both product development and delivery. While regional suppliers may come at a slight cost premium, the benefit lies in reduced transportation risks associated with longer distances.

Stress Testing

Mapping the supply chain network is merely the first step. True resilience requires a proactive approach. Regular and comprehensive **stress testing** is invaluable for identifying vulnerabilities, some of which may be deeply embedded within the supply chain. By simulating various disruption scenarios, companies can proactively develop contingency plans and identify areas for improvement.

Building Buffers

While maintaining buffer inventory and capacity represents an added expense, it can be a strategic investment. New product launches or market expansions present ideal opportunities to create buffer capacity. Furthermore, stockpiling critical products during high-risk periods (e.g., hurricane season) can significantly mitigate risk for businesses operating in regions prone to climate-related disruptions (Marotta, 2024).

Improvements In Cyber Security

While the Internet of Things (IoT) and other technologies optimize operations, they also introduce new cybersecurity vulnerabilities – malware, ransomware, phishing attacks, and hacking. Environmental disruptions can further exacerbate these risks. Some of the strategies are the following:

- *Standardize Security:* Mandate baseline cybersecurity compliance across all supply chain partners.
- *Control Access:* Define user roles and permissions to restrict system access.
- *Vet Your Vendors*: Conduct thorough cybersecurity risk assessments on potential vendors.
- *Data Governance:* Implement clear data ownership and usage protocols.
- *Workforce training:* Train employees to identify and report suspicious cyber activity.
- *Visibility:* Real-time monitoring and anomaly detection across the supply chain.
- *Unified Recovery:* Collaborate with partners to develop a unified disaster recovery plan.
- *Backup and Secure:* Establish robust data backups and maintain updated security software; explore advanced measures for enhanced protection (Canadian Centre for Cyber Security, n.d.).

Selecting a Reliable Freight Carrier

Partnering with dependable freight carriers is crucial for any organization within a supply chain. On-time deliveries are essential for manufacturers to build customer trust and for retailers to ensure timely inventory for sales. For a resilient supply chain, reliable freight partners are essential. Here's what to assess :

- *Transit Time:* How long does the shipment take to reach customers?
- *Stops & Stop Times:* Fewer stops and quicker stops mean faster deliveries.
- *Loading Time:* Faster loading translates to smoother supply chain flow.
- *Route Optimization:* Efficient routes save on cost and time.
- *Maintenance Schedule:* Consistent maintenance reduces breakdown risk (Marotta, 2024).

Use of Technological Innovation

Technology empowers advanced supply chain analytics, enhancing both visibility and transparency. Following are some of the available options under technology:

- *Tracking & Monitoring:* Sensors, GPS, and IoT devices offer real-time data at every stage, from raw materials to finished products, allowing for:
- *Automation:* Robotic technologies increase efficiency and reduce human error, even in hazardous environments.
- *Blockchain:* This secure, shared ledger enhances transparency by verifying product authenticity and tracking goods movement.
- *AI & Machine Learning:* These powerful tools analyze vast datasets to:
    - *Optimize Routes:* Identify the most efficient transportation routes.
    - *Predict Disruptions:* Identify potential disruptions or inconsistencies.
    - *Environmental Impact:* Gain insights into the environmental footprint of the supply chain.
    - *Simulate Scenarios:* Model potential disruptions and develop contingency plans.

By leveraging these technologies, companies can build more resilient and robust supply chains (McGrath & Jonker, 2024).

Video: "How for Fix Broken Supply Chains | Dustin Burke | TED" by TED [11:02] is licensed under the Standard YouTube License. *Transcript and closed captions available on YouTube.*

Supply chain management thrives on smooth operations, but risks are inevitable. Supply chain risk management proactively identifies and addresses these vulnerabilities to ensure business continuity. By understanding and implementing Supply Chain Risk Management strategies, companies can build resilience and navigate the complexities of the global market.

8.5 CHAPTER SUMMARY

Summary

Risk management in supply chain and operations management involves identifying, assessing, and mitigating various risks that can disrupt the flow of goods and services. Key risks include demand variations, natural disasters, global events, supplier risks, cybersecurity threats, and ethical concerns. For instance, demand fluctuations can lead to excess inventory or stockouts, while natural disasters like earthquakes and floods can halt production and distribution. Supplier risks, including financial instability and quality issues, can disrupt supply chains, and cybersecurity threats can compromise data and operations. Ethical concerns, such as labour violations and environmental impact, also pose significant risks to supply chains.

To manage these risks, companies adopt strategies like multisourcing, nearshoring, stress testing, building buffers, and improving cybersecurity. Multisourcing reduces dependency on a single supplier, while nearshoring brings suppliers closer to core operations, reducing transportation risks. Stress testing identifies vulnerabilities through simulated disruption scenarios, and building buffers involves maintaining extra inventory and capacity. Enhancing cybersecurity includes standardizing security protocols, controlling access, vetting vendors, and implementing robust data governance. By leveraging technological innovations like IoT, blockchain, and AI, companies can enhance visibility, transparency, and resilience in their supply chains, ensuring business continuity amidst uncertainties.

OpenAI. (2024, June 28). *ChatGPT.* [Large language model]. https://chat.openai.com/chat

Prompt: *Please take the chapter content in this document attached and summarize the key concepts into no more than two paragraphs. Reviewed by authors.*

Key Terms

- **Nearshoring** involves strategically locating suppliers and distributors closer to your core operations or final product destinations.
- **Stress testing** is invaluable for identifying vulnerabilities, some of which may be deeply embedded within the supply chain.
- **Supply chain management** includes all activities that turn raw materials into finished goods and put them into customers' hands.
- **Supply chain risk management (SCRM)** is the process of finding and addressing potential vulnerabilities in a company's supply chain.

CHAPTER 9: EMERGING TRENDS IN RISK MANAGEMENT

Chapter Overview

9.0 LEARNING OUTCOMES

Learning Objectives

At the end of this chapter, students will be able to:

- Analyze the key factors driving the evolution of risk management practices, focusing on technological innovations and global complexities, and explain their implications for modern organizations.
- Evaluate the impact of advanced technologies such as IoT, blockchain, AI, and automation on risk management practices and demonstrate how these technologies can enhance risk identification, monitoring, and mitigation strategies.
- Assess the changing nature of risk, including cybersecurity, climate change, and geopolitical risks, and develop comprehensive risk mitigation strategies to address these emerging threats in a global business context.

9.1 INTRODUCTION

The field of risk management is experiencing a significant evolution, propelled by technological innovations, global complexities, and shifting business dynamics. Traditional risk management approaches are being reimagined to address the multifaceted challenges of our interconnected world. This chapter explores key trends transforming risk management practices, from the integration of AI and data analytics to the growing focus on organizational resilience. By embracing these emerging trends, businesses can mitigate risks more effectively and leverage risk management as a strategic tool for competitive advantage in an increasingly uncertain global landscape.

We will be discussing some of the important emerging trends in risk management.

9.2 USE OF TECHNOLOGY IN RISK MANAGEMENT

Integrating advanced technologies, particularly the Internet of Things (IoT), has revolutionized supply chain and logistics risk management practices. This technological evolution has enabled organizations to transition from reactive to proactive risk management strategies, fundamentally changing how risks are identified, monitored, and mitigated.

Tracking and Monitoring: The IoT Revolution

The Internet of Things has emerged as a game-changer in risk management, offering unprecedented capabilities in tracking and monitoring across the entire supply chain. IoT devices, including sensors, GPS trackers, and smart tags, create a vast network of interconnected objects that continuously collect and transmit data (SmartMakers, 2023).

Sensors

IoT sensors play a crucial role in monitoring various parameters critical to supply chain integrity:

- **Environmental Sensors:** These devices track temperature, humidity, and light exposure, crucial for perishable goods and sensitive materials. For instance, in pharmaceutical supply chains, temperature-sensitive medications can be monitored in real-time to ensure they remain within safe temperature ranges throughout transportation and storage.
- **Pressure and Impact Sensors:** These are vital for detecting potential damage to goods during transit. They can alert managers to mishandling or accidents, allowing for immediate intervention.
- **Chemical Sensors:** In industries dealing with hazardous materials, these sensors can detect leaks or contamination, preventing environmental hazards and ensuring worker

safety.

GPS Tracking

GPS technology integrated with IoT provides real-time location data of goods and vehicles:

- *Route Optimization:* By tracking the movement of delivery vehicles, companies can optimize routes, reducing fuel consumption and delivery times.
- *Theft Prevention:* Continuous tracking helps in quick detection and recovery of stolen goods.
- *Delay Prediction:* Real-time location data allows for accurate prediction of delays, enabling proactive communication with customers and stakeholders.

Smart Tags and RFID

Radio-Frequency Identification (RFID) and smart tags offer detailed tracking at the item level:

- *Inventory Management:* These technologies enable accurate, real-time inventory tracking, reducing the risk of stockouts or overstock situations.
- *Counterfeit Detection*: In industries prone to counterfeiting, such as luxury goods or pharmaceuticals, smart tags can verify product authenticity throughout the supply chain.

The vast amount of data collected through IoT devices serves as the foundation for optimizing supply chain operations and enhancing risk management strategies (SmartMakers, 2023).

Optimization: Supply chain data collected from various points can drive optimization by providing insights into operational efficiencies, potential risks and areas for improvement.

Automation

Automation is achieving impressive results with minimal human effort. Using technology, programs, robots, or even pre-defined processes to get things done with little to no human intervention is automation.

This powerful tool is rapidly becoming a fixture in our modern world. From running businesses more smoothly to creating conveniences in our homes, automation's applications are vast. In the business world, automation takes on many forms. It can streamline everyday tasks (business process automation), manage IT operations with artificial intelligence (AIOps), or even automate entire workflows (enterprise automation).

But its reach extends far beyond the office. Factories use robots powered by automation in car manufacturing, while smart home devices bring automation to our living rooms. From finance and healthcare to utilities and defence, there's hardly an industry untouched by automation's magic. It can be applied to all aspects of a business, giving organizations that leverage it effectively a significant edge over the competition.

Increased productivity and profits, improved customer service, reduced costs and errors, smoother compliance, and optimized efficiency are just a few benefits. Automation is a key ingredient in the recipe for digital transformation and a powerful ally for businesses looking to scale new heights.

There are different levels of automation to tackle repetitive tasks and streamline workflows (McGrath & Jonker, 2023):

1. **Basic Automation:** This level automates simple, routine tasks like sending invoices or onboarding new employees. It eliminates errors, speeds things up, and frees people for more strategic work.
2. **Process Automation:** This tackles more complex, multi-step processes across different systems. It boosts productivity, helps identify bottlenecks, and even suggests solutions using pre-defined rules. Tools like workflow automation and business process

management (BPM) fall under this category.

3. **Intelligent Automation:** This is the ultimate power-up, combining AI with other automation tools. Virtual agents that answer customer questions or AI assistants that help employees. It streamlines decision-making, reduces costs, and creates a smoother experience for everyone.

Key Benefits of Automation in Risk Management

Automation tools and robotics technology are revolutionizing risk management practices by increasing efficiency, reducing human error, and enhancing overall risk mitigation strategies. Key benefits of automation in risk management include:

1. *Reduced Human Error:* Automated systems perform tasks consistently, minimizing errors in critical processes such as data entry, compliance monitoring, and risk assessments.
2. *Real-time Risk Detection and Response:* Automation enables continuous critical process monitoring, allowing instantaneous detection and response to potential risks.
3. *Enhanced Decision Support:* AI-powered risk assessment tools can rapidly analyze complex datasets, supporting more informed decision-making.
4. *Improved Operational Efficiency:* Automation streamlines risk management processes, freeing up human resources for more strategic tasks.
5. *Enhanced Safety in Hazardous Environments:* Robotics and automated systems can operate in dangerous conditions, reducing human exposure to risks in industries like manufacturing, oil and gas, and nuclear power.
6. *Data Analysis and Reporting:* Automated systems can generate insights, trends, and detailed reports, aiding in risk analysis and decision-making.

While automation offers significant benefits, organizations must consider challenges such as potential over-reliance on technology, cybersecurity risks associated with connected systems, and the need for skilled personnel to manage these technologies (Valleskey, 2024; Wrobel, 2023).

Blockchain in Risk Management

Blockchain technology is emerging as a powerful tool for enhancing risk management practices across various industries. Its unique features offer several advantages in mitigating and managing risks:

1. *Immutability and Transparency:* Blockchain's immutable ledger provides an unalterable audit trail of all transactions, enhancing transparency and reducing the risk of fraud or data manipulation.
2. *Decentralization:* The distributed nature of blockchain eliminates single points of failure, improving resilience against cyber attacks and system failures.
3. *Smart Contracts:* Automated, self-executing contracts can reduce operational risks by minimizing human error and ensuring consistent execution of agreed-upon terms.
4. *Enhanced Data Security:* Cryptographic algorithms used in blockchain technology significantly improve data integrity and security, reducing the risk of data breaches.
5. *Real-time Risk Monitoring:* Blockchain enables real-time tracking and monitoring of transactions, allowing for quicker identification and response to potential risks.
6. *Improved Compliance:* The transparent and immutable nature of blockchain can streamline regulatory compliance and auditing processes.
7. *Supply Chain Risk Management:* In supply chains, blockchain can enhance traceability, reducing risks associated with counterfeiting, quality control, and provenance (Deloitte, 2017; Edwards, 2023).

Video: "How will blockchain be used in supply chain logistics ? | Zmodal" by Zmodal [3:06] is licensed under the Standard YouTube License. *Transcript and closed captions available on YouTube.*

As blockchain technology continues to evolve, its application in risk management is likely to expand. Organizations adopting blockchain for risk management should develop comprehensive strategies that address both the opportunities and challenges presented by this innovative technology.

AI and Machine Learning in Risk Management

Artificial Intelligence (AI) and Machine Learning (ML) are revolutionizing risk management practices across industries. These technologies offer powerful capabilities to enhance risk identification, assessment, and mitigation strategies.

Key Applications

1. *Predictive Analytics:* AI algorithms can analyze vast amounts of historical and real-time data to predict potential risks and their likelihood of occurrence.
2. *Fraud Detection:* ML models can identify unusual patterns and anomalies in transactions, helping to detect and prevent fraudulent activities.
3. *Credit Risk Assessment:* AI-powered systems can evaluate creditworthiness more accurately by analyzing diverse data points beyond traditional credit scores.
4. *Market Risk Management:* ML algorithms can process market data in real-time, enabling quicker responses to market volatility and potential risks.
5. *Operational Risk:* AI can monitor internal processes, identifying inefficiencies and potential points of failure.
6. *Compliance and Regulatory Risk:* Natural Language Processing (NLP) can assist in monitoring regulatory changes and ensuring compliance.

Benefits

- Enhanced accuracy in risk assessment
- Real-time risk monitoring and alerts
- Improved efficiency in risk management processes
- Better decision-making through data-driven insights (Resolver, 2023; Analyst Prep, 2023)

As AI and ML technologies continue to evolve, their role in risk management is expected to grow, offering more sophisticated and effective tools for managing complex risk landscapes.

Video: "AI Risk Management" by Now Next Later AI — AI Strategy & Transformation [5:20] is licensed under the Standard YouTube License. *Transcript and closed captions available on YouTube.*

In Supply Chain and Operations Management, AI and machine learning algorithms analyze massive datasets to find the most efficient routes, predict disruptions, and assess environmental impact in transportation. Simulation software complements this by modelling scenarios, aiding risk prediction and contingency planning (McGrath & Jonker, 2023).

9.3 EVOLVING RISK LANDSCAPE

Cybersecurity Risks

In today's digital age, cybersecurity risk has become a critical concern for individuals, organizations, and nations. **Cybersecurity risk** is the potential for loss or damage due to threats to information systems and data. As our reliance on technology grows, so does our vulnerability to cyber threats, making the understanding and management of these risks essential.

Canadian Centre for Cyber Security (2024) defines Cyber Security as

> The protection of digital information, as well as the integrity of the infrastructure housing and transmitting digital information. More specifically, cyber security includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability.

IBM (2024b) defines cyber risk management as "Cyber risk management, also called cybersecurity risk management, is the process of identifying, prioritizing, managing and monitoring risks to information systems" (para. 1).

Type of Cybersecurity Risks

Organizations and individuals face various cybersecurity risks in the ever-evolving landscape of digital threats. Understanding these risks is crucial for developing effective defence strategies. Here are the primary types of cybersecurity risks:

- **Malware:** Malware, short for malicious software, encompasses a broad range of threats designed to infiltrate, damage, or disrupt computer systems. This category includes (IBM, 2024a):
  - **Viruses**: Self-replicating programs that spread by attaching to files or programs
  - **Worms**: Self-propagating malware that spreads across networks
  - **Trojan horses**: Deceptive software that appears legitimate but contains malicious code
  - **Spyware**: Software that covertly gathers user information
- **Phishing and Social Engineering**: These attacks exploit human psychology rather than technical vulnerabilities. Techniques include:

    - **Email phishing**: Sending fraudulent emails to trick recipients into revealing sensitive information
    - **Spear phishing**: Targeted phishing attacks on specific individuals or organizations
    - **Vishing**: Voice phishing using phone calls to manipulate victims
    - **Pretexting**: Creating a fabricated scenario to obtain information
- **Ransomware**: A particularly disruptive form of malware that encrypts a victim's files and demands a ransom for their release. Ransomware attacks have become increasingly sophisticated and prevalent, targeting both individuals and large organizations.
- **Denial-of-Service (DoS) Attacks:** These attacks aim to overwhelm systems, networks, or services to make them inaccessible to intended users. Distributed Denial-of-Service (DDoS) attacks use multiple compromised systems to launch the attack, making them more difficult to mitigate.
- **Man-in-the-Middle (MitM) Attacks**: In these attacks, cybercriminals intercept communication between two parties, potentially eavesdropping or altering the data in transit. This can occur over unsecured Wi-Fi networks or through compromised web browsers.
- **Password Attacks**: Cybercriminals use various methods to obtain or crack passwords.
- **Insider Threats**: These risks come from within an organization, whether intentional or accidental. They can be current or former employees, contractors, or business partners with inside knowledge and access to systems.
- **Supply Chain Attacks**: Attackers target less secure elements in an organization's supply network to gain access to the primary target. This has become increasingly common as businesses rely more on third-party vendors and software.
- **IoT-based Attacks**: As the Internet of Things (IoT) expands, so do the potential vulnerabilities. Unsecured IoT devices can be exploited to gain access to networks or be used in large-scale DDoS attacks.
- **Code Injection Attacks**: These attacks involve inserting malicious code into vulnerable software applications. Common types include SQL injection and cross-site scripting (XSS) attacks.
- **DNS Tunneling**: This sophisticated technique uses the Domain Name System (DNS) protocol to bypass standard security measures, potentially exfiltrating data or establishing covert command and control channels.
- **AI-Powered Attacks**: As artificial intelligence becomes more advanced, cybercriminals are leveraging AI to enhance their attack capabilities, creating more sophisticated and harder-to-detect threats.
- **Zero-day Exploits**: These attacks target previously unknown vulnerabilities in software or systems. Because they exploit undiscovered weaknesses, zero-day attacks can be particularly dangerous and difficult to defend against (IBM, 2024a; Baker, 2024).

Cybersecurity Risk Sources

The cybersecurity landscape is populated by diverse actors with varying motivations and methods. Here's a breakdown of the key threats according to IBM (2024a):

- **Cybercriminals**: These actors engage in financially motivated cybercrime. Common tactics include ransomware attacks and phishing scams designed to steal sensitive data and extort funds.
- **Malicious Hackers**: These individuals possess advanced technical skills and utilize them for nefarious purposes. They may breach systems to exfiltrate critical information or disrupt operations.
- **Hackers**: Individuals with the skills to compromise a computer system or a network.
- **Nation-State Actors**: Cybersecurity threats can also originate from nation-states seeking to achieve strategic goals. These attacks, often well-funded and meticulously planned, may involve espionage to acquire sensitive information or cyberwarfare targeting critical infrastructure to disrupt essential services.
- **Insider Threats**: Employees, either through negligence or malicious intent, can inadvertently or intentionally expose an organization to significant risk. Unintentional actions may involve accidentally installing malware or losing a company device containing sensitive data. In more egregious cases, employees may deliberately compromise systems or steal information for personal gain.

Risk Mitigation Strategies

Effective cybersecurity risk mitigation involves a multi-layered approach combining technical, administrative, and physical controls and robust incident response and disaster recovery planning.

Technical Controls

- *Firewalls:* Filter network traffic
- *Encryption:* Protect data confidentiality
- *Access Controls:* Limit user access based on need

Administrative Controls

- *Policies and Procedures:* Establish security guidelines
- *Training:* Educate employees on cybersecurity awareness
- *Risk Assessments:* Identify and prioritize vulnerabilities

Physical Controls

- *Secure Facilities:* Restrict access to critical areas
- *Biometrics:* Advanced authentication for high-security zones

Incident Response and Disaster Recovery

- *Incident Response Plan:* Approach for handling security incidents
- *Disaster Recovery Plan:* Procedures for quick system and data restoration

This comprehensive strategy helps organizations reduce cybersecurity risks and enhance their overall security posture.

Climate Change and Environmental Risks

Climate change and associated environmental risks pose significant challenges to businesses across various sectors. These risks can profoundly impact operations and necessitate adherence to evolving regulatory frameworks.

Video: "Comprehensive Disaster and Climate Risk Management" by United Nations Office for Disaster Risk Reduction [3:56] is licensed under the Standard YouTube License. *Transcript and closed captions available on YouTube.*

Impact on Business Operations

Climate change and environmental risks increasingly affect businesses across various sectors, presenting challenges and opportunities. Here's how these risks impact business operations:

1. *Physical Risks:* Extreme weather events like floods, hurricanes, and droughts can damage

infrastructure, disrupt supply chains, and lead to operational downtime.
2. *Resource Scarcity:* Climate change can affect the availability of critical resources, potentially increasing costs and disrupting production.
3. *Market Shifts:* Changing consumer preferences towards sustainable products can impact demand and revenue streams.
4. *Employee Health and Productivity:* Increased temperatures and air pollution can affect worker health and productivity, particularly in outdoor industries.
5. *Supply Chain Disruptions:* Climate-related events can cause delays, shortages, and increased costs throughout the supply chain.
6. *Financial Impacts:* Businesses may face higher insurance premiums, increased operational costs, and potential asset devaluation in high-risk areas.

These impacts underscore the need for businesses to integrate climate and environmental considerations into their strategic planning and risk management processes. Companies that proactively address these challenges may find opportunities for innovation, cost savings, and competitive advantage in an increasingly climate-conscious market (Boyles, 2024; Kole, 2023).

Climate change and sustainability are discussed in detail in Chapter 10 of this book.

Geopolitical Risks

Geopolitical risks have become an increasingly critical factor in the global business landscape. These risks encompass a wide range of threats stemming from political tensions, international conflicts, and shifts in global power dynamics. From trade wars and economic sanctions to regional instabilities and cyber threats, geopolitical risks can significantly impact business operations, financial markets, and economic growth. As the world becomes more interconnected, the ripple effects of geopolitical events can be felt across borders, industries, and supply chains, making it essential for businesses and investors to understand and navigate these complex challenges (Kaya, 2024).

Video: "Measuring geopolitical risk" by Export Development Canada | Exportation et développement Canada – EDC [6:18] is licensed under the Standard YouTube License. *Transcript and closed captions available on YouTube.*

Geopolitical risks represent a complex and evolving set of challenges that can significantly impact businesses and economies worldwide. These risks stem from various factors, including international conflicts, political tensions, and shifts in global power dynamics. Key geopolitical risks include:

1. *Global Conflicts:* Ongoing and emerging international conflicts can disrupt business operations, affect investments, and cause supply chain issues.
2. *Economic Sanctions:* The increasing use of sanctions as a political tool can create compliance challenges and market access issues for businesses.
3. *Social Unrest:* Political demonstrations and activism can pose risks to assets and security across various sectors and countries.
4. *Misinformation and Disinformation:* These pose growing threats to businesses, potentially leading to reputational damage and financial losses.
5. *Cybersecurity Threats:* Increased cyber attacks, often linked to geopolitical tensions, target both government and private sector entities.
6. *Regulatory Changes:* Shifts in international governance and regulatory frameworks can create compliance challenges for businesses operating globally.
7. *Supply Chain Disruptions:* Geopolitical tensions can impact supply chain integrity, forcing companies to reconsider their networks and partnerships.
8. *Economic Instability:* Factors like inflation and currency fluctuations can affect international business operations and contracts.

To navigate these risks, businesses must stay informed, conduct regular risk assessments, and develop flexible strategies to adapt to the changing global landscape (Mason & Oxnevard, 2024).

9.4 CHAPTER SUMMARY

Summary

Chapter 9, “Emerging Trends in Risk Management,” explores how technological advancements and global complexities are reshaping traditional risk management practices. Key technologies like the Internet of Things (IoT), blockchain, artificial intelligence (AI), and machine learning are revolutionizing the field by enabling real-time tracking, predictive analytics, and enhanced data security. IoT devices, for instance, provide continuous data collection and monitoring across supply chains, improving risk identification and mitigation. Automation reduces human error, enhances operational efficiency, and offers real-time risk detection, while blockchain ensures data integrity and transparency. AI and machine learning facilitate advanced risk assessment and fraud detection, significantly enhancing decision-making processes.

The chapter also addresses the evolving risk landscape, highlighting the increasing importance of cybersecurity, climate change, and geopolitical risks. Cybersecurity threats, including malware, phishing, and ransomware, pose significant challenges, necessitating robust mitigation strategies such as firewalls, encryption, and incident response plans. Climate change impacts business operations through physical risks and resource scarcity, requiring companies to integrate environmental considerations into their risk management frameworks. Geopolitical risks, driven by political tensions and global power shifts, demand adaptive strategies to navigate the complexities of international business. By embracing these emerging trends and technologies, organizations can better manage risks and leverage them for strategic advantage in a rapidly changing global environment.

OpenAI. (2024, July 4). *ChatGPT.* [Large language model]. https://chat.openai.com/chat

Prompt: *Please take the chapter content in this document attached and summarize the key concepts into no more than two paragraphs. Reviewed by authors.*

Key Terms

- **AI-Powered Attacks**: As artificial intelligence becomes more advanced, cybercriminals are leveraging AI to enhance their attack capabilities, creating more sophisticated and harder-to-detect threats (Baker, 2024).
- **Automation is** achieving impressive results with minimal human effort. Using technology, programs, robots, or even pre-defined processes to get things done with little to no human intervention is automation.
- **Basic Automation:** This level automates simple, routine tasks like sending invoices or onboarding new employees.
- **Chemical Sensors:** In industries dealing with hazardous materials, these sensors can detect leaks or contamination, preventing environmental hazards and ensuring worker safety.
- **Code Injection Attacks**: These attacks involve inserting malicious code into vulnerable software applications. Common types include SQL injection and cross-site scripting (XSS) attacks.
- **Cybercriminals**: These actors engage in financially motivated cybercrime. Common tactics include ransomware attacks and phishing scams designed to steal sensitive data and extort funds.
- **Cybersecurity risk** is the potential for loss or damage due to threats to information systems and data.
- **Denial-of-Service (DoS) Attacks:** These attacks aim to overwhelm systems, networks, or services to make them inaccessible to intended users (IBM, 2024a).
- **DNS Tunneling**: This sophisticated technique uses the Domain Name System (DNS) protocol to bypass standard security measures, potentially exfiltrating data or establishing covert command and control channels (Baker, 2024).
- **Effective cybersecurity risk mitigation** involves a multi-layered approach combining technical, administrative, and physical controls and robust incident response and disaster

recovery planning.

- **Email phishing**: Sending fraudulent emails to trick recipients into revealing sensitive information
- **Environmental Sensors:** These devices track temperature, humidity, and light exposure, crucial for perishable goods and sensitive materials.
- **Hackers**: Individuals with the skills to compromise a computer system or a network.
- **Insider Threats**: Employees, either through negligence or malicious intent, can inadvertently or intentionally expose an organization to significant risk. Unintentional actions may involve accidentally installing malware or losing a company device containing sensitive data. In more egregious cases, employees may deliberately compromise systems or steal information for personal gain.
- **Insider Threats**: These risks come from within an organization, whether intentional or accidental. They can be current or former employees, contractors, or business partners with inside knowledge and access to systems (Baker, 2024).
- **Intelligent Automation:** This is the ultimate power-up, combining AI with other automation tools. Virtual agents that answer customer questions or AI assistants that help employees.
- **IoT-based Attacks**: Unsecured IoT devices can be exploited to gain access to networks or be used in large-scale DDoS attacks (Baker, 2024).
- **Malicious Hackers**: These individuals possess advanced technical skills and utilize them for nefarious purposes. They may breach systems to exfiltrate critical information or disrupt operations.
- **Malware:** Malware, short for malicious software, encompasses a broad range of threats designed to infiltrate, damage, or disrupt computer systems (IBM, 2024a).
- **Man-in-the-Middle (MitM) Attacks**: In these attacks, cybercriminals intercept communication between two parties, potentially eavesdropping or altering the data in transit. This can occur over unsecured Wi-Fi networks or through compromised web browsers (IBM, 2024a).
- **Nation-State Actors**: These attacks, often well-funded and meticulously planned, may involve espionage to acquire sensitive information or cyberwarfare targeting critical infrastructure to disrupt essential services.
- **Password Attacks**: Cybercriminals use various methods to obtain or crack passwords.
- **Phishing and Social Engineering**: These attacks exploit human psychology rather than technical vulnerabilities (IBM, 2024a).
- **Pressure and Impact Sensors:** These are vital for detecting potential damage to goods

during transit. They can alert managers to mishandling or accidents, allowing for immediate intervention.

- **Pretexting**: Creating a fabricated scenario to obtain information
- **Process Automation:** This tackles more complex, multi-step processes across different systems. It boosts productivity, helps identify bottlenecks, and even suggests solutions using pre-defined rules.
- **Ransomware**: A particularly disruptive form of malware that encrypts a victim's files and demands a ransom for their release (IBM, 2024a).
- **Spear phishing**: Targeted phishing attacks on specific individuals or organizations
- **Spyware**: Software that covertly gathers user information
- **Supply Chain Attacks**: Attackers target less secure elements in an organization's supply network to gain access to the primary target (Baker, 2024).
- **Trojan horses**: Deceptive software that appears legitimate but contains malicious code
- **Viruses**: Self-replicating programs that spread by attaching to files or programs
- **Vishing**: Voice phishing using phone calls to manipulate victims
- **Worms**: Self-propagating malware that spreads across networks
- **Zero-day Exploits**: These attacks target previously unknown vulnerabilities in software or systems. Because they exploit undiscovered weaknesses, zero-day attacks can be particularly dangerous and difficult to defend against. (IBM, 2024a)

CHAPTER 10: RISK MANAGEMENT FROM A SUSTAINABILITY PERSPECTIVE

Chapter Overview

10.0 LEARNING OUTCOMES

Learning Objectives

At the end of this chapter, students will be able to:

- Analyze the paradigm shift from traditional risk management to sustainable risk management, highlighting the key differences and implications for organizations in the 21st century.
- Evaluate the interconnectivity between sustainability challenges and organizational risks, providing examples of how sustainability issues can impact various aspects of an organization's operations.
- Identify and classify the different types of ESG risks, explaining their potential impacts on an organization's value, operations, and long-term viability.
- Apply various sustainability risk management frameworks, such as the UN SDGs, TCFD recommendations, and GRI Standards, to develop strategies for assessing and mitigating ESG-related risks.
- Assess how integrating sustainability into risk management can create opportunities for competitive advantage, innovation, improved decision-making, and enhanced stakeholder trust and reputation.

10.1 INTRODUCTION

In today's rapidly evolving global landscape, integrating sustainability into risk management has become crucial for organizations across all sectors. Risk management from a sustainability perspective represents a paradigm shift, offering a more comprehensive approach to addressing the complex challenges of the 21st century.

This approach can be defined as the process of identifying, assessing, and responding to potential threats and opportunities related to environmental, social, and governance (ESG) factors that may impact an organization's long-term value creation and protection. It recognizes the inextricable link between sustainability issues, an organization's risk profile, and overall performance.

The importance of this integration cannot be overstated. Traditional risk management approaches are no longer sufficient as organizations face interconnected challenges such as climate change, resource scarcity, and shifting societal expectations. By incorporating sustainability considerations, organizations can better anticipate and respond to emerging challenges while identifying opportunities for innovation and value creation.

This evolution requires a significant shift from conventional practices. While traditional risk management typically focuses on short-term, easily quantifiable risks, sustainable risk management demands a longer-term perspective and the consideration of complex, often qualitative factors. This necessitates new tools, metrics, and ways of thinking about risk and value creation.

Understanding the intersection of risk management and sustainability is crucial for students preparing to enter or advance in the business world. It equips future leaders with the knowledge and skills needed to navigate complex challenges, fostering organizational resilience and driving sustainable value creation in an increasingly interconnected world.

10.2 SUSTAINABILITY AND RISK

Sustainability issues and organizational risks are deeply interconnected in today's business environment. This interconnectivity manifests in several key ways:

1. Sustainability challenges can create significant risks for organizations, while organizational decisions and risk management practices can impact sustainability outcomes.
2. Sustainability risks often have ripple effects across various aspects of an organization's operations and the broader economy. For example, climate change can simultaneously affect supply chains, asset values, and market demand.
3. These risks stem from complex *environmental, social, and governance (ESG)* systems, often affecting multiple organizational aspects concurrently.
4. Sustainability risks typically unfold over longer timeframes than traditional business risks, making them challenging to predict and manage.
5. The complex nature of sustainability risks often makes them difficult to quantify using traditional risk assessment methods.

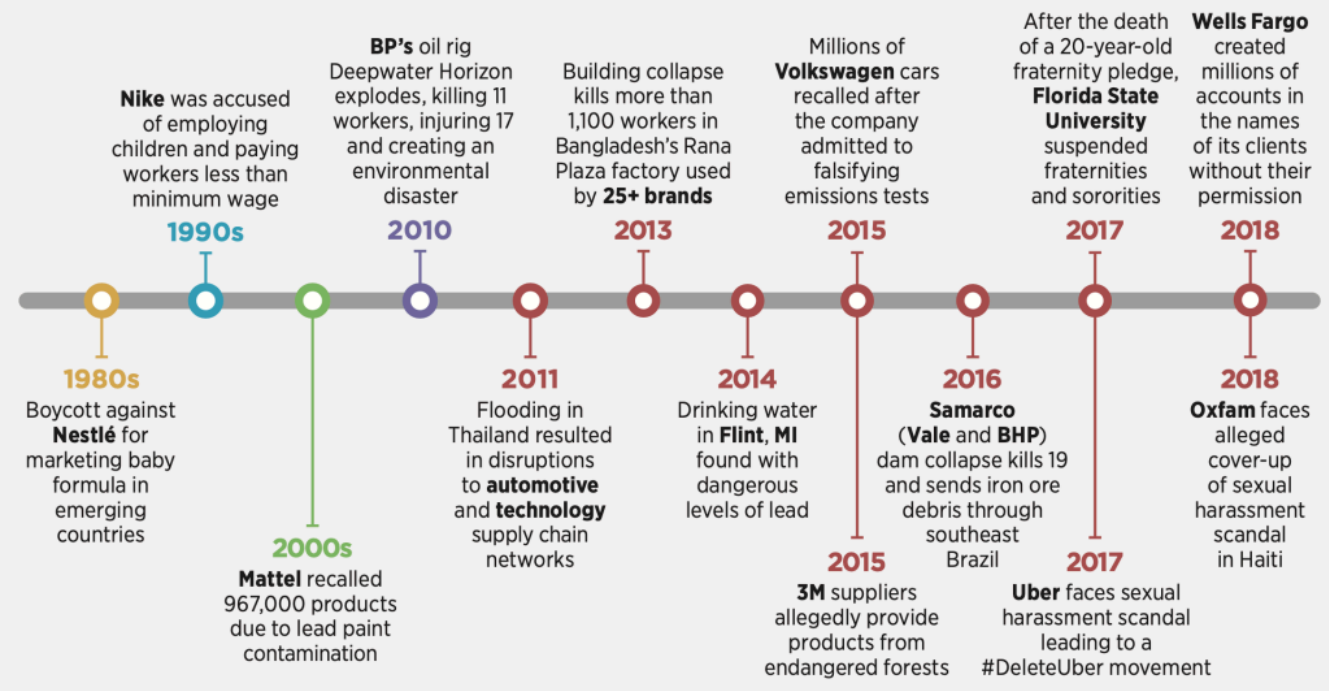

Figure 10.2.1: "Examples of Organizations that have experienced ESG-related impacts" in *Enterprise Risk Management: enterprise risk management to environmental, social and governance-related risks*, © 2018 Committee of Sponsoring Organizations of the Treadway Commission (COSO) and World Business Council for Sustainable Development (WBCSD). All rights reserved. Used with permission. (See Acceptable Use of COSO Materials [PDF] for permission details).

Image Description

The image is a timeline that highlights various significant incidents involving organizations that have experienced environmental, social, and governance (ESG) related impacts. The events are as follows:

1. **1980s**: Boycott against Nestlé for marketing baby formula in emerging countries.
2. **1990s**: Nike accused of employing children and paying workers less than minimum wage.
3. **2000s**: Mattel recalls 967,000 products due to lead paint contamination.
4. **2010**: BP's oil rig Deepwater Horizon explodes, killing 11 workers, injuring 17, and creating an environmental disaster.
5. **2011**: Flooding in Thailand disrupts automotive and technology supply chain networks.
6. **2013**: Building collapse in Bangladesh's Rana Plaza factory kills more than 1,100 workers; over 25 brands used this factory.
7. **2014**: Drinking water in Flint, MI, found with dangerous levels of lead.
8. **2015**: Millions of Volkswagen cars recalled after the company admitted to falsifying emissions tests.
9. **2015**: 3M suppliers allegedly provided products from endangered forests.
10. **2016**: Samarco (Vale and BHP) dam collapse kills 19 and sends iron ore debris through southeast Brazil.

11. **2017**: Uber faces a sexual harassment scandal leading to the #DeleteUber movement.
12. **2017**: After the death of a 20-year-old fraternity pledge, Florida State University suspends fraternities and sororities.
13. **2018**: Wells Fargo created millions of accounts in the names of its clients without their permission.
14. **2018**: Oxfam faces alleged cover-up of a sexual harassment scandal in Haiti.

The figure above shows examples of how ESG-related risks impacted some known organizations.

To effectively manage these interconnected risks, organizations need to:

- Adopt a holistic approach to risk assessment and mitigation
- Integrate ESG factors into traditional risk management frameworks
- Develop new metrics and tools for measuring sustainability-related risks
- Enhance transparency around sustainability risks and opportunities
- Align business strategies with sustainability goals

Understanding this interconnectivity is crucial for modern risk management. It allows organizations to mitigate potential threats and identify opportunities for innovation and value creation in a rapidly changing world (Segun, 2023).

10.3 TYPES OF SUSTAINABILITY RISKS: ENVIRONMENTAL, SOCIAL, AND GOVERNANCE (ESG)

Sustainability risks are environmental, social, or governance events or conditions that, if they occur, could cause a negative material impact on an organization's value, operations, and long-term viability. These risks are often interconnected and can have cascading effects across different aspects of an organization's operations and the broader economy. Understanding and managing these risks is crucial for effective risk management and sustainable business practices (Segun, 2023).

Video: "Sustainability 101: ESG Reporting" by Constellation [3:47] is licensed under the Standard YouTube License. *Transcript and closed captions available on YouTube.*

Environmental Risks

Environmental risks stem from an organization's impact on and dependence on the natural environment. Key environmental risks include (COSO, 2018):

- *Climate Change:* The increasing frequency and severity of natural disasters pose significant threats to business operations, supply chains, and infrastructure.
- *Natural Resources:* Depletion of natural resources can lead to increased operational costs and supply chain disruptions.
- *Waste Management & Pollution:* Mishandling of industrial waste and increase in pollution
- *Environmental Opportunities:* Pollution, deforestation, and other forms of environmental damage can lead to regulatory penalties and reputational damage.

Social Risks

Social risks relate to an organization's impact on and relationship with society, including its workforce, customers, and communities. Key social risks include (COSO, 2018):

- *Human Rights:* Violations in the supply chain or operations can lead to legal consequences and severe reputational damage.
- *Labour Standards Problems:* Poor working conditions, unfair wages, or lack of diversity and inclusion can result in talent retention issues and negative public perception.
- *Social Inequality:* Growing wealth disparities can lead to social unrest and market instability.
- *Community Relations:* Failure to engage positively with local communities can result in loss of social license to operate.

Governance Risks

Governance risks are how an organization is managed, overseen, and held accountable. Key governance risks include (COSO, 2018):

- *Corporate Governance:* Poor decision-making structures, lack of transparency, or unethical practices can lead to financial losses and reputational damage.
- *Regulatory Compliance:* Evolving sustainability regulations can create compliance risks and additional costs.
- *Business Ethics:* Unethical business practices can result in legal penalties and loss of stakeholder trust.
- *Executive Compensation/Board Pay:* Excessive or misaligned executive pay can lead to stakeholder dissatisfaction and reputational issues.

Table 10.3.1: "MSCI ESG Issues and Themes" in *Enterprise Risk Management: enterprise risk management to environmental, social and governance-related risks*, © 2018 Committee of Sponsoring Organizations of the Treadway Commission (COSO) and World Business Council for Sustainable Development (WBCSD). All rights reserved. Used with permission. (See Acceptable Use of COSO Materials [PDF] for permission details).

3 pillars	10 themes	37 ESG key issues
Environment	Climate change	• Carbon emissions • Product carbon footprint • Financing environmental impact • Climate change vulnerability
	Natural resources	• Water stress • Biodiversity and land use • Raw material sourcing
	Pollution and waste	• Toxic emissions and waste • Packaging materiality and waste • Electronic waste
	Environmental opportunities	• Opportunities in clean tech • Opportunities in green building • Opportunities in renewable energy
Social	Human capital	• Labor management • Health and Safety • Human capital development • Supply chain labour standards
	Product liability	• Product safety and quality • Chemical safety • Financial product safety • Privacy and data security • Responsible investment • Health and demographic risk
	Stakeholder opposition	• Controversial sourcing

	Social opportunities	• Access to communications • Access to finance • Access to healthcare • Opportunities in nutrition and health
Governance	Corporate governance	• Board • Pay • Ownership • Accounting
	Corporate behavior	• Business ethics • Anti-competitive practices • Tax transparency • Corruption and instability • Financial system instability

Interconnectedness of ESG Risks

It's important to note that these risk categories are often interconnected. For example:

- Climate change (environmental risk) can lead to resource scarcity, which may cause social unrest (social risk).
- Poor governance practices can result in inadequate environmental management or labour issues.
- Social issues like inequality can influence consumer behaviour, affecting a company's market position.

Managing ESG Risks

Effective management of ESG risks requires:

1. Integration of ESG factors into overall risk management frameworks
2. Development of new metrics and tools to measure and monitor sustainability-related risks
3. Enhanced disclosure and transparency around sustainability risks and opportunities
4. Alignment of business strategies with sustainability goals

Figure 10.3.1: "COSO ERM – ESG Integration" in *Enterprise Risk Management: enterprise risk management to environmental, social and governance-related risks*, © 2018 Committee of Sponsoring Organizations of the Treadway Commission (COSO) and World Business Council for Sustainable Development (WBCSD). All rights reserved. Used with permission. (See Acceptable Use of COSO Materials [PDF] for permission details).

Image Description

The image presents a colourful DNA-like spiral graphic that outlines the steps for integrating and managing Environmental, Social, and Governance (ESG) risks within an organization. Each segment of the spiral corresponds to a step in the ESG risk management process:

1. **Governance & Culture for ESG-Related Risks** (represented by a yellow circle with people icons)
2. **Strategy & Objective-Setting for ESG-Related Risks** (represented by a blue circle with gear icons)
3. **Performance for ESG-Related Risks** (represented by a green circle with a magnifying glass and plus sign icons):

    - Encompasses three sub-steps: a. Identifies Risk b. Assesses & Prioritizes Risks c. Implements Risk Responses

4. **Review & Revision for ESG-Related Risks** (represented by a purple circle with document icons)
5. **Information, Communication & Reporting for ESG-Related Risks** (represented by a red circle with communication and reporting icons)

The DNA-like spiral visually connects these steps, illustrating the integrated and continuous nature of managing ESG-related risks.

By understanding and proactively addressing these risks, organizations can mitigate potential threats and identify opportunities for innovation, efficiency, and value creation in a rapidly changing world (COSO, 2018).

How Sustainability Risks Can Impact

The financial impact of deforestation-free supply chains on Brazilian beef production

Brazil is the world's largest exporter of beef, making up almost 20% of the world market. However, the impact on Brazil's natural resources – and global GHG emissions – is significant. With only 1% of beef production in Brazil certified as sustainable, NYU Stern's Center for Sustainable Business led a research project to assess the financial benefits (e.g., productivity and profitability) of shifting to sustainable beef production. This analysis assessed the benefits for all players in the industry's value chain – namely, ranchers, slaughterhouses and retailers.

The project looked at the benefits of sustainable and deforestation-free practices across five areas: cost reduction, revenue increase, risk avoidance, financial and valuation, and other. Using research,

data analysis and interviews, benefits were calculated based on market demand, probabilities and penalty costs consistent with each indicator.

The results are powerful for decision-makers, with evidence that sustainable agricultural practices lead to improved profitability across the value chain. The uptake of sustainable agricultural practices provided the most financial benefit, while the uptake of deforestation-free commitments reduced risk. In particular, ranchers reaped the most benefits as a percentage of total income – between USD$18 million and USD$34 million (12% and 23% of revenues) net present value over ten years.

Sustainability risks are environmental, social, and governance (ESG) factors that can significantly impact an organization's operations, financial performance, and long-term viability. The following are some of the most critical sustainability risks facing businesses today:

1. *Climate Change and Extreme Weather Events:* Climate change poses both physical risks (e.g., increased frequency and severity of natural disasters) and transition risks (e.g., policy changes, market shifts). These can disrupt operations, damage infrastructure, and affect supply chains (ESG Risk Guard, n.d.).
2. *Resource Scarcity and Biodiversity Loss:* Depletion of natural resources and loss of biodiversity can lead to increased operational costs, supply chain disruptions, and reduced ecosystem services that many industries rely on (World Economic Forum, 2023).
3. *Social Inequality and Human Rights Issues:* Growing wealth disparities and human rights concerns can lead to social unrest, reputational damage, and legal consequences. These issues can affect labour markets, consumer behaviour, and a company's social license to operate (ESG Risk Guard, 2024).
4. *Regulatory Changes and Compliance Challenges:* Evolving sustainability regulations can

create compliance risks and additional costs. Failure to comply can result in penalties, legal action, and reputational damage (ESG Risk Guard, n.d.).

5. *Technological Disruptions and Transitions:* The shift towards sustainable technologies can render existing products or processes obsolete. Companies that fail to adapt may lose competitive advantage and market share (COSO, 2018).

These risks are often interconnected and can have cascading effects across different aspects of an organization's operations and the broader economy. Effective management of these sustainability risks requires integrating ESG factors into overall risk management frameworks, developing robust sustainability strategies, and proactively adapting to changing environmental and social landscapes.

Following are some of the examples of how organizations are impacted:

Examples

Financial Performance

- Increased operational costs due to resource scarcity or climate change
- Compliance costs from evolving sustainability regulations
- Revenue impacts from shifting consumer preferences towards sustainable products
- Limited access to capital or higher costs of capital due to poor sustainability performance
- Supply chain disruptions affecting sales and profitability
- Potential asset impairment due to climate change and resource scarcity

Reputation

- Damage to brand value and consumer trust
- Strained relationships with key stakeholders
- Negative media attention
- Difficulties in attracting and retaining talent

Long-term Viability

- Threats to license to operate in certain markets
- Risk of technological obsolescence if failing to adapt to sustainable technologies
- Existential threats for companies heavily reliant on scarce resources

Table 10.3.2: "Examples of Risk Owners for ESG-Related risks "*Enterprise Risk Management: enterprise risk management to environmental, social and governance-related risks*, © 2018 Committee of Sponsoring Organizations of the Treadway Commission (COSO) and World Business Council for Sustainable Development (WBCSD). All rights reserved. Used with permission. (See Acceptable Use of COSO Materials [PDF] for permission details).

Enterprise-level risk	ESG element	Relevant risk owner	Supporting the risk owner
Risk of increasing raw material prices	Change in prices caused by rising energy costs associated with climate change regulation	Vice president of supply chain	Chief sustainability officer/ Sustainability analyst (energy)
Risk of injury or fatality in operations	Health- and safety-related considerations	Environmental health and safety manager	Site managers
Risk of reputational damage because of poor communication on ESG issues in the supply chain	Pressure for greater supply chain transparency around human rights	Chief procurement officer	Chief sustainability officer

Effective management of these risks requires integrating ESG factors into risk management frameworks, developing robust sustainability strategies, enhancing transparency, investing in sustainable innovation, and proactively engaging with stakeholders. This approach mitigates potential negative impacts and identifies opportunities for innovation and value creation, essential for maintaining competitiveness and ensuring long-term viability in a rapidly changing business environment (Federation of European Risk Management Association, 2021; Segun, 2021).

10.4 FRAMEWORKS FOR SUSTAINABLE RISK MANAGEMENT

In response to growing demands for transparency and accountability on environmental, social, and governance (ESG) issues, many voluntary frameworks have emerged. These frameworks provide companies with standardized structures to report on their ESG performance, catering to the information needs of external stakeholders.

Benefits of Voluntary Frameworks

Voluntary ESG reporting frameworks offer several advantages for businesses:

- *Standardization:* They create a common language for ESG reporting, allowing for easier comparison between companies in the same industry.
- *Transparency:* Following a framework helps companies disclose relevant ESG information to investors, regulators, and other stakeholders.
- *Improved Management:* The reporting process can encourage companies to identify and manage ESG risks more effectively.
- *Enhanced Credibility:* Alignment with a recognized framework can boost a company's reputation for responsible business practices.

The table below highlights some of the prominent voluntary ESG reporting frameworks organizations use to disclose ESG risks and their management strategies.

Table 10.4.1: "Existing guidance to support external ESG-related risk disclosures" *Enterprise Risk Management: enterprise risk management to environmental, social and governance-related risks*, © 2018 Committee of Sponsoring Organizations of the Treadway Commission (COSO) and World Business Council for Sustainable Development (WBCSD). All rights reserved. Used with permission. (See Acceptable Use of COSO Materials [PDF] for permission details).

Framework	Addresses financial filings, annual reports or ESG-specific reports	Description
CDSB Framework	Financial filings and annual reports	• Recommends reporting requirements for disclosing environmental information in mainstream reports where that information is material to an understanding of companies' financial risks and opportunities, as well as the resilience of their business models • Aligns with TCFD recommendations
GRI	ESG-specific reports	• Provides a widely adopted framework for reporting material economic, environmental, social and governance issues • Advises reporting on topics that present risks to a company's business model or reputation
<IR> Framework	Annual reports	• Provides a framework for integrated reporting on all six capitals (i.e., financial, manufactured, intellectual, human, social and relationship, and natural) • Advises entities to disclose the specific risks that affect the ability to create value over the short, medium and long term and how the organization manages them
Recommendations of the TCFD	Financial filings	• Recommends voluntary disclosures for companies to report on governance, risk management and impacts of climate change on the organization • Includes industry-specific guidance
SASB Implementation Guide and Reporting Guidelines	Financial filings	• Provides a framework for management to assess financial materiality of sustainability issues, considering risk, for inclusion in financial reports • Recommends minimum disclosure requirements by sustainability issue • Includes industry-specific guidance
Sustainable Development Goals	ESG-specific reports	• Offers goals and targets that organizations can consider in presenting their impacts

Some of them are explained below:

UN Sustainable Development Goals (SDGs) as a Risk Management Tool

Video: "Do you know all 17 SDGs?" by United Nations [1:25] is licensed under the Standard YouTube License. *Transcript and closed captions available on YouTube.*

The 17 SDGs, adopted by all United Nations Member States in 2015, provide a shared blueprint for peace and prosperity for people and the planet. While primarily designed as development goals, they can also serve as a risk management tool for organizations. SDGs help identify potential sustainability risks and opportunities relevant to an organization's operations and value chain. They provide a common language for communicating sustainability efforts to stakeholders. Aligning business strategies with SDGs can help organizations anticipate and mitigate future resource scarcity, climate change, and social inequality risks (UN Department of Economic & Social Affairs, n.d.).

Task Force on Climate-Related Financial Disclosures (TCFD) Recommendations

Video: "2020 TCFD Status Report – Message from Mike Bloomberg" by Secretariat TCFD [1:24] is licensed under the Vimeo Terms of Use. Transcript.

The **TCFD**, established by the Financial Stability Board (FSB – an international body that monitors and makes recommendations about the global financial system), provides recommendations for more effective climate-related disclosures. TCFD framework focuses on governance, strategy, risk management, and metrics and targets related to climate risks and opportunities. It encourages scenario analysis to assess the potential impact of climate-related risks and opportunities on an organization's business strategy and financial planning. TCFD recommendations help organizations integrate climate-related risks into their existing risk management processes (TCFD, n.d.).

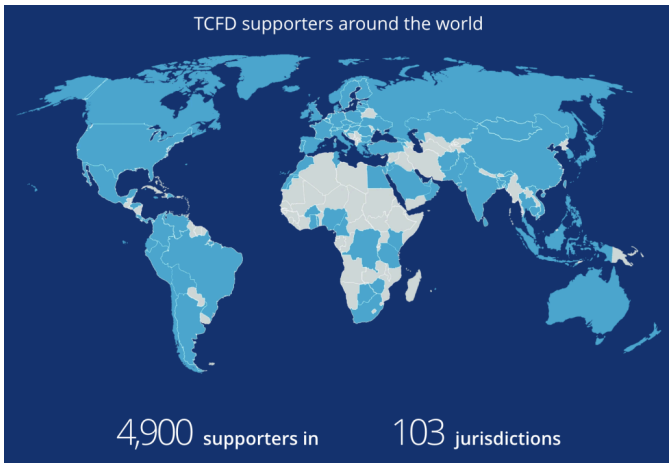

Figure 10.4.1: "TCFD supporters around the world" by TCFD. Used under Fair Dealing for Educational Purposes (Canada).

Global Reporting Initiative (GRI) Standards

Video: "Sustainability reporting with the GRI Standards" by GRI Secretariat [2:41] is licensed under the Standard YouTube License. *Transcript and closed captions available on YouTube.*

GRI (Global Reporting Initiative) is an independent, international organization that helps businesses and other organizations take responsibility for their impacts by providing them with a global common language to communicate those impacts. The GRI Secretariat is headquartered in Amsterdam, Netherlands, and has a network of seven regional offices worldwide.

The GRI Standards are the widely adopted global standards for sustainability reporting. They provide a comprehensive framework for reporting on economic, environmental, and social impacts. GRI Standards help organizations identify and assess material sustainability topics, which often correlate with key risks and opportunities. The standards promote transparency and accountability in sustainability performance, which can enhance stakeholder trust and support risk management efforts (Global Reporting Initiative, n.d.).

Example

Selecting indicators to monitor risk

To determine appropriate indicators to monitor a risk, risk management and sustainability practitioners may leverage the entity's key performance indicators (e.g., target employee retention, carbon intensity reduction target) or existing ESG-related frameworks used for sustainability reporting, such as the GRI. Although not designed to measure risks, the GRI indicators can provide example metrics used to review the organization's response and performance. The table below shows how GRI's water standard could be used for this purpose (COSO, 2018).

Table 10.4.2: "Example application of GRI to risk monitoring" *Enterprise Risk Management: enterprise risk management to environmental, social and governance-related risks*, © 2018 Committee of Sponsoring Organizations of the Treadway Commission (COSO) and World Business Council for Sustainable Development (WBCSD). All rights reserved. Used with permission. (See Acceptable Use of COSO Materials [PDF] for permission details).

Metrics	Description
Risk	Water scarcity impacts the entity's ability to operate.
Response	The entity is decreasing its water use, increasing its recycling and monitoring the water table to prevent further reductions.
Monitoring indicators	• Total water withdrawal by source and allocable share of water availability • Total water sources significantly affected by withdrawal • Total volume of water recycled and reused

Risk Assessment Techniques for ESG-Related Risks

A good risk assessment isn't just about listing potential problems. It's about understanding how those problems could impact a company's ability to achieve its goals. Organizations achieve this by (COSO, 2018):

1. *Identifying the Consequences:* This means figuring out how a risk could affect the company's operations, finances, or reputation.
2. *Choosing the Right Tools:* Different risks require different assessment methods. Some might be evaluated with a simple scoring system, while others require more complex financial modelling.

These steps help guide discussions about which risks are most important to address. This prioritization considers two key factors:

- *Severity:* How badly could this risk hurt the company's ability to achieve its goals?

- *Risk Appetite:* How much risk is the company comfortable taking on?

It's important to remember that risk assessment isn't a one-time, step-by-step process. Organizations may need to go back and forth between identifying risks, assessing them, and refining their priorities.

Here's the catch: there's no single "best" way to measure risk severity. The best approach depends on the specific risk and the data available. Similarly, the chosen assessment method will depend on the company's risk prioritization.

Assessment Approaches

When evaluating the severity of ESG risks within the context of their business strategy, management needs to make informed decisions about the assessment approach. This involves selecting each risk's most appropriate data, parameters, and assumptions (COSO, 2018).

A Toolbox of Techniques

There are several approaches to measuring ESG risk severity, both qualitative and quantitative:

- *Expert Input:* Leveraging the knowledge of experienced professionals to assess risk likelihood and impact.
- *Forecasting and Valuation Techniques:* Predicting potential financial consequences of ESG events using financial modelling or similar tools.
- *Scenario Analysis:* Exploring possible future situations and their ESG risk implications for the business.
- *ESG-Specific Tools:* Utilizing specialized software or frameworks for ESG risk assessment.

Table 10.4.3: "Measurement approaches" *Enterprise Risk Management: enterprise risk management to environmental, social and governance-related risks*, © 2018 Committee of Sponsoring Organizations of the Treadway Commission (COSO) and World Business Council for Sustainable Development (WBCSD). All rights reserved. Used with permission. (See Acceptable Use of COSO Materials [PDF] for permission details).

Approach	Description	Advantages and disadvantages
Expert input	Expert input refers to a forecasting method that relies on a panel of experts (e.g., Delphi approach) or interviews and discussions with subject-matter specialists.	• Relatively quick, limited analysis • Not always effective for ESG-related risks when relevant experts are not available to participate • May be appropriate for emerging risks where data is sparse • Allows criteria other than "likelihood" and "impact," such as velocity or resilience, to be included in the risk assessment discussion
Forecasting and valuation	Forecasting and valuation predicts the impact of a future event based on past and present data. Traditional ERM tools, such as statistical regression and Monte Carlo simulation, as well as tools that leverage big data and artificial intelligence, can support quantification of ESG-related risks.	• Requires forecasting skills and internal or external data • Requires large amounts of data and probabilistic modelling tools
Scenario analysis	Scenario analysis develops plausible pathways to describe a future state.	• Requires forecasting and research of future outcomes • Allows simulation of events or disruptions
ESG-specific tools	Tools and approaches are available in the Natural Capital Protocol Toolkit and Social & Human Capital Protocol Toolkit.	• Leverages ESG issue and geography-specific assessment methods • Varying degrees of quality and maturity among the available tools

Beyond this core set, additional tools can support a data-driven approach:

- *Competitor Analysis:* Comparing ESG practices and risks faced by competitors in the industry.
- *Stakeholder Assessments:* Understanding the perspectives of key stakeholders like investors, regulators, and communities regarding ESG risks.
- *Peer Benchmarking:* Measuring a company's ESG performance against industry leaders to identify areas for improvement.
- *Data-Driven Approaches with Technology:* Utilizing big data and advanced analytics to

assess ESG risks more comprehensively.

By selecting the right tools and data for each risk, businesses can gain a deeper understanding of how ESG issues might impact their strategies and objectives (COSO, 2018).

Strategies for Responding to Sustainability Risks

The COSO ERM Framework provides a structure for selecting appropriate responses to identified ESG risks. These responses fall into five main categories:

Figure 10.4.2: "Five Main Categories of ESG Risk Responses in the COSO ERM Framework"

Accept

This involves taking no action to change the risk's severity. It's suitable when the risk falls within the organization's risk appetite and is unlikely to worsen.

For instance, a manufacturer might accept potential human rights risks in its supply chain if they have low-risk suppliers and haven't faced public pressure on the issue. The cost of mitigation programs might outweigh the perceived risk. However, accepting a risk requires continuous monitoring of the underlying assumptions. If circumstances change, a different response might be necessary.

Avoid

This strategy aims to eliminate the risk entirely or at least reduce its likelihood of occurring. Certain ESG risks might have a zero-tolerance policy, prompting complete avoidance.

For example, an insurance company might refuse to reinsure businesses heavily reliant on thermal coal. Similarly, a service provider to governments might avoid working in countries with high-risk corruption.

Pursue

This strategy transforms risks into opportunities. Responding to ESG risks can unlock new business avenues.

The Business and Sustainable Development Commission estimates that achieving the UN's Sustainable Development Goals (SDGs) could generate over $12 trillion in business opportunities by 2030.

Reduce

This is the most common response when a risk's severity exceeds the risk appetite. Organizations aim to lessen the risk's impact through mitigation activities. This might involve:

- **Strategic Adjustments:** Developing a new strategy, goal, or target to address the risk.
- **Human Capital Investment:** Building a dedicated team or providing training to foster innovation with environmental benefits.
- **Process Improvement:** Establishing codes of conduct, certification programs, and audit processes to manage risks and enhance stakeholder transparency.
- **Systems Implementation:** Implementing management systems for ongoing monitoring of risks based on established standards.

Share

This involves transferring some or all of the risk to another party. Sharing can be achieved through insurance, outsourcing, or joint ventures.

Table 10.4.4: Examples of responding to risks through innovation " *Enterprise Risk Management: enterprise risk management to environmental, social and governance-related risks*, © 2018 Committee of Sponsoring Organizations of the Treadway Commission (COSO) and World Business Council for Sustainable Development (WBCSD). All rights reserved. Used with permission. (See Acceptable Use of COSO Materials [PDF] for permission details).

ESG-related risk	Responses	Value created, preserved or realized
Scarcity of raw materials or excessive waste	• Following a circular economy model, the Timberland apparel company and the tire manufacturer and distributor Omni United teamed up to produce a line of tires capable of being recycled into footwear outsoles once they reach end-of-life. • MUD Jeans identified an opportunity related to ownership for its products at end of life. Under a circular economy model, the company collects and recycles its products. • Pathway 21, which was developed beginning with a pilot project created by the United States Business Council for Sustainability Development, initiated the materials marketplace to facilitate company-to-company industrial reuse. Through the cloud-based platform, industrial waste streams are matched with new product and revenue opportunities, enabling a shift towards a circular, closed-loop economy.	• Increased availability of raw materials through reuse • Improved profitability through sourcing lower-cost inputs • Improved reputation regarding material use and waste
Animal welfare	• Procter & Gamble (P&G) identified a risk related to performing research on animals. In response, the company developed more than 50 alternatives and non-animal testing methods and has invested more than USD$410 million in finding alternatives and seeking regulator acceptance around the world. P&G scientists invented the first non-animal alternative to skin allergy tests.	• Improved its reputation with animal rights activists • Leadership in delivery of non-animal testing methods resulting in satisfied and loyal customers
Climate change	• An automobile company looks to reduce the greenhouse gas emissions of its products manufactures electric vehicles. • An energy company identifies pricing and availability risks related to conventional forms of energy and invests in renewable energy. • Microsoft, like a growing number of other companies, places a price on carbon for internal accounting purposes as part of its long-term risk management strategy. This enables the company to talk about carbon in the language of business and reward parts of the company that can demonstrate cost savings from lowering emissions.	• Offered new, in-demand products • Enabled the company to meet rising customer demands for renewable energy

Employee retention	• The hospitality industry has historically experienced low employee retention. Hyatt pursued this risk and now experiences an average tenure of more than 15 years for more than 14,000 housekeeping employees. The company offers a training program called "Change the Conversation," which is based on principles from the Stanford School of Design that emphasize listening. Employees are encouraged to find new, creative ways to solve problems and accomplish everyday tasks.	• Improved employee retention • Reduced hiring and retention costs • Enhanced efficiency and productivity from employee innovation
Changing customer profile	• Westpac, an Australian bank, identified the rapidly changing shifts in societal demographics as one of the four issues material to its business. In anticipating the future needs of aging customers, Westpac developed new planning investment and insurance proceeds to increase financial security, including: ◦ A product that allows customers to generate growth for retirement through their investment portfolio while preserving a minimum outcome at the end of an agreed term ◦ A contact center for customers aged 50 or older ◦ A life insurance product that provides customers with recommendations on life insurance tailored to their situation	• Developed new products and services • Improved customer service • Captured new customers and retained existing customers

In conclusion, effectively managing ESG risks requires a tailored approach. Businesses can leverage various assessment tools and choose from a range of response strategies outlined by the COSO ERM Framework (Accept, Avoid, Pursue, Reduce, Share). By selecting the right response based on risk severity and appetite, businesses can navigate the ESG landscape, mitigate potential threats, and even unlock new opportunities, contributing to a more sustainable future (COSO, 2018).

10.5 OPPORTUNITIES IN SUSTAINABLE RISK MANAGEMENT

Sustainable risk management allows companies to incorporate environmental, social, and governance (ESG) factors into their overall risk assessment and decision-making processes. This holistic approach helps identify potential risks and opportunities that may be overlooked in traditional risk management frameworks. By considering ESG factors, organizations can better anticipate and mitigate risks related to climate change, resource scarcity, social issues, and regulatory changes.

Enhanced Stakeholder Trust and Reputation

Implementing sustainable risk management practices demonstrates a company's commitment to responsible business practices. This can lead to increased stakeholder trust, including investors, customers, employees, and local communities. Organizations that effectively manage sustainability risks are often viewed favourably, potentially leading to improved reputation, customer loyalty, and investor confidence.

Competitive Advantage and Innovation

Sustainable risk management can drive innovation and create competitive advantages. By identifying and addressing sustainability-related risks early, companies can develop new products, services, and business models that are more resilient and aligned with evolving market demands. This proactive approach can help organizations stay ahead of regulatory changes and consumer preferences, positioning them as industry leaders.

Improved Decision-Making and Performance

Integrating sustainability considerations into risk management processes enables more informed decision-making. It provides a more comprehensive view of potential risks and opportunities, allowing organizations to make strategic choices that balance short-term goals with long-term sustainability objectives. This approach can lead to improved overall performance and resilience in the face of complex, interconnected global challenges.

Access to Capital and Investment Opportunities

As investors increasingly prioritize sustainability and ESG factors in their investment decisions, companies with robust, sustainable risk management practices may gain better access to capital. They may also be better positioned to take advantage of emerging investment opportunities in sustainable technologies, products, and markets.

Regulatory Compliance

Sustainable risk management helps organizations stay ahead of evolving regulations related to environmental and social issues. By proactively addressing sustainability risks, companies can reduce compliance costs, avoid penalties, and be better prepared for future regulatory changes. This forward-looking approach contributes to the long-term viability and resilience of the organization.

Collaboration and Partnerships

Sustainable risk management often requires collaboration across different departments within an organization, as well as with external stakeholders. This presents opportunities for cross-functional learning, knowledge sharing, and the development of innovative solutions to complex sustainability challenges. It also encourages partnerships with suppliers, customers, and other stakeholders to address shared risks and create mutual value.

By exploring these opportunities in sustainable risk management, postgraduate students can gain valuable insights into how organizations can create long-term value while addressing critical environmental and social challenges. This knowledge will be increasingly important as businesses navigate the complex landscape of sustainability risks and opportunities in the coming years (Deloitte, 2019).

10.6 CHAPTER SUMMARY

Summary

Chapter 10, "Risk Management from a Sustainability Perspective," emphasizes the importance of integrating sustainability into risk management to address complex challenges such as climate change, resource scarcity, and shifting societal expectations. This approach, known as Environmental, Social, and Governance (ESG) risk management, recognizes the interconnected nature of these factors and their long-term impacts on an organization's value creation and protection. Traditional risk management methods, which focus on short-term and easily quantifiable risks, are insufficient for addressing the broader, more complex sustainability challenges that organizations face today. Sustainable risk management requires a holistic approach, incorporating new tools, metrics, and frameworks to assess and mitigate risks while also identifying opportunities for innovation and value creation.

The chapter outlines various types of sustainability risks, including environmental, social, and governance risks, and their potential cascading effects on an organization's operations and the broader economy. Effective management of these risks involves integrating ESG factors into traditional risk management frameworks, enhancing transparency, and aligning business strategies with sustainability goals. Additionally, the chapter discusses various frameworks and techniques for assessing and responding to ESG-related risks, such as the UN Sustainable Development Goals (SDGs), the Task Force on Climate-related Financial Disclosures (TCFD) recommendations, and the Global Reporting Initiative (GRI) Standards. Organizations can mitigate potential threats by adopting these frameworks and proactive strategies, enhance stakeholder trust, and gain a competitive advantage in a rapidly changing global landscape.

OpenAI. (2024, July 3). *ChatGPT*. [Large language model]. https://chat.openai.com/chat

Prompt: *Please take the chapter content in this document attached and summarize the key concepts into no more than two paragraphs. Reviewed by authors.*

Key Terms

- **Environmental risks** stem from an organization's impact on and dependence on the natural environment.
- **Governance risks** are how an organization is managed, overseen, and held accountable.
- **GRI (Global Reporting Initiative)** is an independent, international organization that helps businesses and other organizations take responsibility for their impacts by providing them with a global common language to communicate those impacts.
- **Social risks** relate to an organization's impact on and relationship with society, including its workforce, customers, and communities.
- **Sustainability risks** are environmental, social, or governance events or conditions that, if they occur, could cause a negative material impact on an organization's value, operations, and long-term viability.
- **Sustainable risk management** allows companies to incorporate environmental, social, and governance (ESG) factors into their overall risk assessment and decision-making processes.
- **TCFD**, established by the Financial Stability Board (FSB – an international body that monitors and makes recommendations about the global financial system), provides recommendations for more effective climate-related disclosures. TCFD framework focuses on governance, strategy, risk management, and metrics and targets related to climate risks and opportunities.

REFERENCES

Agarwal, K. (2023, June 19). The Monte Carlo simulation: Understanding the basics. *Investopedia*. https://www.investopedia.com/articles/investing/112514/monte-carlo-simulation-basics.asp.

Airmic. (2016). Scenario analysis – A practical system for Airmic members: Guide 2016. *Oric International*. https://www.airmic.com/sites/default/files/technical-documents/Scenario-Analysis.pdf

Al Kazimi, A. & Mackenzie, C. A. (2016, April 29). The economic costs of natural disasters, terrorist attacks, and other calamities: An analysis of economic models that quantify the losses caused by disruptions. IEEE systems and information engineering design symposium (SIEDS). https://www.imse.iastate.edu/files/2016/04/Al-Kazimi-and-MacKenzie-The-Economic-Costs-of-Natural-Disasters-Terrorist-Attacks-and-Other-Calamities.pdf

Analyst Prep. (2023, January 10). Machine learning and AI for risk management. Analystprep.com. https://analystprep.com/study-notes/frm/machine-learning-and-ai-for-risk-management/.

Baker, K. (2024, May 14). 12 most common types of cyberattacks. *CrowdStrike.* https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/.

Barlow, J. (2016, April 14). The role of the board in risk management. *The Board Effect*. https://www.boardeffect.com/blog/role-of-the-board-in-risk-management/.

Borrelli, R. (2015). *Risk assessment*. Pressbooks. https://uidaho.pressbooks.pub/riskassessment/

Boyles, M. (2022, August 2). 7 ways climate change is affecting businesses. *Harvard Business Scholl Online*. https://online.hbs.edu/blog/post/climate-change-affecting-businesses.

Canadian Centre for Cyber Security (2023, February 8). The cyber threat from supply chains. *Government of Canada.* https://www.cyber.gc.ca/en/guidance/cyber-threat-supply-chains.

Canadian Centre for Cyber Security. (n.d.). Glossary – Canadian Centre for Cyber Security. *Government of Canada*. https://www.cyber.gc.ca/en/glossary.

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *COSO enterprise risk management-Integrating with strategy and performance.*

COSO (2013, May). Internal control – Integrated framework: Executive summary. https://www.coso.org/_files/ugd/3059fc_1df7d5dd38074006bce8fdf621a942cf.pdf

COSO. (2018, October). *Enterprise risk management: Applying ERM to ESG related risks.* https://docs.wbcsd.org/2018/10/COSO_WBCSD_ESGERM_Guidance.pdf.

Deloitte. (2017). Blockchain risk management: Risk functions need to play an active role in shaping blockchain strategy. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-blockchain-risk-management.pdf

Deloitte (2019). *Sustainability risk management*. www2.deloitte.com/content/dam/Deloitte/my/Documents/risk/my-risk-sdg12-sustainability-risk-management.pdf.

Edwards, D. J. (2023, September 22). Blockchain and risk management: A match made in heaven? *LinkedIn.com*. https://www.linkedin.com/pulse/blockchain-risk-management-match-made-heaven-dr-jeffrey/.

Edwards, D. J. (2024, May 30). Leveraging Predictive Analytics for Risk Management. *LinkedIn*. https://www.linkedin.com/pulse/leveraging-predictive-analytics-risk-management-dr-jeffrey.

Elliott, M. W. (Ed.). (2018). *Risk management principles and practices*. The Institutes.

Elliott, M. W. (Ed.). (2012). *Risk financing* (6th Edition). The Institutes.

Elliott, M. W. (Ed.). (2017). *Risk assessment and treatment* (2nd Edition). The Institutes.

Elliott, M. W. (Ed.). (2018). *Risk management principles and practices* (3rd Edition). American Institute for Chartered Property Casualty Underwriters.

ESG Risk Guard. (n.d.). Environmental, social, and governance (ESG) strategy and risk management consulting. https://esgriskguard.com/.

Federation of European Risk Management Association. (2021).*People, planet, & performance – The contribution of ERM to sustainability.* https://www.ferma.eu/app/uploads/2021/03/Ferma-sustainability_2021_final.pdf.

Financial Reporting Council. (2014, September). Guidance on risk management, Internal control and related financial and business reporting. https://media.frc.org.uk/documents/Guidance_on_Risk_Management_Internal_Control_and_Related_Financial_and_Business_Reporting_September.pdf

Global Reporting Initiative. (n.d.). Global sustainability standards board. https://www.globalreporting.org/standards/global-sustainability-standards-board/

Gordon, R. (2023, July 14). Ethical issues in supply chain management and procurement. *American Public University.* https://www.apu.apus.edu/area-of-study/business-and-management/resources/ethical-issues-in-supply-chain-management-and-procurement/.

Hall, H. (2024, May 30). How to perform a SWOT analysis. *Project Risk Coach*. https://projectriskcoach.com/how-to-perform-a-swot-analysis/.

Halton, C. (2024, July 19). Empirical probability: What it is, how it works, FAQ. *Investopedia*. https://www.investopedia.com/terms/e/empiricalprobability.asp.

Hayes, A. (2023, December 14). Scenario analysis: How it works and examples. *Investopedia.* https://www.investopedia.com/terms/s/scenario_analysis.asp.

Hillson, D. & Hulett, D. T. (2004). Assessing risk probability: alternative approaches. Paper presented at PMI® Global Congress 2004—EMEA, Prague, Czech Republic. Newtown Square, PA: Project Management Institute. https://www.pmi.org/learning/library/assessing-risk-probability-impact-alternative-approaches-8444

Hopkin, P. & Thompson, C. (2022). *Fundamentals of risk management* (6th ed). Kogan Page Publishers.

Horvath, I. (2024, January 16). Roles and responsibilities of a chief risk officer. *Invensis*. https://www.invensislearning.com/blog/chief-risk-officer-roles-responsibilities/.

Howell, M. (2024, May 29). Top-down or bottom-up risk management: Why not both? *Protecht*. https://www.protechtgroup.com/en-au/blog/top-down-or-bottom-up-risk-management-why-not-both.

IBM. (2024a). Types of cyberthreats. https://www.ibm.com/think/topics/cyberthreats-types.

IBM (2024b). What is cyber risk management? https://www.ibm.com/topics/cyber-risk-management.

Inbound Logistics. (October, 2023). Supply chain risk management: Definition, examples, and strategies. https://www.inboundlogistics.com/articles/supply-chain-risk-management/.

The Institute of Internal Auditors. (n.d.). Internal auditing: Assurance, insight, and objectivity. https://www.theiia.org/globalassets/documents/about-us/what-is-internal-audit/ia-assurance-insight-and-objectivity.pdf

Institute of Risk Management – IRM. (2002). A risk management standard. https://www.theirm.org/media/4709/arms_2002_irm.pdf

Institute of Risk Management. (n.d.). From the cube to the rainbow double helix: a risk practitioner's guide to the COSO ERM frameworks. https://www.theirm.org/news/from-the-cube-to-the-rainbow-double-helix-a-risk-practitioner-s-guide-to-the-coso-erm-frameworks/

International Organization for Standardization. (2018). ISO 31000:2018 Risk management- Guidelines. https://www.iso.org/standard/65694.html

International Organization for Standardization. (2022). ISO 31073:2022 Risk management- Vocabulary (1 Ed).

The Institute of Risk Management. (2002). *IRM's risk management standard*. https://www.theirm.org/what-we-do/what-is-enterprise-risk-management/irms-risk-management-standard/.

Kaya, A. (2024, March 1). How are geopolitical risks affecting the world economy? *Economics Observatory*. https://www.economicsobservatory.com/how-are-geopolitical-risks-affecting-the-world-economy.

Kole, J. (2023, June 13). Partners in Project Green: The impacts of climate change on business. *Ontario Chamber of Commerce*. https://occ.ca/partners-in-project-green-the-impacts-of-climate-change-on-business/.

Kost, E. (2024, May 03). The biggest security risks in your supply chain in 2024. *UpGuard*. https://www.upguard.com/blog/biggest-supply-chain-security-risks.

Krishnamoorthy, G. (n.d.). The role of the board when managing risk. *Corporate Governance Institute*. https://www.thecorporategovernanceinstitute.com/insights/guides/the-role-of-the-board-when-managing-risk.

Leland, A. (2023, May 23). Fundamentals of the COSO Framework: Building blocks for integrated internal controls. *AuditBoard*. https://www.auditboard.com/blog/coso-framework-fundamentals/.

Leslie, J. (2022, March 10). How climate change is disrupting the global supply chain. *Yale Environment 360*. https://e360.yale.edu/features/how-climate-change-is-disrupting-the-global-supply-chain.

Lobdell, K. (2023, December 13). *Supply chain risk management strategies*. Thomson Reuters.

Marotta, D. (n.d.). Supply chain risk management: 10 strategies for success. *Hitachi Solutions.* https://global.hitachi-solutions.com/blog/supply-chain-risk-management/.

Mason C. & Oxnevad I. (2024, April 16). 10 geopolitical risks your organization needs to prepare for this year. *Risk Management.* https://www.rmmagazine.com/articles/article/2024/04/16/10-geopolitical-risks-your-organization-needs-to-prepare-for-this-year.

Mbiam, S. (2023, February 24). 5 strategies to manage supply chain risks. *Linkedin.com.* https://www.linkedin.com/pulse/5-strategies-manage-supply-chain-risks-sunny-mbiam-msc-mba-mcips/.

McGrath A. & Jonker, A. (2023, December 2). What is SCRM? *IBM*. https://www.ibm.com/topics/supply-chain-risk-management.

Muscad, O. (2024, January 9). What is HAZOP? A comprehensive guide to Hazard and Operability Analysis. *DATAMYTE*. https://datamyte.com/blog/hazard-and-operability-analysis-hazop/.

Navarro, A. (2024, May 20). The role of internal audit in risk management. *LinkedIn*. https://www.linkedin.com/pulse/role-internal-audit-risk-management-arturo-navarro-cpa-gwb8c

Oktaviani, O., Susetyo, B. Purwoko Kusumo Bintoro, B. (2021, August). Risk management model using cause and effect analysis in industrial building project. *International Journal of Research and Review*, *8*(8), 227-235. https://doi.org/10.52403/ijrr.20210832.

Onischuk, P. M. (2023, May 25). From the examiner's desk: Customer information risk assessments: Moving toward enterprise-wide assessments of business risk. *Federal Deposit Insurance Corporation (FDIC)*. https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin09/siwinter2009-article03.html.

PWC. (2011). In times of uncertainty- an insight into effective Risk Reporting in a changing market. https://www.pwc.com.au/industry/banking-capital-markets/assets/insight-into-effective-risk-reporting-sep11.pdf

Reaiche, C., Papavasiliou, S., & Anglani, F. (2022). *Risk assessment and quality project management*. James Cook University – PressBooks. Retrieved from https://jcu.pressbooks.pub/pmriskquality.

Resolver. (2023, August 28). Embracing machine learning in risk management. *Resolver.com*. https://www.resolver.com/blog/machine-learning-in-risk-management/.

Risk Management Team. (2020, June 29). HAZOP Analysis: An Intuitive Risk Assessment Tool. *ComplianceBridge*. https://compliancebridge.com/hazop-analysis/.

TCFD. (n.d.) Task Force on climate-related financial disclosures. https://www.fsb-tcfd.org/

S&P Global. (n.d.). Top geopolitical risks of 2024. https://www.spglobal.com/en/research-insights/market-insights/geopolitical-risk.

SAP. (n.d.). What is Supply Chain Management (SCM). https://www.sap.com/canada/products/scm/what-is-supply-chain-management.html

Schnellbächer, W., Nee, C., Oleynikova, Y., & Jha, C. (2023, September 25). Two keys to success in supplier risk management. *BCG*. https://www.bcg.com/publications/2023/how-to-mitigate-supply-chain-risk.

Sedex (2024). What does "ethically sourced" mean? https://www.sedex.com/blog/what-does-ethically-sourced-mean/.

Segun, W. (2021). ESG environmental risks overview. *Auditboard*. https://www.auditboard.com/blog/environmental-risks-esg/.

Segun, W. (2023, October 28). ESG risks: Why ESG risks should be on your radar. *Auditboard*. https://www.auditboard.com/blog/esg-risks/.

Setiawan, A., Wibowo, A., Hartanto Susilo, A. (2017, August). Risk analysis on the development of a business continuity plan. *4th International Conference on Computer Applications and Information Processing Technology (CAIPT)*. http://dx.doi.org/10.1109/CAIPT.2017.8320736

SmartMakers. (2023, December 22). How IoT improves logistics and supply chain risk management. https://smartmakers.io/en/iot-verbessert-das-risikomanagement-in-logistik-und-supply-chain/

Stammers, R. (2024, May 29). Using Monte Carlo Analysis to estimate risk. *Investopedia*. https://www.investopedia.com/articles/financial-theory/08/monte-carlo-multivariate-model.asp.

Strawser, B. (2023). Navigating the rise of chief risk officers in organizations. *BryghtPath*. https://bryghtpath.com/the-rise-of-chief-risk-officers-in-organizations/.

Tuovila, A. (2024, June 24). Internal audit: What it is, different types, and the 5 Cs. *Investopedia*. https://www.investopedia.com/terms/i/internalaudit.asp

UK Government. (2023, 4 May). The orange book – Management of risk. https://www.gov.uk/government/publications/orange-book.

UN Department of Economic & Social Affairs. (n.d.). The 17 goals – Sustainable development. *United Nations*. https://sdgs.un.org/goals.

USAFacts Team (2023, March 28). Are major natural disasters are increasing?*USA Facts*. https://usafacts.org/articles/are-the-number-of-major-natural-disasters-increasing/.

Valleskey, B. (2024, June 29). Automation in risk management: A complete overview. *Inscribe*. https://www.inscribe.ai/financial-risk-management/automation-in-risk-management.

Vicente, V. (2023, April 27). Supply chain risk management: Best practices. *Auditboard*. https://www.auditboard.com/blog/supply-chain-risk-management-best-practices/.

Waller Lansden Dortch & Davis (2005). The board's role in risk management. *Law & Governance*, *9*(9), 61-63. https://www.longwoods.com/product/download/code/17807.

World Economic Forum. (2023, January). *The global risk report 2023*. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf.

Wrobel, M. (2023, June 14). The ABC of risk management automation. *Invgate*. https://blog.invgate.com/risk-management-automation.

VERSION HISTORY

This page provides a record of edits and changes made to this book since its initial publication. Whenever edits or updates are made in the text, we provide a record and description of those changes here. If the change is minor, the version number increases by 0.1. If the edits involve a number of changes, the version number increases to the next full number.

The files posted alongside this book always reflect the most recent version.

Version	Date	Change	Affected Web Page
1.0	August 2024	First publication	N/A