12 INFORMATION & RISK MANAGEMENT

CHAPTER IN *UNDERSTANDING BUSINESS*

KEY TAKEAWAYS:

- **Business information** refers to collective data related to a company and its operations, including statistical information, raw analytical data, customer feedback, and sales numbers.
- **Big data** refers to datasets that are so large and complex that traditional data-processing methods cannot handle them. The defining characteristics of big data are volume, velocity, variety, veracity, and value (the 5Vs).
- **Data mining** involves extracting valuable patterns and relationships from large datasets. Businesses use techniques like clustering, classification, and predictive modelling to derive actionable insights.
- **Data security** is paramount to protect sensitive information from breaches, unauthorized access, and cyberattacks.
- Effective **information sharing** enhances collaboration and decision-making within and between organizations.
- **Visualization** converts data into graphical representations, making complex datasets easier to understand and interpret. Popular tools include Tableau, Power BI, and Google Charts.
- **Information management** encompasses the collection, storage, organization, and distribution of information to optimize business operations and decision-making.
- **Risk management** is the structured process of identifying potential threats, evaluating their likelihood and impact, and developing strategies to minimize or eliminate their adverse effects.

LEARNING OBJECTIVES:

LO1: Explain how analyzing Big Data can help businesses.

LO2: Express some of the major threats to data security a business may experience.

LO3: Clarify what is meant by "information sharing" and the challenges this may present.

LO4: Define information mining and visualization.

LO5: Explore the key elements and trends in information management and their impact on business operations.

LO6: Discuss ways to manage common business risks within one or more sectors.

LO7: Distinguish between real risk and perceived risk by providing an example of each.

LO8: Illustrate the major factors that influence an organization's risk tolerance.

LO9: Show how risk impacts business and outline the five steps of risk management.

LO10: Demonstrate the utility of risk management across different sectors.

LO11: List the most common risk response strategies and provide examples for each.

LO12: Describe how Artificial Intelligence is being used in business to enhance information and risk management.

LO13: Assess the principles and guidelines of ISO 31000 and its role in standardizing risk management practices.

- There are a number of risk management standards designed to consolidate best practice principles and streamline and improve risk management implementations for businesses. For example, **ISO** refers to the International Organization for Standardization; the 31000 part refers to a family of **standards** for risk management. As well as being an umbrella term for many different standards, **ISO 31000** also refers to a singular standard, specifically known as ISO 31000:2018.

KEY TAKEAWAYS:

- **Business risk** refers to the potential for a company to experience financial losses or other challenges that could impact its ability to achieve its objectives. These risks arise from uncertainties in the internal and external environment in which the business operates.

- **Real risks** are backed by data, evidence, or historical trends. They are measurable and often require proactive mitigation.

- **Perceived risks** are based on feelings, fears, or assumptions and may lack concrete evidence. They often result from misinformation, cognitive biases, or heightened awareness.

- **Risk tolerance** in a business context refers to the degree of uncertainty and potential loss an organization is willing to accept to achieve its objectives. It reflects the company's capacity and willingness to take on risks as part of its strategy and decision-making processes.

- **Personal risk tolerance** refers to an individual's ability or willingness to accept uncertainty and potential loss in pursuit of a goal. It plays a critical role in decision-making, particularly in areas like investments, career choices, and lifestyle decisions.

- In the **financial sector**, risk management is crucial for banks, insurance companies, and investment firms. These institutions face a wide range of risks, including credit risk, market risk, operational risk, and liquidity risk. Effective risk management practices in the financial industry help ensure stability and prevent financial crises.

- The **healthcare industry** relies heavily on risk management to ensure patient safety and quality of care. Health care organizations face risks related to medical errors, patient privacy breaches, and regulatory compliance. By implementing robust risk management strategies, providers can identify and mitigate potential risks, leading to improved patient outcomes and reduced legal liabilities.

- **Project risk management** involves dealing with uncertainties and potential risks that can significantly impact project success. By incorporating risk management into project planning and execution, project managers can identify potential obstacles, allocate resources effectively, and implement contingency plans to minimize project delays and cost overruns.

- **Information risk management** is defined as the policies, procedures, and technology an organization adopts to reduce the threats, vulnerabilities, and consequences that could arise if data is not protected.

- **Supply chain management** is yet another area where effective risk management is critical. Supply chains are vulnerable to various risks, such as disruptions in logistics, supplier failures, and natural disasters. By implementing risk management strategies, organizations can identify potential vulnerabilities, establish alternative supply sources, and develop contingency plans to minimize the impact of supply chain disruptions.

- **Risk response strategy**. The choice of risk response for organizations depends on the severity of the risk, cost-benefit analysis, organizational goals, and risk appetite. Risk response strategies include: avoidance, mitigation, transfer, acceptance, exploitation, and enhancement.

- **Artificial Intelligence (AI)** is revolutionizing the way businesses manage information and mitigate risks. AI-powered systems provide businesses with the ability to process vast amounts of data in real time, identify risks before they escalate, and support informed decision-making. AI enhances information management by automating data collection, organizing unstructured data, and providing predictive insights that improve business operations. From financial institutions monitoring fraud to supply chain managers predicting disruptions, AI is becoming an integral tool in modern business environments.

Types of Risk
Operational risk - arises from internal processes, people, and systems.
Financial risk - is related to financial operations and transactions.
Strategic risk - stems from business strategies and industry changes.
Compliance risk - is due to legal and regulatory requirements.
Reputational risk - impacts public perception and brand reputation.
Market risk - is a result of market dynamics like price and demand fluctuations.
Credit risk - due to potential default on financial obligations.
Technology risks - include cybersecurity threats and system failures.

NOTES: