Simplifying Risk Management
An Evidence-Based Approach to Creating Value for Stakeholders

Patrick Roberts, PhD

Routledge
A PRODUCTIVITY PRESS BOOK
Simplifying Risk Management
The author provides a comprehensive story that radiates a better understanding of organisational risk, through to the motivations for managing risk and its application in practice. The connectivity of these aspects is profound and enables such an approach to be defensible and more likely to stick in practice.

— Peter Noble, Chief Operating Officer, Newcastle Health Innovation Partners.

With a practitioner approach to risk management, Patrick brings what can be seen as a compliance obligation into ways of working that in my experience have added genuine value to management team business planning and collaboration.

— Matt Margereson, Chief Operating Officer, Hotel Chocolat.

Patrick Roberts’s practical sense backed by sound academic research has gone a long way to embed risk management into many organisational cultures. To the surprise of many this has been achieved without the need for costly software or bureaucratic form filling and the ultimate nightmare of the risk management tail wagging the management dog. This book, for the first time, challenges accepted wisdom on risk management and takes it out of its silo and places it squarely into mainstream management where it truly belongs.

— Mike Stephens, formerly Director of Safety, Security and Resilience, the Medical Research Council.

What is offered is a light bulb moment in collating and translating all the theory into a practical next level Risk Management solution. More than an expert opinion, but an expert solution; integrating risk assessment and mitigation within a structured process. This approach has already added value to the business
in dealing with COVID disruptions and associated Global Supply Chain issues.

—Malcolm Watling, Group Sourcing Director, Domino Printing Sciences.

Risk is mismanaged by most organisations from project selection through to completion. We all know of failed projects which have been buried and careers destroyed; and highly successful projects which rewarded executives but were, in reality, just an extremely lucky punt. Patrick’s quantitative approach to risk management allows organisations to assess managers’ performance based on the quality of their decision making rather than short-term results.

—Sean Blackburn, fixed failing projects whilst at McKinsey and now growing businesses as an executive within global organisations.

I have had the pleasure of working closely with Patrick on a number of projects over several years. His professionalism, depth of knowledge and pragmatic approach when communicating the strategic requirements when reviewing a business continuity plan and the various considerations when analysing the impact on the business.

This book clearly explains Patrick’s unique approach to risk management, drawing on his years of practical experience in implementing business continuity management and information security management systems for clients. In doing so, it goes well beyond the details of how to do risk management; to explore the fundamental questions of why we are trying to manage risk and how we can measure if we are delivering value for our stakeholders.
This is a must-read book for any CEO or board level executive involved in risk management.

—Dave Watson, Group Head of Property, Facilities Management and Fleet Operations, JLA Group.

A truly engaging, insightful and refreshing examination of the approach to risk management. An invaluable text for academics and practitioners alike to consider risk management techniques differently to bridge the gap between theory and application. Patrick uses his vast experience and extensive research to present a compelling and innovative case, with the focus on simplifying the process and placing return on investment at the heart of the decision-making process, driving efforts to truly manage risk to the benefit of all organisational stakeholders.

—Head of Corporate Security UKI & EMEA, Financial Services.

In this well-timed work, Patrick Roberts uses his extensive practical experience of risk management to offer a pragmatic look at the topic, offering organisations and the groups within these organisations a different and more tangible perspective. It's a refreshing take on the why, the how and (crucially) the return on investment of risk management for leaders and managers at every level within ‘everyday’, relatable organisations.

—Rupert Johnston, Director, Risk & Resilience Ltd and Specialist Member of the Institute of Risk Management.
Dedication

This book is dedicated to the memory of Professor George A F Roberts (1939-2018), a wonderful father and friend.
# Contents

Acknowledgements ............................................................................. xv
About the Author ................................................................................... xvii
Introduction .......................................................................................... xix
List of Figures and Tables ..................................................................... xxix
Testimonials .......................................................................................... xxxiii

## 1 What Do We Mean by Risk? ......................................................... 1
   Upside and Downside Risk ............................................................... 2
   Risk versus Uncertainty ................................................................. 2
   Risk to Whom? ............................................................................ 3
   Owners ....................................................................................... 4
   Senior Management ...................................................................... 8
   Lenders, Staff and Other Stakeholders .......................................... 10
   Reconciling Conflicting Interests ................................................. 11
   Risk Measures .......................................................................... 13
   Likelihood of Financial Distress ................................................... 14
   Variability in Outcomes ............................................................... 14
   Counting Events ........................................................................ 15
   Value at Risk ............................................................................. 15
   Categorisation of Risks ............................................................... 17
   Summary .................................................................................... 18
   References ............................................................................... 19
# Contents

2 Why Do We Try to Manage Risk? ..............................................21
- Improving Expected Outcomes........................................22
- Reducing the Likelihood of Extreme Events....................23
- Crises and “Black-Swans”..............................................25
- Reducing Variability in Outcomes................................28
- Demonstrating Good Corporate Governance..................31
- Compulsion ..................................................................32
- Why Do We Not Manage Risk? ....................................32
- Empirical Evidence..........................................................35
- How Many Organisations Manage Risk? .......................36
- Which Organisations Manage Risk? ..............................37
- The Incidence of Catastrophic Events and “Crises”.........38
- Summary .....................................................................39
- References ....................................................................40

3 Risk Management Systems .................................................43
- Integrated Risk Management .........................................44
- The Aims of Integrated Risk Management ......................44
- Implementation of Integrated Risk Management Systems ........................................................................45
- ISO 31000 .....................................................................47
- The Risk Management Framework ................................48
  - Leadership and Commitment......................................48
  - Integration ................................................................49
  - Design ......................................................................49
- Implementation, Evaluation and Improvement ...............50
- The Risk Management Process .....................................51
  - Communication and Consultation .............................51
  - Scope, Context and Criteria .....................................52
  - Risk Assessment ..........................................................52
  - Risk Treatment .............................................................55
  - Monitoring and Review .............................................61
  - Recording and Reporting .................................62
- Risk Displacement and Risk Compensation ..................62
- Summary .....................................................................64
- References ....................................................................65
4 Scope, Context and Criteria .............................................67
   Agreeing Risk Criteria ....................................................68
   Reducing the Probability of an Extreme Event ............70
   Reducing Variability of Outcomes ...............................71
   Ownership and Delegated Authority ............................73
   Justifying Resources ....................................................75
   Summary ........................................................................75
   References .....................................................................76

5 Risk Assessment .............................................................77
   Risk Identification ..........................................................78
   Granularity of Risks .........................................................78
   Risk Categorisations .......................................................80
   Recording and Reporting ..................................................82
   Risk Analysis ..................................................................83
   Distributions Based on Events .........................................83
      Frequency Distributions ................................................84
      Impact Distributions .....................................................85
      Monte-Carlo Modelling .................................................89
   Distributions Based on Continuous Variation ..............91
   Aggregating Profit and Loss Distributions ..................93
   Recording and Reporting ................................................99
   Summary .....................................................................100
   References ....................................................................100

6 Risk Treatment ...............................................................103
   Modelling the Risk Treatment .........................................104
   Improving Expected Outcomes .....................................106
   Reducing the Likelihood of Extreme Events ................106
   Reducing the Variability in Outcomes ..........................107
      Entrepreneurial Firms ................................................107
      Corporations ...............................................................108
   Public Sector and Not-for-Profit Organisations ..........109
   Some Parting Observations ............................................110
   Combining Risk Treatments ..........................................111
Recording and Reporting ........................................................ 111
Summary .................................................................................. 112

7 Measuring the Effectiveness of Risk Management ......................... 113
Measuring the Effectiveness of Individual Risk Treatments .................. 114
Estimating the Mitigating Effect on Major Disruptions ....................... 116
Evaluating the Success of Implementation ..................................... 121
Quantifying the Overall Impact of Risk Management Programmes .......... 122
Taking a Pragmatic Approach to Measurement .................................. 125
Summary .................................................................................. 126
References .............................................................................. 127

8 Underlying Themes and Summary ................................................. 129
Is a Quantitative Approach Really Practical? .................................. 130
How Does Strategy Link to Risk? ................................................. 132
Where Does Risk Management Belong in the Organisation? ................. 134
Crises and Black-Swans .............................................................. 135
Applicability to the Public and Not-for-Profit Sectors ......................... 139
Would Any of This Have Made a Difference in the Covid-19 Pandemic? .... 140
Summary of Key Ideas ................................................................ 145
  Know Your Organisation’s Stakeholders ..................................... 145
  Risk Assessment Is Not an End in Itself ..................................... 145
  Data ...................................................................................... 146
  The Role of Standards and “Good Practice” ............................ 146
  Granularity of Risks .............................................................. 146
  Managing Conflict and Tensions .............................................. 147
References .............................................................................. 147
Appendix A: Risk Return Relationships in UK Listed Companies .......................... 149
Appendix B: The Impact of Covid-19 on FTSE 100 Share Prices........................................ 155
Appendix C: Alternative Numerical Example ............ 167
Appendix D: Some Useful Sources of Risk Information............................................... 173
Index ..................................................................................................................... 175
Acknowledgements

I should like to thank all of my clients over the last 15 years for tolerating my constant desire to experiment and innovate: it must have been very trying for them at times. Your feedback over the years has been invaluable in developing the ideas that I set out in this book. In the interests of confidentiality, I don’t wish to name any individuals or organisations; but you know who you are.

I can, however, name two individuals who have made very significant contributions to the book. Despite being very busy responding to the Covid-19 pandemic at the time, Joanna Ragsdell very kindly agreed to review the first draft of the manuscript and identified numerous opportunities for improvement. I am most grateful for all the feedback. I should also like to express my profound gratitude to my wife and business partner, Helen Molyneux, without whom this book would never have happened. Not only has Helen encouraged and supported me throughout the process, and kept our business going whilst I have been distracted, but somehow she also found time to review and comment on the first draft.

Finally, I should like to thank the team at Taylor and Francis, Kristine Mednansky and Samantha Dalton, for guiding me through the slightly daunting process of getting a book published for the first time.
Patrick Roberts is a director of Cambridge Risk Solutions Ltd, which he founded with Helen Molyneux in 2008. Together, they have delivered risk management consultancy and training to a very wide range of clients, from sole traders to multi-national organisations, in the United Kingdom and overseas. Patrick was also a director of British Weightlifting from 2015 to 2019.

In addition to his extensive practical experience in risk management, Patrick has had a number of articles published in various professional journals. He is a Fellow of the Institute of Strategic Risk Management and obtained a PhD in risk and risk management from Nottingham University Business School.
This book attempts to place the practice of risk management within organisations into the mainstream of management, looking as much at \textit{why} we seek to manage risk as at \textit{how} we seek to manage risk. In doing this, I aim to bridge the significant gap between the academic and practitioner literatures on risk management.

Specifically, this book seeks to challenge two alarming trends in the practice of risk management:

- The treatment of risk management primarily as a compliance issue within an overall corporate governance narrative; and
- The very widespread use of qualitative risk assessment tools which have absolutely no proven effectiveness.

Taken together, these trends have resulted in much attention being devoted to developing formalised systems for identifying and analysing risks, and the production of many detailed risk registers. However, there is very little evidence that any of this is driving practical, cost-effective efforts to actually manage risk for the benefit of organisations’ stakeholders. There often appears to be a preoccupation with the risks themselves, rather than a positive focus on the actions that can (and should) be taken to benefit various stakeholder
groups. This is dramatically illustrated by the fact that a pandemic was the highest rated risk on the UK National Risk Register* for many years prior to 2020; but capturing it as such neither prevented multiple variants of Covid-19 reaching the UK nor led to robust preparations to deal with the consequences when they did.

It is quite inconceivable that potential R&D projects would be presented to senior management for approval in the form shown in Figure 0.1. Clearly, on the information given, Project “I” is more attractive than Project “A”; but is Project “D” more attractive than Project “E”? How much more would one be prepared to pay to pursue Project “F” than Project “E”? This whole line of argument may seem deliberately obtuse; but this is exactly how risks are generally presented. Even if some scales were added to the axes, descriptive or numerical, one is still not equipped to answer the questions posed with any

---

* Previous editions of the UK National Risk Register have now been withdrawn, but the 2020 version is available at https://www.gov.uk/government/publications/national-risk-register-2020.
certainty. It is argued throughout this book that decisions on risk management should be treated in exactly the same way as any other organisational decisions: on the basis of demonstrating a sufficient return on investment (financial or otherwise). Generally, this return on investment arises because the proposed risk management activities improve expected outcomes, reduce the likelihood of a catastrophic outcome and/or reduce the variability in outcomes. In order to make decisions in this way though, one needs to take a more quantitative approach.

If the use of the word “quantitative” at such an early stage in the book has raised any alarm bells, please do not be put off. There are a modest number of numerical and graphical examples throughout the text to illustrate key points, mainly in Chapters 5, 6 and 7; but there is absolutely no requirement to deal with any complex mathematics. Indeed, the efficacy of the approach that is advocated is based on its simplicity – there is no need for complex statistical methods or advanced software packages to implement it. Readers who are interested in the underlying mathematics are directed, where appropriate, to suitable references. If this book cannot be read and understood (perhaps even enjoyed) by anybody with a reasonable grasp of general management, then I have failed in my main objective.

This book is born out of my personal experience (I hesitate to say “journey”). My initial experience of working in various fields of risk management - primarily, physical security, business continuity management and information security management - proved somewhat unsatisfying without any solid basis in theory or empirical evidence. I therefore embarked on doctoral research, where I found much of interest and potential utility, but not in a format that was immediately usable by practitioners. The past few years have involved many small experiments in applying ideas from the academic literature in consulting projects, commercial training and occasional