

# **A Notion of Enterprise Risk Management**

*This page intentionally left blank*

# **A Notion of Enterprise Risk Management: Enhancing Strategies and Wellbeing Programs**

BY

**SOUMI MAJUMDER**

*Future Institute of Engineering and Management, India*

AND

**NILANJAN DEY**

*Techno International New Town, India*



United Kingdom – North America – Japan – India – Malaysia – China

Emerald Publishing Limited  
Emerald Publishing, Floor 5, Northspring, 21-23 Wellington Street, Leeds LS1 4DL.

First edition 2024

Copyright © 2024 Soumi Majumder and Nilanjan Dey.  
Published under exclusive licence by Emerald Publishing Limited.

**Reprints and permissions service**

Contact: [www.copyright.com](http://www.copyright.com)

No part of this book may be reproduced, stored in a retrieval system, transmitted in any form or by any means electronic, mechanical, photocopying, recording or otherwise without either the prior written permission of the publisher or a licence permitting restricted copying issued in the UK by The Copyright Licensing Agency and in the USA by The Copyright Clearance Center. Any opinions expressed in the chapters are those of the authors. Whilst Emerald makes every effort to ensure the quality and accuracy of its content, Emerald makes no representation implied or otherwise, as to the chapters' suitability and application and disclaims any warranties, express or implied, to their use.

**British Library Cataloguing in Publication Data**

A catalogue record for this book is available from the British Library

ISBN: 978-1-83797-736-9 (Print)

ISBN: 978-1-83797-735-2 (Online)

ISBN: 978-1-83797-737-6 (Epub)



INVESTOR IN PEOPLE

# Contents

About the Authors	<i>vii</i>
Preface	<i>ix</i>
<b>Chapter 1 Enterprise Risk Management</b>	<b>1</b>
1.1. Introduction	1
1.2. Components/Elements of the ERM Process	3
1.3. Types of Enterprise Risks	6
1.4. An Effective Enterprise Risk Management System	8
1.5. Risk Categories	11
1.6. Conclusions	14
<b>Chapter 2 Enterprise Risk Management Life Cycle</b>	<b>17</b>
2.1. Introduction	17
2.2. Risk Management Lifecycle	18
2.3. Benefits of the Enterprise Risk Management Life Cycle	20
2.4. Conclusions	22
<b>Chapter 3 Risk Management Procedures</b>	<b>25</b>
3.1. Introduction	25
3.2. Risk Management Procedures	26
3.3. Examples of ERM and Case Studies by Industry	35
3.4. Conclusions	38
<b>Chapter 4 Risk Management Tools and Practices</b>	<b>41</b>
4.1. Introduction	41
4.2. Risk Management Tools and Techniques	42
4.3. Risk Mitigation Techniques	49
4.4. Risk Impact Analysis	50
4.5. Conclusions	54

<b>Chapter 5 Risk-Enabled Performance Management</b>	<b>57</b>
5.1. Introduction	57
5.2. Elements of EPM	62
5.3. EPM Framework	64
5.4. Modern EPM Methods	65
5.5. Integrating Risk and Performance Management	68
5.6. Steps to Manage Risks and Drive Performance	72
5.7. Aligning Risk with Performance Management Cycle	73
5.8. The Key to the Future Is Linking Risk and Performance	74
5.9. Best EPM Software	75
5.10. Conclusions	77
<b>Chapter 6 Industry 4.0 Challenges and Risks</b>	<b>81</b>
6.1. Introduction	81
6.2. Barriers to Digital Transformation	82
6.3. AI-Empowered Risk Management	87
6.4. Risk Management and Big Data	90
6.5. Capital Investment and Associated Risk	98
6.6. Conclusion	104
<b>Chapter 7 Conclusions</b>	<b>109</b>

## About the Authors

**Soumi Majumder** is a research scholar in the Department of Business and Accounting at Lincoln University College, Malaysia. She is an assistant professor at the Future Business School, Future Institute of Engineering and Management, Kolkata, India. Previously, she was associated with Sister Nivedita University, Techno India College of Technology, NSHM College of Management and Technology, J D Birla Institute of Science and Commerce, West Bengal State Labor Institute, Siliguri, DAITM and many more B Schools. She has 8 years of experience in academia and 2 years of industrial experience. She has 4 authored books, 2 edited books and more than 22 research papers in national and international conferences and journals in the areas of quality work-life, decent work-life, work-life balance, stress management, employee engagement, job satisfaction, leadership, training, learning, knowledge management, people management, safety management, entrepreneurship, etc. She has 3 copyrights from the Government of India for her research work. She is the reviewer for various national and international journals. Furthermore, she is a member of the AIMA, IS, SDIWC and NIPM.

**Nilanjan Dey** is an Associate Professor, Department of Computer Science and Engineering, Techno International New Town, Kolkata, India. He is a visiting fellow at the University of Reading, UK. He was an honorary visiting scientist at Global Biomedical Technologies, Inc., CA, USA (2012-2015). He was awarded his PhD from Jadavpur University in 2015. He has authored/edited more than 70 books with Elsevier, CRC Press and Springer and has published more than 300 papers. He is the Editor-in-Chief of International Journal of Ambient Computing and Intelligence, IGI Global, Associated Editor of IEEE Access and International Journal of Information Technology, Springer. He is the Series Co-Editor of Springer Tracts in Nature-Inspired Computing, Springer, Series Co-Editor of Advances in Ubiquitous Sensing Applications for Healthcare, Elsevier, Series Editor of Computational Intelligence in Engineering Problem Solving and Intelligent Signal Processing and Data Analysis, CRC. His main research interests include medical imaging, machine learning, computer-aided diagnosis, and data mining. He is a Fellow of IETE and Senior Member of IEEE.

*This page intentionally left blank*

# Preface

In any business organisation, risk management is an integral part of strategic management. It is embedded through the ongoing and continuous activities of business. Enterprise risk management is the methodology of identifying and effectively addressing potential events in an enterprise. It represents the risk of accomplishing strategic objectives and opportunities for gaining a competitive advantage in the market. The fundamental concept of enterprise risk management is to assess the significant risks of businesses and the implementation of suitable risk responses. The element risk responses refer to (i) the acceptance or tolerance probability of a risk in business, (ii) the termination or avoidance of risk factors, (iii) the transfer of risk and sharing risk through insurance, (iv) a joint venture and arrangements, (v) risk prevention mechanisms, and (vi) internal control procedures for mitigating or reducing risks. Other enterprise risk management concepts include risk philosophy and strategy, risk culture, and appetite. In business organisations, these are all expressions of attitudes towards risk. It talks about the amount of risk that businesses can willingly take or adapt. In any business, there are a few management responsibilities; architecture and infrastructure of risks; protocols for risk management; documentation of procedures for risk management; training, monitoring, assessing, and reporting on risk management; and many other activities.

In this book, **Chapter 1** is the introduction to enterprise risk management, which includes components/elements of the ERM process, types of enterprise risks, effective enterprise risk management system, and risk categories. **Chapter 2** covers the risk management life cycle and the benefits of enterprise risk management life cycle. Risk management procedures and enterprise risk management examples and case studies by industry are discussed in **Chapter 3**. **Chapter 4** depicts the picture of risk managing tools and practices, which consists of risk management tools and techniques, risk mitigation techniques, and risk impact analysis. The book has also been enlightened by **Chapter 5**, titled Risk-Enabled Performance Management System, which focuses on elements of enterprise performance management, enterprise performance management framework, modern enterprise performance management methods, integrating risk and performance management, steps to manage risks and drive performance, and aligning risk with performance management cycle. The key to the future is linking risk and performance and Best Enterprise Performance Management Software. **Chapter 6** provides a view of Industry 4.0 challenges and risks, including barriers to digital transformation, AI-empowered risk management, risk

management, and big data capital investment and associated risk. **Chapter 7** presents the conclusions of the book.

This book's main objective is to increase organisational efficiency by emphasising the best modern methods for managing risk in a corporate environment. The intended audience of this book includes academics, researchers, research scholars, and industry people who stand to benefit significantly from its contents. This audience includes business management students with various specialities, hospital management, media science, hospitality management, industrial relations, and other courses related to business.

Soumi Majumder  
Nilanjan Dey

# Chapter 1

## Enterprise Risk Management

### 1.1. Introduction

In any business organisation, risk management is an integral part of strategic management. It is embedded through the ongoing and continuous activities of business. Enterprise risk management is the methodology of identifying and effectively addressing potential events in an enterprise. It represents the risk of accomplishing strategic objectives and opportunities for gaining a competitive advantage in the market. The fundamental concept of enterprise risk management is to assess the significant risks of businesses and the implementation of suitable risk responses. The element risk responses refer to (i) the acceptance or tolerance probability of a risk in business, (ii) the termination or avoidance of risk factors, (iii) the transfer of risk and sharing risk through insurance, (iv) a joint venture and arrangements, (v) risk prevention mechanisms, and (vi) internal control procedures for mitigating or reducing risks. Other enterprise risk management concepts include risk philosophy and strategy, risk culture, and appetite. In business organisations, these are all expressions of attitudes towards risk (Bromiley et al., 2015). It talks about the amount of risk that businesses can willingly take or adapt. In any business, there are a few management responsibilities; architecture and infrastructure of risks; protocols for risk management; documentation of procedures for risk management; training, monitoring, assessing, and reporting on risk management; and many other activities. Certain risk management standards exist for different categories of businesses. Several standards have been established worldwide to implement risk management in organisations effectively, efficiently, and systematically. These standards are based on certain common views of frameworks, practices, and procedures and are recognised by international standards bodies. Risk management standards are updated and regularly supplemented. These different standards have created different motivations and have made a technical focus of developers (Hoyt & Liebenberg, 2011). Standards are generally voluntary in nature. These standards are regulated by

## 2 *A Notion of Enterprise Risk Management*

contracts. Different standards are based on the motivations and technological focus of their designers, which provide a suitable basis for different organisations and situations. Standards are usually optional, although they may be subject to regulatory or contractual requirements. A list of important standards that have been used is provided below.

Risk Management Principles and Guidelines – ISO 31000 2018

- i) A Risk Management Standard – AIRMIC 2002
- ii) Risk Assessment Techniques – ISO/IEC 31010:2009
- iii) Enterprise Risk Management with an Integrated Framework – COSO 2004 and 2017

There are different approaches to risk management in enterprises. As a part of day-to-day jobs, business leaders have approached and managed risks for decades. Enterprise risk management also considers how to eliminate the probability of risks that may affect business. Traditionally, the responsibility of business unit leaders consists of managing risks in their daily work. A few examples can be given at this juncture; for example, the chief technology officer (CTO) of any organisation is very much responsible for risk management, which is related to the information technology operation of the business. Treasurers are responsible for managing risks in the area of cash flow and financing. To reduce production and distribution risks, chief operating officers are responsible ([Chapman, 2011](#); [Razali & Tahir, 2011](#)). The Chief Marketing Officers are responsible for increasing sales and customer relationships. In the key responsibility areas of each of these functional leaders, they are bound to take charge of managing risks. The traditional approach to risk management is usually referred to as silo or stovepipe risk management. [Fig. 1.1](#) shows the functional areas and their risk management by each silo leader. This figure indicates that risk is associated with different operating areas of an enterprise, such as sales and customer services, manufacturing and distribution, finance and cash flow, human resources, and risks relating to IT or legal and regulatory compliance.

- I. There are a few important components on which enterprises need to focus. Some action must be taken based on that area.
  - i) It is well established that Enterprise Risk Management (ERM) requires support from top management and the board.
  - ii) Employees should be engaged in risk management with a board based on managers.
  - iii) The process starts with a few key risk factors and builds ERM incrementally.
  - iv) There is a need to use existing knowledge, skills, and other resources. Internal audits and compliance data are also used.
  - v) The Enterprise Resource Planning is embedded into the fabric of the business organisation.
  - vi) Management should take a holistic and portfolio view of risk management.

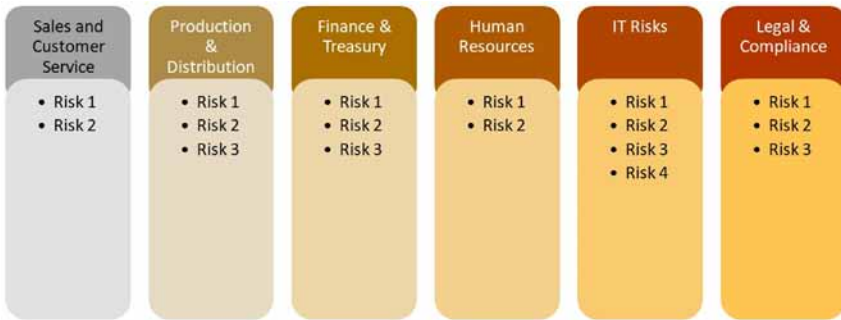


Fig. 1.1. Enterprise Risk Management.

## II. Action to be avoided for Enterprise Risk Management

- i) Enterprise risk management is a vital process; it should not be treated as a project.
- ii) The process of ERM must be forward-looking and strategy-oriented so that it is not bogged down in detail or history.
- iii) Do not rely only on a few key staff members. ERM is needed in everybody's job.
- iv) The impact of risks should be calculated by business leaders on other parts of the business. Not to take a silo or stove-pipe approach towards risks.
- v) The key risk factors need to be identified, and mitigation plans need to be developed.
- vi) Not to obsess too much on the categorisation of risks.
- vii) No one should assume that the risk register is complete and that there is always an unknown fact hidden.

## 1.2. Components/Elements of the ERM Process

When we focus on enterprise risk assessment, different elements exist. As part of day-to-day tasks, in any business organisation, leaders manage risks. They embrace enterprise risk management (Beasley et al., 2005). They always think differently about reducing risk factors in business and try to suggest solutions. The elements of the enterprise risk management process are described below (Fig. 1.2).

### 1.2.1. Code of Conduct in an Organisation

Identifying the risk attitude of an organisation's core values and code of conduct has played a major and vital role. In the face of dynamic trends, it is essential to know when the business should take calculated risks and when to make decisions to go the extra mile. A healthy and safe work culture sets work standards for employees, and it also determines the ability to deal with risks. The managerial



Fig. 1.2. Components/Elements of the ERM Process.

hierarchy is responsible for setting up a code of conduct. The skills, knowledge, and talent of leaders will ensure that no risk factor is overlooked in the area of completion of a project.

### ***1.2.2. Setting Goals and Objectives***

Every organisation has a purpose to serve. This purpose includes their mission and vision statements. Every member of the organisation works towards common goals (Arenas et al., 2010). After setting up this goal, all senior and junior members are aware of their duties, roles, and responsibilities. The objective of business is to act as a guidebook while employees generate risk management plans. When everyone has difficulty working to accomplish objectives, they can easily assess whether risk-taking is worthwhile. In addition, they must focus on a few aspects, i.e. risk tolerance, risk appetite, etc. Risk tolerance refers to the optimum level of risk that a business can take to accomplish its mission and vision. On the other hand, the willingness to take a level of risk to pursue objectives and goals is known as risk appetite. A high-level risk management plan can be formulated that includes strategies and goals when the business is able to define these attributes.

### ***1.2.3. Identification of Opportunities and Risks***

The identification of opportunities and risks is the most crucial component of the enterprise resource management framework. In any execution of the project, two

types of events occur: (i) opportunities and (ii) risks. Opportunities can provide some tangible benefits to the firm, whereas risks can disrupt the progression of a project. Under the risk mitigation strategy, these events are analysed carefully. The evaluation of potential risks and opportunities is the core strategy of any business.

#### ***1.2.4. Assessment of Risks and Categorisation***

Several business areas are affected by different types of risk. It consists of strategic risks, compliance risks, safety risks, operational risks, etc. Strategic risk threatens the sustainability of businesses. Compliance risk involves violating the rules, regulations, and guidelines of a business. Safety risks define the lack of employee health and safety measures (Grace et al., 2015). Operational risks can occur due to inefficiency in managing corporate resources. Currently, there is a risk called cyber security risk, which is crucial for information technology firms. The categorisations of risk always determine the priority of risk management in the course of business action.

#### ***1.2.5. Risk Response and Mitigation***

After careful assessment and mitigation of business risk categorisation, a response must be decided upon because the types of risk responses will vary. A few ways to respond to risks, such as reducing risks to shorten their impact, minimising or neglecting the risk, eliminating the risk if it is large, and transferring or assigning the mitigation of risk to a competent third party, are discussed. In favour of a strategic planning process, risk response is always ensured by leaders along with employees' implementation.

#### ***1.2.6. Checks and Balances***

The checks and balances **ensure** that the response activities are carried out in accordance with the policies. Risk mitigation measures are of equivalent importance to the company's values and ethics. This period is not avoided in the event of an employee's failure to comply with defined and existing legislation. The Board of Directors shall be responsible for clarifying the duties and responsibilities associated with transparency, in accordance with the risk management strategy and its framework. Some internal control measures shall be included in this documentation in the event of any unethical conduct (Desender, 2011).

#### ***1.2.7. Information and Communication***

Communication is the fragrance of any business firm. The digital advanced world protects the immense value of business. In the process of risk management, every employee of the organisation must identify potential risks and communicate with its managers and stakeholders. This process provides a prominent picture that no risk factors have been overlooked. Training programs on risk assessment

and identification should be implemented in every organisation for the purpose of learning for their employees. This approach helps to achieve an exponential increase in efficiency.

### 1.3. Types of Enterprise Risks

Business organisations must take the initiative to protect themselves from risk areas through different functions. There are many challenges, such as traditional labour concerns, new technologies, cyber threats, financial losses, and resistance to change management, that play a critical role in the business environment. If risk areas of operations are not identified properly, losses will occur. Every business has its status quo in terms of mission and vision. To accomplish mission and vision statements, firms must identify, assess, and monitor risk management procedures. In this section, we have discussed various types of organisational risks and how they work (Fig. 1.3).

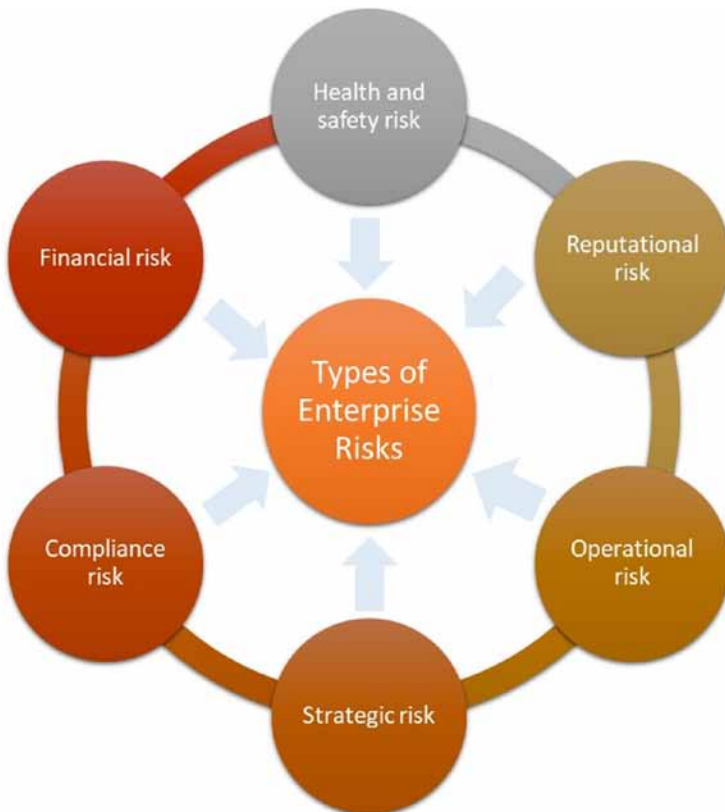


Fig. 1.3. Types of Enterprise Risks.

### ***1.3.1. Health and Safety Risk***

In a variety of forms, general health and safety risks can be presented in an organisation irrespective of whether the workplace is a construction site or a head office. The key is to identify the types of hazards, such as physical, chemical, ergonomic, and biological hazards. Risk assessment in these fields is critical, and appropriate control measures must be taken in the proper place to ensure that employees are safe and taken care of physically and mentally in both directions. The greatest amount of protection with high reliability is the best practice for workplace health and safety (Paape & Speklé, 2012; Sweeting, 2017).

### ***1.3.2. Reputational Risk***

Every business has its own reputation to maintain for the long run, along with investors, customers, and employees. Decisions made by the business are vital because they impact brand perception. Due to the rise of social media, reputational risk has become a great concern. The global communication chain makes this process more challenging for companies. Reputational threats can have adverse effects on organisational effectiveness.

### ***1.3.3. Operational Risk***

Another important risk area of business is operational risk. To minimise danger, critical incidents and unexpected circumstances during day-to-day operations are tested. Operational risk is based on internal processes, systems, external events, and people. A few examples include global crises, data breaches, people lost, IT system hang-ons, litigation, and many more. Therefore, an organisation must know the daily processes, functions, and systems of its business and need to set up a plan for risk management in these functional domains. One software package, RiskWare, is helpful in identifying these critical functions and can improve plans for risk management (Lin et al., 2012; McShane et al., 2011).

### ***1.3.4. Strategic Risk***

To achieve future success, the fundamental goal is to formulate a strategy for businesses. Strategic risk includes external causes or circumstances; if they occur, the strategic direction of the business must change. The degree of opportunities and threats vary from business to business. Exploring strategic risks in these parts may help to mitigate the issues that might be created.

### ***1.3.5. Compliance Risk***

Compliance risk includes the areas of industrial laws, regulations, policies, and best practices. It provides assurance of ethical business practices. Compliance risk might affect the financial and legal implications of business. Across the globally interconnected world, the rules and regulations of businesses are

changing quickly, which makes the legal framework difficult to navigate. For this reason, compliance management in business must prioritise, and software such as the riskware compliance module will help clarify any events of uncertainty (Oliva, 2016).

### **1.3.6. Financial Risk**

Financial risk may develop when an organisation earns lost revenue and invests extra money. The cash flow in and out of business can create this kind of financial loss. An example of this can be that if a company wants to expand its business in an international belt, fluctuations in the exchange rate can impose financial risk. If there is a lack of sound financial management practice, then the business is not able to achieve its goals. It is very difficult to assess financial risks, and the impact of those risks cannot be avoided.

## **1.4. An Effective Enterprise Risk Management System**

It is necessary to establish an effective enterprise resource management system for every organisation irrespective of size. The adopted framework should always be marked in relation to the identification of risk, assessment of risk, risk mitigation, and reporting. The enterprise risk management exercise will be closed when documentation is performed based on recognised frameworks and report preparation. The audit committee and board are active in this matter. There are various drivers that may help to assess an effective risk management system in an organisation. The drivers are discussed below (Fig. 1.4).

### **1.4.1. Risk Management Strategy**

First, every organisation needs to determine its risk management priorities, goals and objectives, approaches, and risk governance structure, which is based on its business model, size, and complexity. A risk management strategy consists of an assessment of the needed roles and competencies, compliance and internal functions of risk management, and the positions of strategy and reporting lines that must be placed under an organisational structure.

### **1.4.2. Risk Ownership**

The person who is responsible for executing risk responses and risk ownership is often assigned to him, though this is not an appropriate allocation of accountability. The head of the risk management function has important roles in communicating, coordinating, and administering the organisation's risk management activities and policies. They also ensure the identification and mitigation of material risks by the correct risk owners (Florio & Leoni, 2017; Fraser et al., 2014; Hoyt & Liebenberg, 2015). Sometimes there is a mistake in the process of selecting an appropriate risk owner, so the rest of the management team is responsible for meeting the board's requirements. Another striking point at this juncture is