



6th Edition

FUNDAMENTALS OF RISK MANAGEMENT

UNDERSTANDING, EVALUATING AND IMPLEMENTING EFFECTIVE ENTERPRISE RISK MANAGEMENT

PAUL HOPKIN
WITH CLIVE THOMPSON



Developing risk professionals



Fundamentals of Risk Management

THIS PAGE IS INTENTIONALLY LEFT BLANK

Sixth Edition

Fundamentals of Risk Management

Understanding, evaluating and implementing
effective enterprise risk management

Paul Hopkin and Clive Thompson



Publisher's note

Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publishers and author cannot accept responsibility for any errors or omissions, however caused. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the editor, the publisher or the author.

First published in Great Britain and the United States in 2010 by Kogan Page Limited
Sixth edition 2022

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms and licences issued by the CLA. Enquiries concerning reproduction outside these terms should be sent to the publishers at the undermentioned addresses:

2nd Floor, 45 Gee Street London EC1V 3RS United Kingdom www.koganpage.com	122 W 27th St, 10th Floor New York, NY 10001 USA	4737/23 Ansari Road Daryaganj New Delhi 110002 India
--	--	---

Kogan Page books are printed on paper from sustainable forests.

© The Institute of Risk Management 2010, 2012, 2014, 2017, 2018, 2022

The right of The Institute of Risk Management to be identified as the author of this work has been asserted by it in accordance with the Copyright, Designs and Patents Act 1988.

ISBNs

Hardback	978 1 3986 0288 5
Paperback	978 1 3986 0286 1
Ebook	978 1 3986 0287 8

British Library Cataloguing-in-Publication Data

A CIP record for this book is available from the British Library.

Library of Congress Control Number

2021949187

Typeset by Integra Software Services, Pondicherry
Print production managed by Jellyfish
Printed and bound by CPI Group (UK) Ltd, Croydon CR0 4YY

To a safe, secure and sustainable future

THIS PAGE IS INTENTIONALLY LEFT BLANK

CONTENTS

List of figures xvii

List of tables xix

List of case studies xxii

Foreword by Stephen Sidebottom xxiii

Acknowledgements xxiv

Introduction 1

Risk management in context 1

Nature of risk 1

Risk management 2

Risk management terminology 3

Benefits of risk management 4

Features of risk management 5

Book structure 6

Risk management in practice 6

Future for risk management 7

Changes for the sixth edition 8

PART ONE Introduction to risk management 9

Learning outcomes 9

Further reading 10

Case studies 10

01 What risk is and why it is important 15

Definitions of risk 15

Types of risks 17

Risk description 19

Levels of risk 19

Classification systems 20

Risk likelihood and impact 21

Why understanding risk is important 22

Impact of hazard risks 23

Attachment of risks 24

Risk and reward 26

Attitudes to risk 27

Risk and triggers 28

Notes 30

02 Risk is an opportunity as well as a threat 31

Four types of risk 31

Timescale of risk impact 34

Minimize compliance risks 35

Mitigate hazard risks 36

Manage uncertainty (or control) risks 39

Embrace opportunity risks 40

03 Managing risk: The background, principles and aims of risk management 42

Origins of risk management 42

Taking calculated risks 45

Specialist areas of risk management 47

Enterprise risk management 48

Levels of risk management sophistication 50

Principles of risk management 52

Objectives of risk management 53

Risk management activities 54

Effective and efficient core processes 54

Implementing risk management 56

Achieving benefits 57

Risk management drives and enables activities 57

Notes 58

04 Risk management standards 59

Use of risk management standards for listed companies 60

Risk management process 61

Context 61

The standards in more detail 63

Updating of RM terminology 67

Note 68

05 Risk management in context 69

Scope of the context 69

External context 71

Internal context 72

- Risk management context 74
- Designing a risk register 75
- Using a risk register 76
- The future for risk registers 77

PART TWO Enterprise risk management 79

- Learning outcomes 79
- Further reading 80
- Case studies 80

06 Enterprise risk management 83

- Enterprise-wide approach 83
- Definitions of ERM 85
- ERM in practice 86
- ERM and business continuity management 87
- Integrating strategy and performance 88
- Note 89

07 Implementing enterprise risk management 90

- Investment in change 90
- A worthwhile change 91
- Integrating processes, reviewing and improving 91
- Plan, implement, measure and learn (PIML) 92
- Notes 98

08 The context for ERM 99

- Changing face of risk management 99
- Lessons from the past: Financial and health crises 99
- The power of taking risks 101
- Managing emerging risks 101
- Increasing importance of resilience 103
- Note 104

09 Setting objectives for ERM 105

- Risk management standards and objectives 105
- Strategy and objectives in standards 106
- Implementing objectives 107
- Aligning objectives to risk management principles 108
- Notes 109

PART THREE Assessment and analysis 111

Learning outcomes 111

Further reading 112

Case studies 112

10 Assessing risks: Considerations, causes and consequences 115

Importance of risk assessment 115

Approaches to risk assessment 116

Risk assessment techniques 117

Nature of the risk matrix 120

Risk perception 122

Attitude to risk 123

11 Classifying risks 127

Risk classification systems 127

Time to impact 128

Examples of risk classification systems 129

FIRM risk scorecard 131

PESTLE risk classification system 133

Compliance, hazard, control and opportunity 136

12 Analysing risks: The dimensions of risk 138

Levels of risk 138

Inherent and current level of risk 139

Control confidence 141

4Ts of hazard risk response 142

Risk significance 143

Risk capacity 145

Evaluating risks: Risk appetite 146

Note 147

13 Controlling the downside of risk 148

Risk likelihood 148

Risk magnitude 149

Hazard risks 150

Loss prevention 152

Damage limitation 153

Cost containment 153

14 Maximizing the upside of risk 155

- Defining the upside 155
- Opportunity assessment 157
- Riskiness index 159
- Upside in strategy 162
- Upside in projects/programmes 163
- Upside in operations 164
- Upside of compliance risks 165
- Note 165

PART FOUR Risk response 167

- Learning outcomes 167
- Further reading 168
- Case studies 168

15 Managing and responding to risk 171

- The 4Ts of hazard response 171
- Strategic risk response 178

16 Risk treatment controls for hazard risks 182

- Types of controls 182
- Cost of risk controls 189

17 Ongoing monitoring and review 193

- The importance of monitoring 194
- Frequency 195
- Process 195
- Reporting 196
- Responsibility 197

18 Insurance and risk transfer 198

- History of insurance 198
- Transferring the financial consequences of risk 198
- Types of insurance cover 200
- Evaluation of insurance needs 201
- Purchase of insurance 203
- Captive insurance companies 204

- 19 Surviving shocks and disruption: ERM, BCP and resilience 207**
- VUCA 207
 - Business continuity planning and resilience 208
 - Business continuity planning 208
 - Business continuity standards 210
 - Successful business continuity 212
 - Business impact analysis 214
 - Resilience, business continuity and ERM 215
 - Civil emergencies 216
 - Notes 217

PART FIVE Organizational environment 219

Learning outcomes 219

Further reading 220

Case studies 220

- 20 Business and the risk environment 223**

Dynamic business models 223

Types of business processes 226

Strategy and tactics 227

Effective and efficient operations 229

Ensuring compliance 230

Reporting performance 231

- 21 The organization's business model, visions and values 233**

Components of the business model 233

Risk management and the business model 235

Ethics and corporate governance 236

CSR and risk management 237

Supply chain and ethical trading 239

Importance of reputation 242

Notes 244

- 22 How risk management adds value 246**

What is the evidence? 246

Improved performance and key risk indicators 247

The benefits of an ERM approach 248

Climate change as a key risk 251

Becoming more strategic 252

Notes 253

PART SIX Risk strategy and culture 255

Learning outcomes 255

Further reading 256

Case studies 256

23 Risk architecture and strategy 259

Architecture, strategy and protocols 259

Risk architecture 263

Risk management strategy 263

Risk management protocols 264

Risk management manual 265

Risk management documentation 268

24 Roles, responsibilities and documentation 273

Allocation of responsibilities 273

Range of responsibilities 274

Statutory responsibilities of management 276

Role of the risk manager 278

Risk architecture in practice 280

Risk committees 283

25 Culture and behaviours 286

Styles of risk management 286

Steps to successful risk management 286

Defining risk culture 289

Measuring risk culture 292

Alignment of activities 294

Risk maturity models 296

26 Risk appetite and tolerance 299

Nature of risk appetite 299

Risk appetite and the risk matrix 300

Risk and uncertainty 303

Risk exposure and risk capacity 303

Risk appetite statements 306

Risk appetite and lifestyle decisions 309

Note 310

- 27 Risk training and communication 311**
- Consistent response to risk 311
 - Risk training and risk culture 312
 - Risk information and communication 313
 - Shared risk vocabulary 315
 - Technology to support risk management process and procedures 316
 - Risk management information systems 317
- 28 Risk practitioner competencies 320**
- Competency frameworks 320
 - Range of skills 321
 - Communication skills 323
 - Relationship skills 326
 - Analytical skills 327
 - Management skills 328
-
- PART SEVEN Corporate governance and risk management 331**
- Learning outcomes 331
 - Further reading 332
 - Case studies 332
- 29 Introducing corporate governance 335**
- Corporate governance 335
 - OECD principles of corporate governance 336
 - Future direction of corporate governance 338
 - London Stock Exchange corporate governance framework 338
 - Corporate governance for a financial services organization 340
 - Corporate governance for a government agency 341
 - Evaluation of board performance 344
 - Notes 347
- 30 Stakeholders, ethics and corporate social responsibility 348**
- Range of stakeholders 348
 - Stakeholder dialogue 350
 - Stakeholders and core processes 351
 - Stakeholders and strategy 353
 - Stakeholders and tactics 354
 - Stakeholders and operations 355
 - Notes 356

31 Different approaches to risk management 357

- Operational risk management 357
- Project risk management 366
- Supply chain risk management 375
- Note 381

PART EIGHT Risk assurance and reporting 383

- Learning outcomes 383

- Further reading 384

- Case studies 384

32 The control environment 387

- Nature of internal control 387
- Resilience of the organization in the event of external shock 388
- Purpose of internal control 388
- Control environment 389
- Features of the control environment 392
- Expectations of internal control 392
- CoCo framework of internal control 393
- Good safety culture 395
- The future for control processes 396
- Note 396

33 Internal audit activities 397

- Scope of internal audit 397
- Role of internal audit 398
- Undertaking an internal audit 399
- Risk management and internal audit 401
- Management responsibilities 405
- Five lines of assurance 405

34 Risk assurance techniques 407

- Audit committees 407
- Role of risk management 409
- Risk assurance 411
- Risk management outputs 413
- Control risk self-assessment 414
- Benefits of risk assurance 415

35 Reporting on risk management 416

- Risk reporting 416
- Sarbanes-Oxley Act of 2002 418
- Risk reports by US companies 420
- Charities' risk reporting 421
- Public sector risk reporting 423
- Government report on national security 423
- Notes 425

Appendix A: Abbreviations and acronyms 426

Appendix B: Glossary of terms 429

Index 437

LIST OF FIGURES

- 1.1** Risk likelihood and impact 21
1.2 Attachment of risks 25
1.3 Risk and reward 27
1.4 Risks and the bow-tie 29
3.1 Risk management process 49
3.2 Risk management sophistication 51
4.1 Components of the RM context 62
4.2 ISO 31000 principles, framework and risk management process 65
4.3 COSO ERM cube 66
4.4 COSO ERM rainbow double helix 67
5.1 Three components of context 70
5.2 Components of a risk register 76
7.1 Implementing risk management by PIML 93
9.1 Three levels of objective setting 108
10.1 Risk attitude matrix 124
11.1 Bow-tie representation of risk management 130
11.2 Bow-tie and risks to premises 131
12.1 Inherent, current and target levels of risk 140
12.2 Confidence in controls 142
13.1 Loss control and the bow-tie 152
14.1 Risk matrix for opportunities and hazards 158
15.1 Risk matrix and the 4Ts of hazard management 172
15.2 Risk versus reward in strategy 178
15.3 Opportunity risks and risk appetite 180
16.1 Bow-tie and types of controls 184
16.2 Hazard risk zones 186
16.3 Illustration of control effect 190
16.4 Cost-effective controls 191
18.1 Role of captive insurance companies 205
19.1 Disaster recovery timeline and costs 209
19.2 Model for business continuity planning 211
20.1 Business development model 225
21.1 Components of the business model 234
21.2 Mapping the components of reputation 243
23.1 Risk management framework 260

- 23.2** Example risk management framework 262
- 24.1** Risk architecture for a large corporation 281
- 24.2** Risk architecture for a charity 283
- 25.1** Risk maturity demonstrated on a matrix 298
- 26.1** Risk appetite, exposure and capacity (optimal) 301
- 26.2** Risk appetite, exposure and capacity (vulnerable) 304
- 29.1** LSE corporate governance framework 339
- 29.2** Corporate governance in a government agency 342
- 30.1** Importance of core processes 352
- 31.1** Risk matrix to represent project risks 369
- 31.2** Bow-tie to represent project risks 370
- 31.3** Project lifecycle 371
- 31.4** Decreasing uncertainty during the project 372
- 32.1** The CoCo framework 390
- 33.1** Role of internal audit in ERM 399
- 33.2** Governance, risk and compliance 403
- 35.1** Selected UK security threats 425

LIST OF TABLES

1.1	Definitions of risk 16
1.2	Types of risk 18
2.1	Risks associated with owning a car 32
2.2	Categories of operational disruption 38
3.1	Definitions of risk management 45
3.2	Importance of risk management 46
3.3	Principles of risk management 52
3.4	Risk management objectives 53
4.1	Risk management standards 60
4.2	COSO ERM cube 66
6.1	Features of an enterprise-wide approach 84
6.2	Definitions of enterprise risk management 85
6.3	Benefits of enterprise risk management 87
10.1	Top-down risk assessment 117
10.2	Bottom-up risk assessment 117
10.3	Techniques for risk assessment 118
10.4	Advantages and disadvantages of risk assessment techniques 119
10.5	Definitions of likelihood 121
10.6	Definitions of impact – example hospital risks 121
11.1	Risk classification systems 130
11.2	Attributes of the FIRM risk scorecard 132
11.3	PESTLE classification system 134
11.4	<i>Orange Book</i> risk categories 135
12.1	Levels of risk 139
12.2	Benchmark tests for risk significance 144
13.1	Generic key dependencies 151
14.1	Defining the upside of risk 155
14.2	Riskiness index 160
15.1	Description of the 4Ts of hazard response 172
15.2	Key dependencies and significant risks 173
16.1	Description of types of hazard controls 182
16.2	Examples of the hierarchy of hazard controls 183
16.3	Application of PCDD 185
18.1	Advantages and disadvantages of insurance 199
18.2	Different types of insurance 201
18.3	Identifying the necessary insurance 202

18.4	The 6Cs of insurance buying 203
19.1	Key activities in business continuity planning 212
21.1	Scope of issues covered by CSR 237
21.2	Components of reputation 243
22.1	Key risk indicators 248
22.2	Benefits of ERM 249
22.3	From safeguarding to maximizing value 253
23.1	Types of RM documentation 265
23.2	Risk management manual 266
23.3	Risk management protocols 267
24.1	Risk management responsibilities 275
24.2	Historical role of the insurance risk manager 278
24.3	Responsibilities of the RM committee 284
25.1	Styles of risk management and their features 287
25.2	Achieving successful enterprise risk management 287
25.3	Implementation barriers and actions 288
25.4	Risk-aware culture 290
25.5	Four levels of risk maturity 295
26.1	Definitions of risk appetite 300
26.2	Risk appetite statements for a college 307
26.3	Risk appetite for a manufacturing organization 309
27.1	Risk management training 313
27.2	Risk communication guidelines 314
27.3	Risk management information system 317
28.1	Risk management technical skills 321
28.2	People skills for risk management practitioners 322
28.3	Structure of training courses 325
29.1	OECD principles of corporate governance 337
29.2	Nolan principles of public life 343
29.3	Evaluating the effectiveness of the board 345
30.1	Data for shareholders 351
31.1	ORM principles (Basel II) 360
31.2	Examples of operational risks faced by a bank or financial institution 362
31.3	Operational risk in financial and industrial companies 364
31.4	PRAM model for project RM 374
31.5	Risks associated with outsourcing 379
31.6	Scope of outsourcing contracts 379
32.1	Definitions of internal control 387
32.2	Components of the CoCo framework 391
33.1	Undertaking an internal audit 400

34.1	Responsibilities of the audit committee	408
34.2	Sources of risk assurance	411
35.1	Risk management responsibilities of the board	417
35.2	Risk report in a Form 20-F	421
35.3	Government risk-reporting principles	423

LIST OF CASE STUDIES

Part One

- Ocado: Risk management process (retail, UK)
 Lenovo Group: Significant risks and mitigations (technology, Asia)
 UK Cabinet Office: An essential tool for delivering objectives (government, UK)

Part Two

- bp: Integrated approach to risk management (energy, UK)
 Lincolnshire County Council: Strategic approach to risk management (local authority, UK)
 DP World: Enterprise approach to risk management (logistics, Middle East)

Part Three

- British Land: Risk assessment (real estate, UK)
 Softcat plc: Risk appetite (fintech, UK)
 Darktrace: Governance of risk management (technology, UK)

Part Four

- Dangote Cement plc: Sustainability (building materials, Africa)
 NHS Resolution: Monitoring and review (public body, UK)
 Thomas Miller Holdings Ltd: Risk committees (services, UK)

Part Five

- Whitbread plc: Business model and ethics (hotels, UK)
 East African Breweries Limited: Whistleblowing (drinks, Africa)
 Booz Allen Hamilton: Ethics and community response to Covid-19 (consultancy, USA)

Part Six

- Singapore Airlines: Response to pandemic (airline, Asia)
 Nokia plc: Business model and risk management function (technology, Europe)
 Financial Conduct Authority: Risk culture (regulator, UK)

Part Seven

- Capita: Structure of board and stakeholders (outsourcing, UK)
 Pioneer Food Group: Mergers and regulation (food manufacture, Africa)
 UK Department for Work and Pensions: A chief risk officer (government, UK)

Part Eight

- Unilever: Opportunity assessment (FMCG, UK)
 Colgate Palmolive: Damage to reputation (FMCG, UK)
 Sainsbury's Bank: Evidence of control (financial services, UK)

FOREWORD

Enterprise risk management in a digital age

Organizations face an increasingly challenging and complex environment in which to undertake their activities. Since the fifth edition of this textbook, the inexorable rise of technology, the appearance of a truly global pandemic, further geopolitical instability and the increasing urgency to deal with climate change have all come to the fore.

It is within this increasingly uncertain environment that organizations are required to deliver higher stakeholder expectations, whilst fulfilling greater corporate governance requirements in relation to ethical and social responsibility. For example, legislation has been introduced in many countries to broaden the scope of requirements regarding management of bribery risk and the avoidance of modern slavery.

Given all these developments, the updating of this textbook to position enterprise risk management (ERM) in a digital age is very timely. As the world embraces new ways of working accelerated by the pandemic and exploits our enhanced analytical abilities, successful ERM, including the protection of corporate reputation, will be a business imperative for all organizations. A successful ERM initiative enhances the ability of an organization to achieve objectives and ensure sustainability, based on transparent and ethical behaviours.

The Institute of Risk Management (IRM) has long supported the development of ERM, as a contribution to development and delivery of successful business models and strategy for all types of organizations. The training courses and qualifications offered by the IRM enable risk professionals and others to support their employer and/or clients in achieving maximum benefit from an ERM initiative.

Although this textbook has been designed specifically for the IRM International Certificate in Enterprise Risk Management, the contents outline approaches to achieving successful ERM that will support any type of organization in their efforts to deliver corporate objectives and satisfy stakeholder expectations. This textbook is a valuable resource for all organizations and anyone with an interest in risk management.

*Stephen Sidebottom
Chair, Institute of Risk Management*

ACKNOWLEDGEMENTS

The risk management profession and the expertise of risk professionals continues to develop in line with the ever-increasing expectations placed on risk managers and risk consultants. Many organizations have now appointed individuals with the job title chief risk officer (CRO) which has increased the need for robust professional qualifications and designations for risk management practitioners.

Given the ever-increasing complexity of the business environment, it is not surprising that production of the sixth edition of *Fundamentals of Risk Management* became necessary, three years after production of the fifth edition. The importance and contribution of risk management continues to increase, and centres of risk management expertise and excellence continue to thrive in all business sectors, whether private, public or third sector.

This edition is the first which Paul Hopkin has not authored directly. The text remains largely based on Paul's thoughts, ideas and expertise developed over the course of his extensive career. In updating this book, it was clear that the fundamentals he laid down back in 2010 remain. It has been my privilege to bring my own experience of the lectures, seminars, special interest and other group meetings we both attended over many years to bear. The process of enterprise risk management will continue to be embedded in everyday activity: the UK government has produced new guidance and financial regulation continues to advance in this direction.

This sixth edition remains closely aligned with the syllabus of the IRM qualifications in enterprise risk management. When undertaking this task, I have received considerable help and support from colleagues at the Institute of Risk Management, in particular my team of peer reviewers, particularly Kate Boothroyd and Doug Smith, whose dedication was unwavering, but also Mark Turner, Simona Fionda, Esme Pitasi, and Serrina Galleymore, all of whom volunteered their expertise to review relevant sections and to make the text as up to date as possible. An editorial role requires making choices as to interpretation, and at times I was unable to accept every comment. As always, any mistakes remain my own.

Finally, I must acknowledge the unwavering support of, Laura, my partner of 40 years. In our early days together, her encouragement suggested more diligence in my business studies would be appropriate, and the application she inspired has always bolstered my career. I know students have everyday challenges to overcome in pursu-

ing their studies and I hope this new edition helps them meet those challenges. I am sure it will be worth the effort, and this book is testament to my patient wife's encouragement.

Developments in risk management will continue apace. Technology will have a greater role to play in helping risk managers not only to control risk, but also to exploit opportunities. The scope of risk management will expand as it contributes to the modifications necessary to cope with climate change. In that respect, some of the processes described in this text will age but, as it says in Paul's original title, the fundamentals of risk management will remain. There are some exciting developments ahead, and the future for the new entrants to risk management will be bright if they equip themselves with these fundamentals.

Clive Thompson

Boost your career with the IRM

IRM is the leading professional body for risk management. We drive excellence in managing risk to ensure organisations are ready for the opportunities and threats of the future.

We do this by providing internationally recognised qualifications and training, publishing research and guidance, and setting professional standards. We are a not-for-profit educational institute, with members working in all industries, in all risk disciplines and in all sectors around the world.

What IRM offers Risk Professionals

Training courses



Our risk management training gives you the knowledge, tools and techniques you need to protect your organisation.



Free webinars

You can access free webinars that cover a wide range of presentations, helpful for professionals at every level.



Blended Learning

Increase your chances of exam success and learn directly from module coaches in our face-to-face Blended Learning workshops.



Qualifications

Our risk management qualifications give you the broad knowledge and the practical skills you need to manage risks.



Building a community

We help people connect with our sector-specific Special Interest Groups, Regional Groups and social media platforms.

“

IRM qualifications provide a practical framework and a structured way of thinking. This is vital to success in a risk role.”

”

Find out more at www.theirm.org »

The Institute of
Risk Management

irm

Introduction

Risk management in context

This book is intended for all who want a comprehensive introduction to the theory and application of risk management. It sets out an integrated introduction to the management of risk in public and private organizations. Studying this book will provide insight into the world of risk management and may also help readers decide whether risk management is a suitable career option for them.

Many readers will wish to use this book in order to gain a better understanding of risk and risk management and thereby fulfil the primary responsibilities of their jobs with an enhanced understanding of risk. This book is designed to deliver the syllabus of the International Certificate in Risk Management qualification of the Institute of Risk Management. However, it also acts as an introduction to the discipline of risk management for those interested in the subject but not (yet) undertaking a course of study.

We all face risks in our everyday lives. Risks arise from personal activities and include those associated with health, personal financial decisions and domestic and relationship issues, but these are outside the scope of this discussion. This book is primarily concerned with risks that arise through business, government or charity/third sector activities. And it is concerned with risk in its widest guise, to embrace opportunities that come with ‘taking a risk’.

Nature of risk

Recent events have brought risk into higher profile. The Covid-19 pandemic, extreme weather events and geopolitical upheavals represent the extreme risks that society and commerce face. These extreme risks exist in addition to the daily, somewhat more mundane, risks mentioned above.

Evaluating the range of risk responses available and deciding on the most appropriate one in each case is at the heart of risk management. Responding to risks should produce benefits for us as individuals, as well as for the organizations where we work and/or are employed.

Within our personal and domestic lives, many of the responses to risk are automatic. Our ways of avoiding fire and road traffic accidents are based on well-established and automatic responses. Fire and accident are the types of risks that can only have negative outcomes, and they are often referred to as hazard risks.

Keeping your car in good mechanical order will reduce the chances of a breakdown. However, even vehicles that are fully serviced and maintained do occasionally break down. These types of risks that have a large degree of uncertainty associated with them are often referred to as control risks.

We all need to comply with rules and regulations to bring order to society, and a failure to comply can only be negative. For businesses, achieving compliance is often mandatory but can be advantageous and represent an additional benefit in its business, representing the ‘upside of risk’.

As well as hazard, control and compliance risks, there are risks that we take because we desire (and probably expect) a positive return. For example, you invest money in anticipation that you will make a profit from the investment. Likewise, placing a bet or gambling on the outcome of a sporting event is undertaken in anticipation of receiving positive payback. People participate out of choice in motor sports and other potentially dangerous leisure activities. In these circumstances, the return may not be financial, but can be measured in terms of pride, self-esteem or peer group respect. Undertaking activities involving risks of this type, where a positive return is expected, can be referred to as taking opportunity risks.

Risk management

Organizations face a very wide range of risks that can impact the outcome of their operations. The desired overall aim may be stated as a mission or a set of corporate objectives. The events that can impact an organization may inhibit what it is seeking to achieve (hazard risks), enhance that aim (opportunity risks) or create uncertainty about the outcomes (control risks).

Risk management needs to offer an integrated approach to the evaluation, control and monitoring of these three types of risk. This book examines the key components of risk management and how it can be applied. Examples are provided that demonstrate the benefits of risk management to organizations in both the public and private sectors. Risk management also has an important part to play in the success of not-for-profit organizations such as charities and (for example) clubs and other membership bodies.

The risk management process is well established, although it is presented in a number of different ways and often in differing terminologies. The different terminologies that are used by different risk management practitioners and in different business sectors are explored in this book. In addition to a description of the established risk management standards, a simplified description of risk management that sets out the key stages in the risk management process is also presented to help with understanding.

The risk management process cannot take place in isolation. It needs to be supported by a framework within the organization. Once again, the risk management

framework is presented and described in different ways in the range of standards, guides and other publications that are available. In all cases, the key components of a successful risk management framework are the communications and reporting structure (architecture), the overall risk management strategy that is set by the organization (strategy) and the set of guidelines and procedures (protocols) that have been established. The importance of the risk architecture, strategy and protocols (RASP) is discussed in detail in this book.

The combination of risk management processes, together with a description of the framework in place for supporting the process, constitutes a risk management standard. There are several risk management standards in existence, including the IRM standard and British Standard BS 31100:2011. There is also the American COSO enterprise risk management (ERM) cube. The most high-profile addition to the available risk management standards is the International Standard, ISO 31000, first published in 2009 and updated in 2018.

Further information on existing standards and other published guides is set out in Chapter 4. Additionally, references are included in each part of this book to provide further material to enable the reader to gain a comprehensive introduction to the subject of risk management. Abbreviations and acronyms are used throughout the book as an aid to learning and understanding. A list of all abbreviations and acronyms is included in Appendix A.

Risk management terminology

Most risk management publications refer to the benefits of having a common language of risk within the organization. Many organizations manage to achieve this common language and common understanding of risk management processes and protocols at least internally. However, it is usually the case that within a business sector, and sometimes even within individual organizations, the development of a common language of risk can be very challenging.

Reference and supporting materials use a great range of terminologies. The different approaches to risk management, the different risk management standards that exist and the wide range of guidance material that is available often use different terms for the same feature or concept. This is regrettable and can be very confusing, but it is inescapable.

Attempts are being made to develop a standardized language of risk, and ISO Guide 73 has been developed as the common terminology that should be used in all ISO standards. The terminology set out in ISO Guide 73 is used throughout this book as the default set of definitions wherever possible. However, the use of a standard terminology is not always possible and alternative definitions may be required. Indeed, ISO itself also publishes a terminology guide, ISO/IEC Guide 51:2014, entitled

Safety Aspects: Guidelines for their inclusion in standards, and the definitions in Guide 51 are not fully aligned with those in Guide 73.

To assist with the difficult area of terminology, Appendix B sets out the basic terms and definitions that are used in risk management. It also provides cross-reference between the different terms in use to describe the same concept. Where appropriate and necessary, a table setting out a range of definitions for the same concept is included within the relevant chapter of the book, and these tables are cross-referenced in Appendix B.

Benefits of risk management

There are a range of reasons why organizations undertake risk management activities. These reasons are summarized in this book as mandatory, assurance, decision making and effective and efficient core processes (MADE2). Mandatory refers to risk management activities designed to ensure that an organization complies with legal and regulatory obligations, as well as customer or client requirements. Chapter 22 itemizes how risk management adds value to an organization.

The board of an organization will require assurance that significant risks have been identified and appropriate controls put in place. In order to ensure that correct business decisions are taken, the organization should undertake risk management activities that provide additional structured information to assist with business decision making.

Finally, a key benefit from risk management is to enhance the effectiveness and efficiency of operations within the organization. Additionally, it should help ensure that business processes (including process enhancements by way of tactics, projects and other change initiatives) are also effective and efficient.

Risk management inputs are required in relation to strategic decision making, but also in relation to the effective delivery of projects and programmes of work, as well as in relation to the routine operations of the organization. The benefits of risk management can also be identified in relation to these three timescales of activities within the organization. The outputs from risk management activities can benefit organizations in three timescales and ensure that the organization achieves effective and efficient strategy, tactics and operations.

Strategy, tactics and operations are underpinned by the need to achieve compliance. Strategy, tactics, operations and compliance (STOC) core processes and activities encompass the whole range of processes of an organization. These processes are the core processes of the organization and analysis of the core processes provides a comprehensive approach to risk management that is used in several sections of the book.

In order to achieve a successful risk management contribution, the intended benefits of any risk management initiative have to be identified. If those benefits have not been identified, then there will be no means of evaluating whether the risk management initiative has been successful. Therefore, good risk management must have a clear set of desired outcomes/benefits. Appropriate attention should be paid to each stage of the risk management process, as well as to details of the design, implementation and monitoring of the framework that supports these risk management activities.

Features of risk management

Failure to adequately manage the risks faced by an organization can be caused by inadequate risk recognition, insufficient analysis of significant risks and failure to identify suitable risk response activities. Also, failure to set a risk management strategy and to communicate that strategy and the associated responsibilities may result in inadequate management of risks. It is also possible that the risk management procedures or protocols may be flawed, such that these protocols may actually be incapable of delivering the required outcomes.

The consequences of failure to adequately manage risk can be disastrous and may result in ineffective and/or inefficient operations, projects that are not completed on time and strategies that are not delivered, or were incorrect in the first place. The hallmarks of successful risk management are considered in this book. In order to be successful, the risk management initiative should be proportionate, aligned, comprehensive, embedded and dynamic (PACED).

Proportionate means that the effort put into risk management should be appropriate to the level of risk that the organization faces. Risk management activities should be aligned with other activities within the organization. Activities will also need to be comprehensive, so that any risk management initiative covers all the aspects of the organization and all the risks that it faces. The means of embedding risk management activities within the organization are discussed in this book. Finally, risk management activities should be dynamic and responsive to the changing business environment faced by the organization.

As with all management activities and processes in an organization, risk management needs to be adapted and modified to align with the core processes and organizational culture. In relation to risk management, an organization will first need to specifically respond to statutory obligations and the requirements of regulators. Once they have been satisfied, most organizations can work on the basis that whatever works within the organization and delivers the required benefits, outputs and outcomes is the correct and appropriate approach to ERM for that organization.

Book structure

The book is presented in eight parts, together with two appendices. An introduction to risk and risk management is provided in Part One. Part Two examines applying these concepts across an enterprise as a whole. Parts Three and Four describe the application of risk management in terms of risk assessment and risk response. Analysis of the various risk control techniques is presented, together with examples of options for the control of selected hazard risks. Part Four also considers the importance of insurance and risk transfer, as well as business continuity planning.

The practical application of risk management is considered in Part Five. There is also a consideration of reputation and the business model and the importance of the risk management context. Part Six considers risk strategy and culture, and also reflects on the fact that the emergence of risk management as a profession has resulted in more attention being paid to risk management competency frameworks and the importance of people or soft skills.

Part Seven describes risk governance and the impact of risk on organizations. The analysis of stakeholder expectations and the relationship between risk management and a simple business model are considered. Finally, Part Eight considers risk assurance and risk reporting. The role of the internal audit function, together with the importance of corporate social responsibility and the options for reporting on risk management are all considered. Appendix A is a full list of the main acronyms and abbreviations used in the book. Appendix B provides a glossary of terms and cross-references the different terminologies used by different risk management practitioners.

In order to bring the subject of risk management to life and provide context to the ideas and concepts that are described, short illustrative examples are used throughout the text. In addition to these general examples, real-life situations and examples are also used, where a case study is helpful. Each part of the book commences with case studies taken from the websites of high-profile organizations or from published annual reports and accounts, to illustrate the main risk management topics covered in that part. These examples have been taken from around the world and from different sectors.

Throughout the book, boxes are included within the text. These boxes either provide practical examples of the application of the theory being discussed, or they provide opinions and commentary on real situations that have arisen.

Risk management in practice

The Covid-19 pandemic has been devastating for those who have lost loved ones. The resulting economic dislocation has exposed some weaknesses in systems but

also forced us to show resilience and accelerate the trend towards the use of technology in everyday activity. The need for physical presence has lessened as more activity has migrated online. Sectors like tourism and transport have suffered but others, especially in the technology sector, have reaped rewards. Efficiencies have been revealed in how we conduct business, be that commercial or otherwise, that will be difficult to turn down in future.

However the world of work changes in future, it is undeniable that it will involve greater use of technology and the creation and analysis of more and more data. This trend towards data management will also help society as it shifts towards a carbon-neutral and more sustainable system to counter the effects of climate change. Both of these drivers will impact on the risks we face and the ways we manage risk. Both of these drivers are considered throughout this book where it is felt they will have specific impact.

Achieving benefits from risk management requires carefully planned implementation of the risk management process in the organization, as well as the design and successful embedding of a suitable and sufficient risk management framework. By setting out an integrated approach to risk management, this book provides a description of the fundamental components of successful management of business/corporate risks. It describes a wealth of risk management tools and techniques and provides information on the successful delivery of an integrated and enterprise-wide approach to risk management.

The future for risk management

Risk management is changing rapidly, in terms both of the tools and techniques that are applied and the governance structures that are being introduced to ensure successful management of risk. Organizations will always be cost-conscious, but increasing regulation also brings the need for focus on governance, risk and compliance (GRC). GRC represents an approach that is designed to be both efficient and cost effective in terms of the results that are achieved.

With many organizations changing to exploit and adapt to a new digital age, emerging risks have never been more important. For many organizations, it is a challenge to keep their risk exposure within the risk capacity of the organization. Events can occur that could be devastating for the organization. In these circumstances, organizations need to pay more attention to an analysis of the triggers that could result in significant risks materializing, as well as developing detailed plans to manage any crisis that does arise.

From a study of this book, the reader will see that risk management has established a body of knowledge, developed a comprehensive set of skills and, through the Institute of Risk Management, formed an educational and training body that can

assess both and ensure competence. All of these point to risk management taking on professional status. The future risk manager will have a firm grasp of the fundamentals described in this book, but will also find that this remains a young profession where there is scope for developing more and better ways to manage risk. They will find there is room to develop the use of digital analysis to exploit opportunities better and use risk management techniques to increase the chances of success.

Changes for the sixth edition

Risk management continues to be a dynamic and developing discipline and the changes that were necessary in this sixth edition reflect that fact. Written during periods of 'lockdown' in the Covid-19 pandemic, the health crisis has had a bearing on some of the examples provided. More meaningfully, however, the opportunity has been taken to provide examples of risk management activity when new digital techniques are available and applied, for example the use of 'crowd sourcing' techniques and other uses of technologies in developing risk registers.

Certain types of risk have increased dramatically, and the need for a robust ERM initiative to be adopted by organizations has never been greater. Risks that have increased considerably since the fifth edition of this book include the impact of climate change, global migrations, economic disruption caused by technology, and the increasingly sophisticated levels of cyber crime, particularly ransomware.

The book remains substantially in the same form as the fifth edition. Part One has expanded to include discussion of risk management standards and context so that Part Two can concentrate on enterprise risk management as a separate topic. New chapters have been provided for implementing ERM, setting objectives and considering how ERM adds value.

One of the important considerations in producing this edition was to remain closely aligned to the structure of the Institute of Risk Management (IRM) International Certificate in Enterprise Risk Management. Accordingly, the first four parts of the textbook are concerned with the basic principles of risk and risk management. Parts Five through to Eight are concerned with the practice of risk management and include consideration of risk strategy, culture, governance and assurance.

PART ONE

Introduction to risk management

LEARNING OUTCOMES

Having studied this section readers will be able to:

- Summarize the origins and development of the discipline of risk management, including the various specialist areas and approaches.
- Produce and articulate a range of established definitions of risk and risk management, and describe the efficacy of these definitions.
- Identify the characteristics of a risk in order to provide a full risk description and justify the inclusion of each item.
- Summarize the options for the attachment of risks to various characteristics of an organization and describe the advantages of each approach.
- Identify the features of compliance risks, hazard risks, control risks and opportunity risks.
- Explain the characteristics and benefits of enterprise risk management.
- Summarize the principles (proportionate, aligned, comprehensive, embedded and dynamic) and aims of risk management and its importance to strategy, tactics, operations and compliance.
- Describe the key outputs of risk management in terms of mandatory obligations, assurance, decision making and effective and efficient core processes.

- State the key features of the best-established risk management standards, including ISO 31000, the COSO ERM cube and the IRM standard.
- Describe the scope and importance of establishing the context as the first stage in the risk management process.
- Explain the importance of the relationship between the external context, internal context and the risk management context.
- Describe the key stages in the risk management process and the main components of a risk management framework.

Further reading

- Bernstein, P (1998) *Against the Gods: The remarkable story of risk*, Wiley, Hoboken, NJ
- Grenfell Tower Inquiry (2019) Phase 1 report, www.grenfelltowerinquiry.org.uk/phase-1-report
- Institute of Risk Management (2010) *A Structured Approach to Enterprise Risk Management (ERM) and the Requirements of ISO 31000*, IRM, London
- ISO (2009) *ISO Guide 73:2009 Risk Management – Vocabulary*, www.iso.org/standard/44651.html
- ISO (2018) *International Standard ISO 31000:2018 Risk Management – Guidelines*, www.iso.org/standard/65694.html
- Kloman, F (2009) A short history of risk management, Risk Journal, <https://riskjournal.blogspot.com/2009/02/short-history-of-risk-management.html>
- Pullan, P and Murray-Webster, R (2011) *A Short Guide to Facilitating Risk Management*, Gower Publishing, Aldershot

CASE STUDIES

The reader can review the following examples to illustrate further the areas discussed in Part One and throughout this book.

Ocado: Risk management process

Ocado is a delivery only internet-based grocery company based in the UK which also sells the intellectual property it has derived from its innovative software to other grocery companies, predominantly outside the UK. The Group's annual report and accounts discuss risks, strategy, stakeholders, ethics and compliance, all of which form part of the

discussion in this book. It provides a clear discussion of how their world of grocery retail is changing with digital enhancements.

The outline of their risk management framework states:

Ocado's risk management process is designed to improve the likelihood of delivering our business objectives, protect the interests of our key stakeholders, enhance the quality of our decision making, and assist in the safeguarding of our assets, including people, finances, property and reputation.

They further clarify that 'The Board is responsible for the review and approval of the risk management framework and for the identification of Ocado's key strategic and emerging risks.'

They explain that their risk management process:

is designed to identify key risks and to provide assurance that these risks are understood and managed in line with the agreed risk appetite. The risk appetite is reviewed by the Board as part of its annual strategy review. The risk management process is aligned to our strategy and each principal risk and uncertainty is considered in the context of how it relates to the achievement of the Group's strategic objectives.

The main significant risks they identify in this report include:

- the impact of Covid-19 on the Group;
- UK withdrawal from the European Union;
- technology;
- emerging risk such as climate change and the impact of this on our business.

Edited extracts from: Ocado Group plc (2020) Reimagining Shopping: Annual Report and Accounts for the 52 weeks ended 29 November 2020, www.ocadogroup.com/investors/annual-report

Lenovo Group: Significant risks and mitigations

Lenovo Group is a Chinese multinational company with global headquarters in Beijing and operational headquarters in the USA. It is listed on the Hong Kong Stock Exchange, and has 63,000 employees. It delivers technology solutions and is worth studying in light of the fast-moving applications it is developing and the environment in which it operates.

The following table is an edited extract of how they communicate through the annual report to discuss the key risks that they consider to be of significance, with some illustrations of the mitigation or controls that they apply.

Table 1.1

Risk description	Key risk mitigations
Business risk Market competition: they operate in 'an industry which faces rapid changes in market trends, consumer preferences and constantly evolving technological advances in hardware performance, software features and functionality'.	In addition to monitoring market trends they discuss their '3S strategy (smart IoT, smart infrastructure and smart verticals) [to] protect and drive profitability'.
Cyber attack and security risk 'The Group may be impacted negatively if it sustains cyber-attacks and other data security breaches that disrupt its operations or damage its reputation.'	They discuss investment in a 'robust cyber security culture, enhanced security controls, compliance with mandatory privacy and security standards imposed by law, regulation, industry standards, or contractual obligations'.
Supply risk They have identified that some 'products may be reliant on a few component suppliers and the suppliers' locations may be concentrated in one country or region within the country'.	They utilize 'cost and operational analysis to understand potential impacts. Ensure broad supplier sourcing and ensure adaptation plans in place'.

Edited extracts from: Lenovo Group Limited (2020) Smarter Technology for All: Lenovo Group Limited 2019/20 annual report, <https://doc.irasia.com/listco/hk/lenovo/annual/2020/ar2020.pdf>

UK Cabinet Office: An essential tool for delivering objectives

The Cabinet Office is the central ministry that brings a unifying focus to UK government activity. They say that 'Risk management is an essential tool used to minimize levels of uncertainty and to maximize the Department's chances of successfully delivering its objectives, helping to inform both operational decision making and strategic planning.'

The publicly available report outlines their 'quarterly performance reporting routine, [where] all business units are required to fill in a Leadership Team Risk Register. This then feeds into a Strategic Risk Register.'

The document states that 'although significant improvements have been recognized across a number of areas, there remains areas for improvement, including:

- Putting in place arrangements for the management of risks with partners, including suppliers, Arms Length Bodies or other Government Departments,
- Increased clarity and governance around key charging models and income recovery,
- Development of a comprehensive Cyber Security Governance structure that covers the entire Cabinet Office'.

Edited extracts from: Cabinet Office (2020) Cabinet Office Annual Report and Account 2019–20, www.gov.uk/government/collections/cabinet-office-annual-reports-and-accounts#annual-report-and-accounts

THIS PAGE IS INTENTIONALLY LEFT BLANK

What risk is and why it is important

01

Whatever we think of as ‘risk’, it is changing in the digital age. Organizations of all types – government, local and health authorities, manufacturers and service providers, financiers and criminals – now use computers and are digitally processing immense amounts of data. Almost half of all households worldwide have a computer at home, and, whilst it is estimated that number is a third of households in developing countries, the impact on everyday lives and activity cannot be underestimated.¹

As our everyday activity is changing, so should our attitude to risk. Mark Zuckerberg famously said that ‘in a world that is changing really quickly, the only strategy that is guaranteed to fail is not taking risks’. In this book the processes to manage risk that have been developed over the last century will be outlined with particular consideration to the changes and disruption brought about by our increased reliance on computing and data analytics.

Definitions of risk

Risk is often perceived as being undesirable: The *Oxford English Dictionary* defines risk in terms of hazard, danger, loss or adverse consequence. If we go back in time to discover the origin of the word ‘hazard’ this probably comes from the Arabic for a dice (al-zahr) and became common in 12th-century Europe when referring to a game of chance, or the throw of a dice. Risk in this sense means the opportunity for gain as well as a threat.

There has been extensive academic discussion as to the concepts of risk and uncertainty. In 1985 Perry and Hayes differentiated the two concepts through measurement where ‘risk is a measurable uncertainty, while uncertainty is an un-measurable risk’.² Another way of looking at it was provided by Flanagan and Norman in 1993, who stated that ‘Uncertainty is a situation where no historical data exists or previous history related to the situation under scrutiny’.³ This is a particularly important concept to bear in mind when seen from the perspective of the 2020s. Our digital age

has seen the generation of, and enabled unrestricted access to, almost unlimited amounts of data when compared to the 1980s.

Definitions of risk can be found from many sources, and some key definitions are set out in Table 1.1. The Institute of Risk Management (IRM) defines risk as the combination of the probability of an event and its consequence. Consequences range from positive to negative. This is a widely applicable and practical definition that can be easily applied.

The international guide to risk-related definitions, ISO Guide 73⁴ and The Institute of Internal Auditors (IIA) define risk as the ‘effect of uncertainty on objectives’. This is neither negative nor positive, and offers a more nuanced view than that of the ‘popular’ or dictionary definition. These definitions are considered in more detail in Chapter 4.

ISO Guide 73 explains that an effect may be positive, negative or a deviation from the expected; these outcomes show risks are opportunities, threats or uncertainties. The guide notes that risk is often described by an event, a change in circumstances, a consequence, or a combination of these, and how they may affect the achievement of objectives.

Different disciplines define the term risk in very different ways. When looking to ‘manage’ risk it is important you, or your organization, choose the definition that is most appropriate. The definition can be as narrow or as comprehensive as you wish.

Risk in an organizational context is usually defined as anything that can impact the fulfilment of the organization’s objectives. For our purposes, it will be important that the organization’s objectives are fully established and agreed.

It is generally accepted that risk is best defined by concentrating on events. This is the route taken in many standards and by the IIA in Table 1.1. The UK Government’s 2020 definition of risk mirrors that of ISO Guide 73.

Table 1.1 Definitions of risk

Organization	Definition
ISO Guide 73	Effect of uncertainty on objectives. Note that an effect may be positive, negative, or a deviation from the expected. Also, risk is often described by an event, a change in circumstances or a consequence.
Institute of Risk Management	Risk is the combination of the probability of an event and its consequence. Consequences can range from positive to negative.

(continued)

Table 1.1 (Continued)

Organization	Definition
Institute of Internal Auditors	The uncertainty of an event occurring that could have an impact on the achievement of the objectives. Risk is measured in terms of consequences and likelihood.
HM Government: The Orange Book. Management of Risk – Principles and Concepts 2020 ¹	The effect of uncertainty on objectives. Risk is usually expressed in terms of causes, potential events, and their consequences.

SOURCE 1 HM Government (2020) *The Orange Book: Management of risk – principles and concepts*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866117/6.6266_HMT_Orange_Book_Update_v6_WEB.PDF

Greater clarity is likely to be brought to the risk management process if the focus is on events or the possibility of an event (which henceforth we shall term ‘events’). For example, consider what events may have an effect on treating patients in a general hospital. These could include power cuts, the absence of qualified doctors, or an infectious disease that transmits to other patients. Having identified these events, the hospital’s management needs to decide what to do to reduce the chances of one of these events causing them to fail to help patients. This analysis by the hospital’s supervisors is an example of risk management in practice.

Types of risks

Risk may have positive or negative outcomes and may be considered to be related to an opportunity or a threat, or simply to uncertainty of outcome for an organization. Every risk has its own characteristics that require particular management or analysis. In this book, risks are divided into four categories:

- compliance (or mandatory) risks;
- hazard (or pure) risks;
- control (or uncertainty) risks;
- opportunity (or speculative) risks.

In general terms, organizations will seek to minimize compliance risks, mitigate hazard risks, manage control risks and embrace opportunity risks. It is important to note that there is no ‘right’ or ‘wrong’ subdivision of risks. Readers will encounter other subdivisions in other texts and these may be equally appropriate. Within this book, for ease of reference we will often use opportunity and threat to describe risks (in line with ISO 31000), unless specifically discussing one of the four types. Risks

can also be described as either pure or speculative. Whatever the theoretical discussions, the most important issue is that an organization adopts the risk classification system that is most suitable for its own circumstances.

Table 1.2 Types of risk

Risk type	Key feature
Compliance risks	The importance of compliance risks should not be underestimated. They are associated with adherence to the law of the country and the regulations that apply to the sector in which you operate. Compliance risk captures the legal and financial penalties for failing to act or acting inappropriately and are especially significant for those business sectors that are heavily regulated. Compliance with mandatory requirements represents a 'licence to operate' and failure to achieve the level of compliance required by the relevant regulator will impact routine business activities. Penalties may be financial but increasingly they are personal to the management involved, such as the Senior Managers and Certification Regime imposed after the global financial crisis by the Financial Conduct Authority in the UK.
Hazard risks	These are associated with a source of potential harm or a situation with the potential to undermine objectives in a negative way. Organizations usually accept some hazard risks but they need to be managed within tolerable levels. Hazard risks are the most common risks associated with operational risk management, including occupational health and safety programmes. A good example of a hazard risk faced by many organizations is that of theft.
Control risks	These are associated with unknown and unexpected events. They are sometimes referred to as uncertainty risks and they can be extremely difficult to quantify. Control risks are frequently associated with new projects where it is known that events will occur, but the precise consequences of those events are difficult to predict and control. Therefore, the approach is based on managing the uncertainties around the timing, eventual cost or delivery of the project.
Opportunity risks	These fall into two camps: the risks associated with taking the opportunity, and the risks of not acting. Although opportunity risks are taken with the intention of obtaining a positive outcome, this is not guaranteed. In the rapidly changing environment caused by the global pandemic, organizations have deliberately taken risks in order to survive. These can be considered as opportunity or speculative risks. Some organizations have altered their business models, for example a farm shop providing new services such as 'click and collect' or delivery services. The purpose has been to take action that involves risk to achieve positive gains or, in extreme cases, survival.

Starting up a company supplying technology to the financial sector

In order to understand the distinction between compliance, hazard, control and opportunity risks, the example of a 'start-up' in the financial sector may be helpful. The company will need to be authorized by the relevant authorities, which in the UK is the Financial Conduct Authority, and the company will need to nominate senior managers to be responsible for its compliance risks. Theft or fraud caused by an employee is an operational or hazard risk. When they design their new software package, control risks will be associated with this project. When released, the software may have the potential to be used by clients in a sector they had not specifically targeted, thereby creating an opportunity risk; the intention is to achieve results by attracting customers, but it is possible that the project will fail to deliver the functionality that was intended. In fact, the failure of the functionality of the new software system may critically undermine the operations of the organization.

Risk description

In order to fully appreciate a risk, a detailed description is necessary so that a common understanding of the risk can be identified and ownership/responsibilities may be clearly established. To determine the correct range of information to collect about each risk, the distinction between compliance, hazard, control and opportunity risks needs to be clearly understood. This is discussed in Chapter 11.

Levels of risk

It is important to understand the level of risk that has been identified if no controls are in place:

- **Inherent level of risk:** The level of risk before any actions have been taken to change the likelihood or magnitude of the risk.
- **Current or residual level of risk:** The level of risk after initial control measures have been put in place.
- **Target level of risk:** The level of risk that is desired or will be obtained with the application of further control measures.

Although there are advantages in identifying the inherent level of risk, there are practical difficulties in doing so with some types of risks.

Identifying the inherent and current level of the risk makes it possible to identify the importance of the control measures in place. Often, a risk matrix is used to show the inherent level of the risk in terms of likelihood and magnitude. The current or residual level of the risk can then be identified, and the effort that is required to reduce the risk from its inherent level to its current level can be clearly indicated on the risk matrix.

Terminology varies, and the inherent level of risk is sometimes referred to as the ‘gross’ or absolute risk. The current or residual level of risk is sometimes referred to as the ‘net’ or the managed level of risk. The example in the box below provides an example of how inherently high-risk activities are reduced to a lower level of risk by the application of sensible and practical risk response options.

Crossing the road

Crossing a busy road would be inherently dangerous if there were no controls in place and many more accidents would occur. The risk is inherently dangerous, so attention is paid to controls that manage the risk: Pedestrians do not cross the road without looking out for traffic, and drivers are always aware that pedestrians may step into the road. Controls include pedestrian crossings, traffic calming measures and speed cameras or signals to reduce the speed of vehicles.

Classification systems

Risks can be classified according to the nature of the attributes of the risk. These can be:

- timescale – both at impact and after the event;
- source of the risk, for example counterparty or credit risk;
- nature of the impact and/or likely magnitude of the risk;
- component or feature that will be impacted (eg risks can impact people, premises, processes or products).

Individual organizations will decide on the risk classification system that is most relevant to their activity and which suits them best, depending on the nature of the organization and its activities. Also, many risk management standards and frameworks suggest a specific risk classification system. If the organization adopts one of these standards, then it will tend to follow the classification system recommended. There is no universal classification system that fulfils the requirements of all organizations. It

is likely that each risk will need to be classified in several ways in order to clearly understand its potential impact. However, many classification systems offer common or similar structures, as described in Chapter 11.

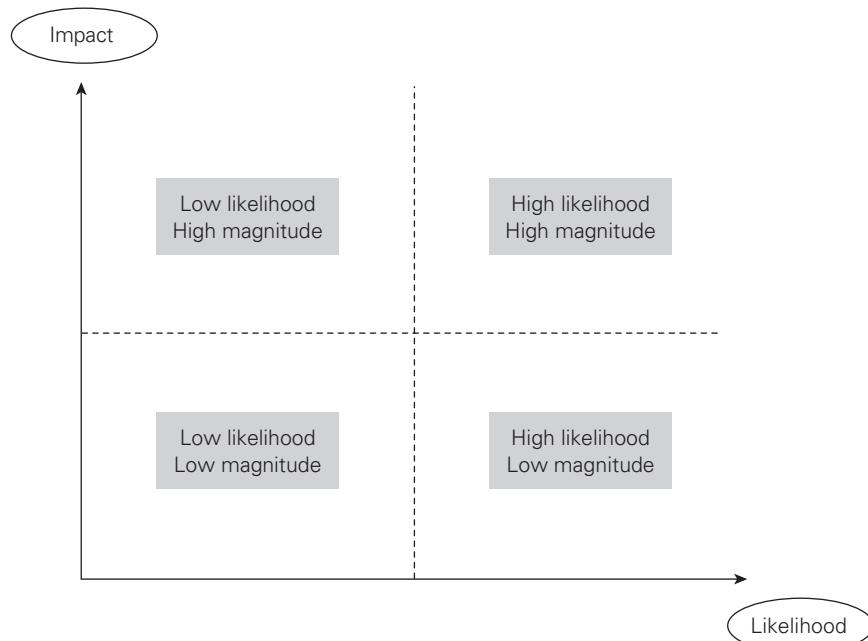
Risk likelihood and impact

Risk likelihood and impact (or magnitude) are best demonstrated using a risk matrix. This is a fundamentally important risk management tool and can be produced in many formats. Whatever format is used, the basic style plots the likelihood of an event against the impact (or magnitude) should the event materialize.

Figure 1.1 is an illustration of a simple risk matrix, also referred to as a risk map or heat map. This is a commonly used format. The risk matrix can be used to plot the nature of individual risks, so that the organization can decide whether the risk is acceptable and within the risk appetite and/or risk capacity of the organization.

Throughout this book, a standard format for presenting a risk matrix has been adopted. The horizontal axis is used to represent likelihood. This term is used rather than frequency, which can imply an event will definitely occur. Likelihood refers to

Figure 1.1 Risk likelihood and impact



the chances of an event happening. However, in risk management literature, the word ‘probability’ will often be used to describe the likelihood of a risk materializing.

The vertical axis is used to indicate impact in Figure 1.1. This term embraces compliance, hazard, control and opportunity risks. The magnitude of the risk may be considered to be its gross or inherent level before controls are applied.

Figure 1.1 plots likelihood against the impact of an event. The important consideration for risk managers is the consequences that follow. For example, a large fire could occur that completely destroys a warehouse of a distribution and logistics company. Although the magnitude of the event may be large, if sufficient insurance is in place, the impact in terms of financial costs for the company could be minimal; the impact on management time, lost reputation and potential future sales cannot be recovered but if the company has effective business continuity plans to cope with such an event, the consequences for the overall business may be much less than would otherwise be anticipated.

The risk matrix is used throughout this book to provide a visual representation of risks. It can also be used to indicate the likely risk control mechanisms that can be applied. The risk matrix can also be used to record the inherent, current (or residual) and target levels of the risk.

Shading or colour coding is often used on the risk matrix to provide a visual representation of the importance of each risk under consideration. As risks move towards the top right-hand corner of the risk matrix, they become more likely and have a greater impact. Therefore, the risk becomes more important and immediate and effective risk control measures need to be in place.

Why understanding risk is important

Following the Covid-19 pandemic, many organizations took a greater interest and a proactive approach to risk and risk management. It is increasingly understood that the explicit and structured management of risks brings benefits. Organizations that manage risks will be able to achieve the following four areas of improvement, which are abbreviated as STOC throughout this book:

- **Strategy:** Because the risks associated with different strategic options will be fully analysed, better strategic decisions will be reached.
- **Tactics:** Because consideration will have been given to selection of the tactics and the associated risks involved, available alternatives can be evaluated.
- **Operations:** Because events that can cause disruption will be identified in advance and actions taken to reduce their likelihood of occurring, the damage caused by these events will be limited and the costs contained.

- **Compliance:** This will be enhanced because the risks associated with failure to achieve compliance with statutory and customer obligations will be addressed.

It is undesirable for organizations to find themselves in a position whereby unexpected events cause disruption to normal operations. Stakeholders expect that organizations be resilient and take full account of the risks that may cause operational, project or strategic issues.

The exposure presented by an individual risk can be defined in terms of the likelihood of the risk materializing and the impact of the risk when it does materialize. As risk exposure increases, the likely impact will also increase. ISO Guide 73 refers to this measurement of likelihood and impact (or magnitude) as being the current or residual (or retained) ‘level of risk’. This level of risk should be compared with the risk attitude (according to ISO Guide 73 – the organization’s approach to assess and eventually pursue, retain, take or turn away from risk) and risk appetite (according to ISO Guide 73 – the amount and type of risk that an organization is willing to pursue or retain) of the organization for risks of that type. The risk appetite will sometimes be described as a set of risk criteria.

The term ‘impact’ is used to define how the event affects the finances, infrastructure, reputation and/or marketplace (FIRM) of the organization. This use of terminology is also consistent with the use of impact in business continuity planning evaluations. This is a measure of the risk at the current level. The term ‘consequences’ is used in this book to indicate the extent to which the event results in a change in the planned achievement of effective and efficient strategy, tactics, operations and compliance (STOC).

Impact of hazard risks

Risk management has its longest history and earliest origins in the management of hazard risks. Hazard risks undermine objectives, and the level of impact of such risks is a measure of their significance. Hazard risks are often insurable as they can only have a negative outcome.

Hazard risk management is concerned with issues such as health and safety at work, fire prevention and avoiding the consequences of defective products. Hazard risks can cause disruption to normal operations, as well as resulting in increased costs and poor publicity associated with disruptive events.

Hazard risks are related to business dependencies, including IT and other supporting services. The increased dependence on IT systems in most organizations means hazards such as virus infection, deliberate hacking or denial of service attacks assume a high degree of significance.

Terminology is important. If a hazard risk materializes, it may have a very large impact. For example, a fire could destroy the main distribution warehouse of an

organization, but the risks can be reduced by putting in place controls to minimize financial impact (by insurance) or reduce the extent of damage to reputation (through crisis management).

Attachment of risks

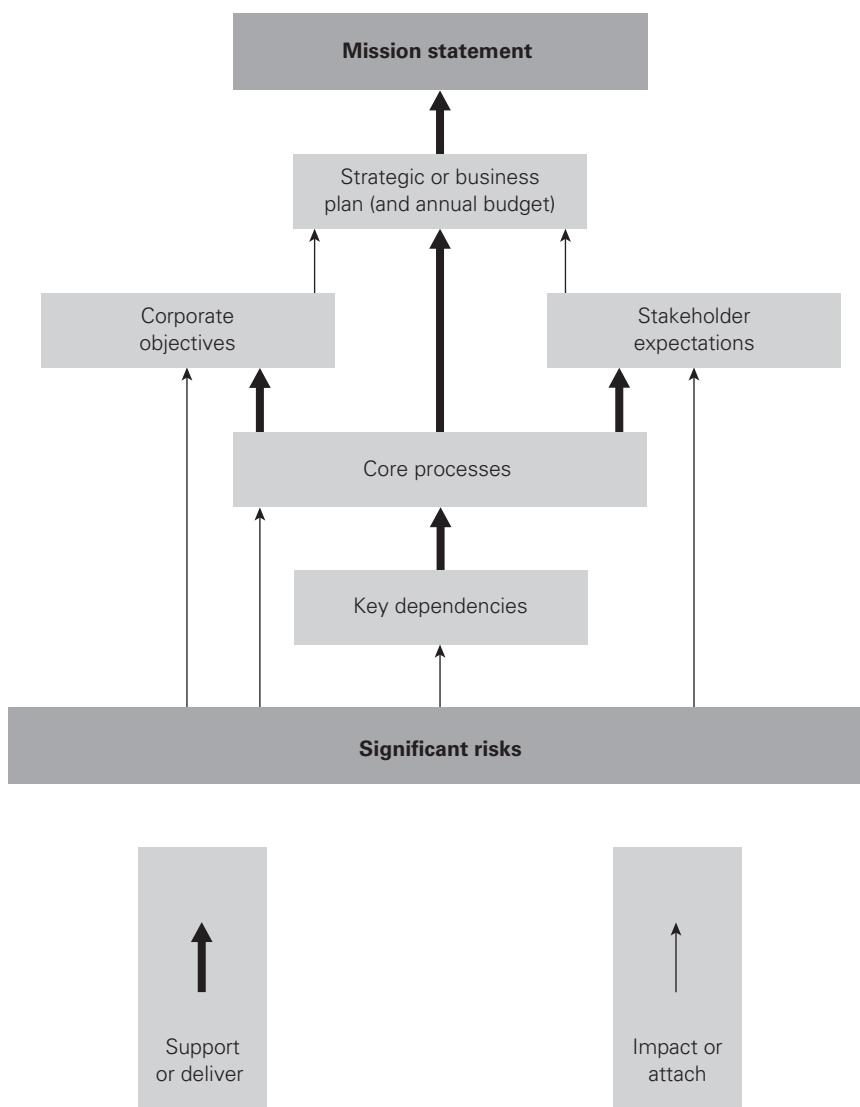
Although most standard definitions refer to risks as being attached to corporate objectives, Figure 1.2 provides an illustration of the options for the attachment of risks. Risks are shown in the diagram as being capable of impacting the key dependencies that deliver the core processes of the organization. Corporate objectives and stakeholder expectations help define the core processes of the organization. These core processes are key components of the existing nature and future enhancement of the business model and can relate to operations, tactics and corporate strategy, as well as compliance activities, as considered further in Chapter 20.

The intention of Figure 1.2 is to demonstrate that significant risks can be attached to aspects of the organization other than corporate objectives. Significant risks can be identified by considering the key dependencies of the organization, the corporate objectives and/or the stakeholder expectations, as well as by analysis of the core processes of the organization. For example, Arcadia, a clothes retailer in the UK, failed in 2020 because they had underinvested in online retailing and were unable to effectively maintain business operations (their core operations) when the Covid-19 pandemic disrupted their business model. The risk of underinvestment was magnified by the impact of the pandemic, which drove customers to online channels.

Another way of viewing the concept of attachment of risks is to consider as alternative starting points for undertaking a risk assessment those features shown in Figure 1.2. For example, a risk assessment can be undertaken by asking ‘What do stakeholders expect of us?’ and ‘What risks could impact the delivery of those stakeholder expectations?’

One of the standard definitions of risk is that it is something that can impact (undermine, enhance or cause doubt about) the achievement of corporate objectives. This is a suitable definition, but to be useful the objectives should be presented as a full statement of the short-, medium- and long-term aims of the organization. Not only do the objectives need to be challenged to ensure that they are full and complete, but the assumptions that underpin the objectives should also receive careful and critical attention.

The ‘objectives-driven’ approach enables the analysis of the positive and uncertain aspects of events as well as the negative and compliance aspects. A drawback of reliance on using objectives is that they may fail to fully identify the strategic (or leadership), operational (or efficiency) and change (or competition) requirements of the organization. There is a danger of considering risks out of the context that gave

Figure 1.2 Attachment of risks

rise to them if relying purely on this method, and a more robust analysis may be achieved when a ‘dependencies-driven’ approach to risk management is adopted.

Attachment of risks to key dependencies and, especially, stakeholder expectations is becoming more common. The importance of stakeholders and their expectations is considered in more detail in Chapter 30. The organization will need to ask what features or components are key to success. This will result in the identification of the strengths, weaknesses, opportunities and threats facing the organization. This is often referred to as a SWOT analysis. Having identified key dependencies, the organization can then

consider the risks that will impact these dependencies. This approach is discussed in more detail with practical examples of risks provided in Tables 13.1 and 15.2.

Core processes are discussed in Chapter 20 and may be considered as the high-level processes that drive the organization. Risks may be attached to core processes, as well as being attached to objectives and/or key dependencies. Core processes can be classified as strategic, tactical, operational and compliance (STOC). In all cases, the core processes need to be effective and efficient. Mature (or sophisticated) risk management activities can then be designed to enhance the effectiveness and efficiency of core processes.

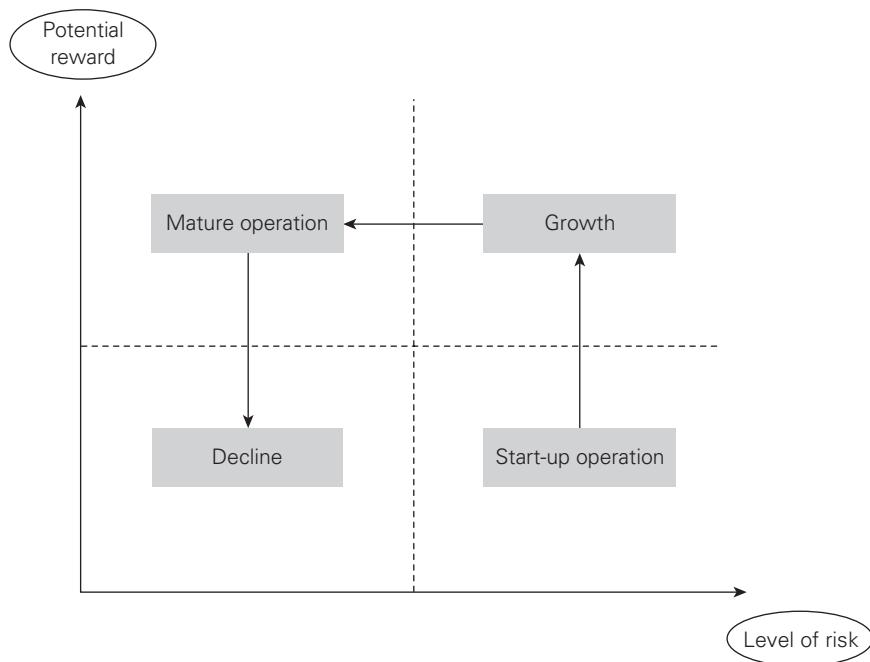
Risk and reward

Building on the opening to this chapter, risk can be desirable and deliver benefits or rewards. A business will launch a new product because it sees opportunities from the successful marketing of that product. In undertaking the launch, the organization will allocate resources which may be wasted if the launch is not successful. These resources represent the value at risk and need to be within the risk appetite of the organization.

When an organization puts value at risk in this way, it should do so with the full knowledge of the risk to which the organization is becoming exposed. Even more importantly, it should ensure that it has sufficient resources to cover the exposure. In other words, the exposure should be quantified, the appetite to take that level of risk should be confirmed, and the capacity of the organization to withstand any foreseeable adverse consequences should be clearly established (in other words, effective resilience).

The digital age has disrupted the traditional lifecycle of product launches. There is now a continuous need to innovate and develop new products from the new opportunities presented by the digital age of data and enhanced processing power. This trend explains, in part, the enhanced need for risk management as the rewards from exploiting digital powers are many multiples of ‘analogue’ solutions. This means that the traditional lifecycle of a product or service may be faster than before digital disruption but it is useful to analyse the cycles that products undergo. These can be seen in a typical maturity cycle described in Figure 1.3. Appropriate risk management techniques are needed when considering the opportunities that will arise from new products. The nature of these risk responses and the nature of their impact are considered in Part Four of this book.

Risk management effort should produce rewards. In the case of hazard risks, that reward will be fewer disruptive events in future. In the case of project risks, the reward for increased risk management effort will be that the project is more likely to be delivered on time, within budget and to specification/quality.

Figure 1.3 Risk and reward

For opportunity risks, risk management should result in a higher rate of successful new products launches or (at worst) a lower level of loss for all new activities or new products. In all cases, profit or enhanced level of service is the reward for taking risk. The concept of the risk versus reward analysis in relation to strategic risks is considered in more detail in Figure 15.2.

Attitudes to risk

Different organizations will have different attitudes to risk. However, risk attitude is the organization's approach to assess, pursue, retain or avoid risks.⁵ Some organizations may be considered to be risk averse, whilst others will be risk aggressive. The attitude of the organization to risk will depend on the attitude of the board, the nature of the sector and the marketplace within which it operates.

Risks need to be considered inside the context that gave rise to them. An organization may appear to be risk aggressive about an opportunity the board has decided should not be missed. The particular opportunity needs to have been fully considered for the organization to evaluate that risk correctly.

One of the major contributions from successful risk management is to ensure that strategic decisions that appear to be high risk are taken on an informed basis.

Improvement in the robustness of decision-making activities is one of the key benefits of risk management. Attitude to risk is a complex subject and is closely related to the risk appetite of the organization, but they are not the same. Risk *attitude* indicates the way the organization perceives the likelihood and impact of uncertainty (including what it can do about the uncertainty). Risk *appetite* indicates the amount of risk an organization is willing to seek or accept in pursuit of its long-term objectives.

Risk and triggers

Risk is sometimes defined as uncertainty of outcomes and this is particularly applicable to the management of control risks. Control risks are the most difficult to identify and define, but are often associated with projects. The overall intention of a project is to deliver the desired outcomes on time, within budget and to specification, quality or performance.

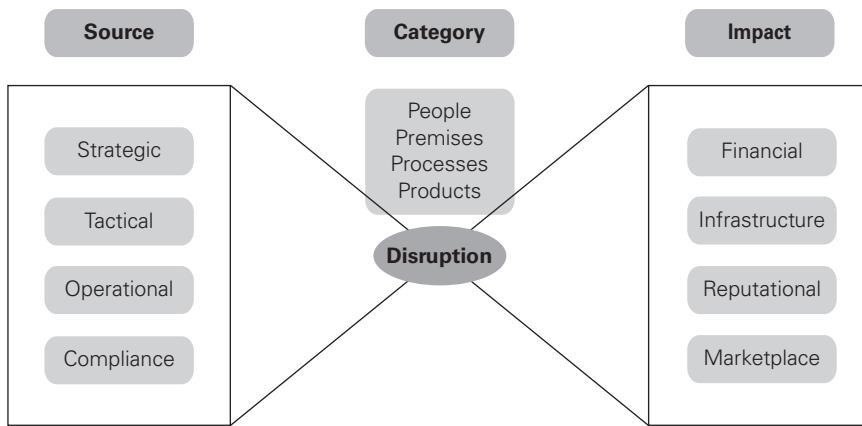
For example, when a building is being constructed, the nature of the ground conditions may not always be known in detail. As the construction work proceeds, more information will be available about the nature of the conditions. This information may be positive news that the ground is stronger than expected and less foundation work is required. Alternatively, it may be discovered that the ground is contaminated or is weaker than expected or that there are other potentially adverse circumstances, such as archaeological remains being discovered.

Given this uncertainty, these risks should be considered to be control risks and the overall management of the project should take account of the uncertainty associated with these different types of risk. It would be unrealistic for the project manager to assume that only adverse aspects of the ground conditions will be discovered. Likewise, it would be unwise for the project manager to assume that conditions will be better than expected, just because they want that to be the case.

Because control risks cause uncertainty, organizations need to manage the potential variability in outcomes. A certain level of deviation from the project plan can be tolerated, but it must not be too great.

Ways of representing the risk management process to make it more accessible to managers and other stakeholders are constantly being developed. One of these tools is the ‘bow-tie’, which is used several times throughout this book. Figure 1.4 shows a simple representation of the bow-tie which in this case is applicable to events that can cause disruption to normal efficient operations, although the concept can be used for all risks.

The left-hand side of the bow-tie represents the source of a particular hazard and will indicate the classification system used by the organization for sources of risk. In Figure 1.4, the sources of risk used are the high-level sources of strategic, tactical, operational and compliance risks. The right-hand side of the bow-tie sets out the

Figure 1.4 Risks and the bow-tie

impact should the risk occur using the high-level components of financial, infrastructure, reputational and marketplace.

In the centre of the bow-tie is the risk. Table 2.2 indicates the categories of disruption that can affect organizations, and the same categories of people, premises, processes and products are used here. The purpose of using the bow-tie illustration is to demonstrate the risk classification systems used by the organization and the potential range of impacts should a risk materialize. Controls can be put in place to optimize the risk occurring (preventing downside or, if it's an opportunity, controls can make it more likely to happen and impact bigger) and these can be represented by vertical lines on the left-hand side of the bow-tie. In a similar manner, recovery controls can be represented on the right-hand side of the bow-tie.

Use of the bow-tie has become widespread, especially in the public sector. The box below provides a practical application of the bow-tie to the identification of preventive and response controls related to a fire in the kitchen of a residential home.

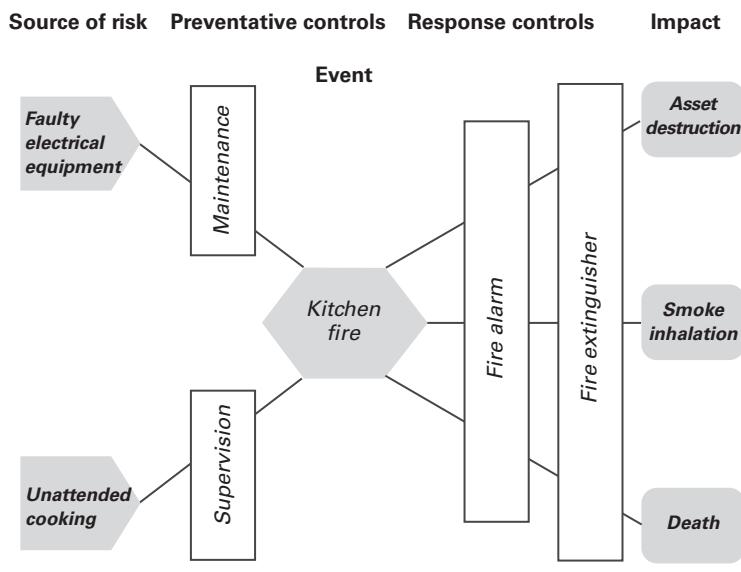
Risk management and the bow-tie

There are various risk analysis techniques available. The most popular method of analysing a risk is using a bow-tie.

A bow-tie is a simple way of analysing a risk to gain a greater understanding. The first stage is to put the risk description into the middle box. The causes of the risk then need to be recorded along with factors to influence its impact. This can be

either preventive controls to minimize a threat or actions to optimize an opportunity. A hazard is used as an example in the figure below. The impact of the risk is also considered. This enables the identification of response controls to lessen the impact of the risk, should it occur.

Figure U1.1



Notes

- 1 Statista (2021) Share of households with a computer at home worldwide from 2005 to 2019, www.statista.com/statistics/748551/worldwide-households-with-computer (archived at <https://perma.cc/R4HE-UM2J>)
- 2 Perry, JG and Hayes, RW (1985) Risk and its management in construction projects, *Proceedings of the Institution of Civil Engineers*, 78 (3), pp 499–521.
- 3 Flanagan, R and Norman, G (1993) *Risk Management and Construction*, Wiley-Blackwell, Oxford.
- 4 ISO (2009) *ISO Guide 73:2009 Risk Management – Vocabulary*, <https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en> (archived at <https://perma.cc/8J9B-N2NW>)
- 5 ISO (2009) *ISO Guide 73:2009 Risk Management – Vocabulary*, <https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en> (archived at <https://perma.cc/8J9B-N2NW>)

Risk is an opportunity as well as a threat

02

The practice of risk management considers all facets of risk but stands out from the popular view of risk as purely a threat by seeking to embrace the opportunities that risk management offers. In this chapter we will consider the four types of risk but emphasize that managing opportunity risk will be of key importance in the future.

In the previous chapter the aspect of uncertainty, measurement and use of historical data was observed. Risk management in the digital age will be more concerned with opportunities than it has ever before. This is because of the wealth of data analytics that will enable greater certainty to be brought to decision making. Risk managers will be required to inform the strategy of organizations to a much greater degree than in the past and, armed with the tools of risk management outlined in this book, should be able to support better-informed decision making about these opportunities.

Four types of risk

Chapter 1 states that risks can be divided into four categories and definitions of these four types of risk are also given in Appendix B. They are:

- compliance risks;
- hazard risks;
- control risks;
- opportunity risks.

A common language of risk is required throughout an organization if the contribution of risk management is to be maximized. The use of a common language will also enable the organization to develop an agreed perception of risk and attitude to risk. Part of developing this common language and perception of risk is to agree a risk classification system or series of such systems.

For example, when reviewing your financial position, the key dependencies will relate to achieving adequate income and managing expenditure. The review should include an analysis of the risks to job security and pension arrangements, as well as property ownership and other investments. This part of the analysis will provide information on the risks to income and the nature of those risks (opportunity risks).

As a practical example of the nature of compliance, hazard, control and opportunity risks, Table 2.1 considers the risks associated with owning a car. In this case, the compliance risks relate to the legal obligations associated with owning and driving a car. The hazard risks relate to events that the owner does not want to occur. Control risks will be the uncertain costs that are known but may vary. Finally, the opportunities are the benefits that car ownership offers.

Table 2.1 Risks associated with owning a car

Compliance requirements of owning a car (events that could result in regulatory enforcement)	
1	Insufficient and/or inadequate third-party car insurance
2	Inattentive or aggressive driving results in traffic offence(s)
3	Tyres in poor condition and other maintenance obligations
Hazards of owning a car (events that you do not want to happen and that can only be negative)	
1	You pay too much for the car or it is in poor condition
2	You are involved in a collision or road accident
3	The car gets stolen or vindictively damaged
Uncertainties of owning a car (control risks) (events that you know will happen, but impacts are variable)	
1	Cost of borrowing money to buy the car could change
2	Price of fuel (petrol or diesel) could go up or down
3	Maintenance, breakdown and repair costs will vary
Opportunities of owning a car (events you hope will happen, but could fail to occur)	
1	You can travel more easily than depending on others or using public transport
2	Enhanced job opportunities because you will be more mobile
3	Save money on other forms of public transport

Compliance risks are often considered a separate category of risk and they are often managed or minimized differently. For highly regulated industries, such as energy, finance, gambling and transportation, compliance issues are very important. The amount of regulation has grown substantially in recent years and in certain industries this is becoming a business imperative. Continued operation often depends upon full compliance with all rules and regulations, and organizations will have zero tolerance for risk in this category. This may be possible for compliance risks, but is almost certainly not going to be the case for hazard, control and opportunity risks. Further consideration of compliance risks is included in Chapter 20, as part of the discussion of STOC risks.

Hazard risks can only inhibit achievement of corporate objectives. Typically, these are insurable-type risks or perils, and will include fire, storm, flood, injury and so on. The discipline of risk management originated in the control and mitigation of hazard risks but has expanded to embrace the other types of risk. Normal efficient operations may be disrupted by loss, damage, breakdown, theft and other threats associated with a wide range of dependencies. Table 2.2 gives examples of disruption caused by people, premises, processes and products (4Ps). These dependencies can also be sources of risk and the 4Ps can be considered to be an example of a risk classification system.

Control risks should not be confused with risk controls or ‘internal controls’. This classification is for risks that cause doubt about the ability to achieve the organization’s mission. Internal financial control protocols are a good example of a response to a control risk. If the control protocols are removed, there is no way of being certain about what will happen. Control risks are associated with uncertainty, and examples include the output achieved from a wind turbine generator or extraction of minerals from an ore body. They are usually dependent on the management of people and monitoring of processes to minimize or mitigate variation from budget. Although most organizations ensure that control risks are carefully managed, they may, nevertheless, remain potentially significant.

Opportunity risks are the risks that are (usually) deliberately sought or embraced by the organization. These risks arise because the organization is seeking to enhance the achievement of the mission, although they might inhibit the organization if the outcome is adverse. This is the most important type of risk for the future long-term success of any organization.

Many organizations are willing to invest in high-risk business strategies in anticipation of a high profit or return. These organizations may be considered to have a large appetite for opportunity investment. Often, the same organization will have the opposite approach to hazard risks and have a small hazard tolerance. This may be appropriate, because the attitude of the organization may be that it does not want hazard-related risks consuming the resources of the organization when it is putting so much value at risk investing in opportunities.

Timescale of risk impact

Risks can be considered as having long-, medium- and short-term impacts, which is a very useful means of analysing the risk exposure of an organization. These risks will be related to the strategy, tactics and operations of the organization, respectively. In this context, risks may be considered as related to events, changes in circumstances, actions or decisions.

In general terms, long-term risks will impact over years, perhaps up to five years, after the event occurs or the decision is taken. Long-term risks therefore relate to strategic decisions. When a decision is taken to launch a new product, the result of that decision (and the success of the product itself) may not be fully apparent for some time.

Medium-term risks have their impact some time after the event occurs or the decision is taken, and typically this will be about a year later. Medium-term risks are often associated with projects or programmes of work. For example, if a new computer software system is to be installed, then the choice of computer system is a long-term or strategic decision. However, decisions regarding the project to implement the new software will be medium-term decisions with medium-term risks attached.

Short-term risks have their impact immediately after the event occurs. Accidents at work, traffic accidents, fire and theft are all short-term risks that have an immediate impact and immediate consequences as soon as the event has occurred. These short-term risks cause immediate disruption to normal efficient operations and are probably the easiest types of risks to identify and manage or mitigate. Short-term risks are quite often insurable, although the exact timing and impact of the insured events is uncertain. In the case of insurable risks, the nature and consequences of the event may be understood, but the timing of the event is unpredictable. In fact, whether the event will occur at all is not known at the time the insurance policy is taken out.

By way of example, consider the operation of a new computer software system in more detail. The organization will install the new software in anticipation of gaining efficiency and greater functionality. The decision to install new software and the choice of the software involve opportunity risks. The installation will require a project, and certain risks will be involved in that. The risks associated with the project are control risks, including the possibility it may not deliver all of the functionality required. After the new software has been installed it will be exposed to hazard risks; for example, the software might be exposed to virus infection or the organization increase its exposure to ransomware due to its reliance on the system. If rules on privacy such as General Data Protection Regulation (GDPR) are breached, this will be a compliance risk.

In this example, each class of risks identified could materialize at different times. It is necessary to consider the circumstances in which one or more of the significant risk events may be triggered. The question of what would trigger such an event requires as much consideration as the source of the risk and the nature of the event if it were to happen.

The box below considers the event that triggered the Grenfell Tower fire in London in 2017.

Triggering major crises

The fire in the 24-storey Grenfell Tower block of flats in North Kensington caused 72 deaths and a further 70 serious injuries. It was the worst UK residential fire since the Second World War. The immediate cause was an electrical fault in a fridge freezer in a domestic flat. The reason that the failure of a common domestic appliance had such disastrous consequences, however, seems to have been the result of a series of poor decisions by the council owners, contractors, designers and suppliers who, intentionally or not, allowed a dangerous form of flammable cladding to be wrapped around the building in 2016. This cladding appears to have been the reason for the rapid and catastrophic spread of the fire. Fire and building controls appear not to have kept pace with developments in refurbishing tower blocks.

At the time of writing, a public inquiry is yet to finalize its report but the reader might wish to consider what action or connected series of actions caused such an appalling loss of life and over what timescale the trigger mechanism operated.

Would it have been the fridge freezer, the owners of the property who commissioned the work, the designers of the work, the contractors installing the flammable cladding, or indeed the fire brigade, who were unaware that the work had overridden the 'stay in place' protocol agreed previously?

For the risk manager it is important to be aware that previous fires had occurred in very similar circumstances in 2009 in London and in 2015 in Dubai. It is also well known amongst industry experts that cladding will alter the fire load of buildings. Data on the risks of flammable cladding was readily available to those who were prepared to look for it. The disaster required a number of failures to take place and it seems to have had multiple causes but there appears to have been no overriding authority that managed these risks.

For more information see www.grenfelltowerinquiry.org.uk

Minimize compliance risks

Organizations will be aware of the wide range of compliance requirements that they have to fulfil. These compliance requirements vary considerably between business sectors and many sectors are highly regulated, with their own dedicated regulator for the industry or sector. Regulation of sectors is increasing. For example, organizations operating in the gambling or gaming industry have significant regulatory requirements placed

on them in most countries in the world. Failure to comply with regulatory requirements may result in the 'licence to operate' being withdrawn by the regulator. If a regulator were to take this extreme action, the organization could ultimately cease to exist.

Organizations that handle financial transactions are required to introduce procedures to reduce the chances of money-laundering activities being undertaken. Banks and other organizations that handle significant amounts of cash need to introduce money-laundering arrangements and, in many cases, a dedicated money-laundering senior executive.

In the insurance industry, compliance issues are significant and can be complex. If an insurance policy is issued in one country to protect the assets and/or cover the liabilities in other countries, compliance issues present particular difficulties. Failure to comply with all obligations may result in insurance claims not being paid or, in the extreme, being illegal in a particular country, if an unauthorized type of insurance or illegal insurance policies have been issued.

For organizations that do not have regulators dedicated to that industry or business sector, there are still a wide range of regulatory requirements that must be fulfilled. In particular, health and safety requirements exist in most countries in the world, and these place obligations on organizations to ensure the health, safety and welfare of employees and other persons who may be affected by their work activities. Typically, these safety requirements apply not only to the place of work under the direct control of the organization, but will extend to the health and safety of employees working in other countries. Also, detailed road safety obligations will apply to organizations that own vehicles, especially if they are engaged in the transportation of people or dangerous goods.

Generally speaking, organizations will work towards ensuring full compliance with all applicable rules and regulations, and thereby minimize the compliance risks. In many cases, dedicated teams of specialist risk professionals will be employed and this is particularly the case in relation to health and safety, money laundering and security arrangements. It is important for organizations to recognize their compliance risks and include consideration of these risks in their risk management activities. It is also important to ensure that the various areas of risk management expertise within the company co-operate with each other, so that an organized and/or co-ordinated approach to compliance is achieved.

Mitigate hazard risks

In general, organizations will tolerate some level of hazard risk exposure. This is because it is unlikely to be appropriate or cost effective to minimize hazard risks completely and mitigating factors will limit exposure to tolerable levels.

In the case of health and safety risks, however, organizations should be much less tolerant and they should take all appropriate actions to eliminate the risks. In

practice, it will not be possible to completely eliminate risk but organizations should minimize safety risks to the lowest level that is cost effective and in compliance with the law. This will need to be considered in the context of the organizational environment and with the full awareness of the board. For example, an automatic braking system fitted to trains to stop them passing through red lights is technically feasible. However, this may be seen to represent an unreasonable investment for the train operating company in the context of its operating licence. The consequences of trains going through red lights may be regarded as the risk exposure or hazard tolerance of the organization but the cost of introducing the automatic braking system may be considered to be prohibitively high and disproportionate to the level of risk. This will need to be constantly reviewed in light of the perception of the consequences which brings the risk attitude into play from the previous chapter.

A less emotive example is related to theft. Most organizations will suffer a low level of petty theft and this may be tolerable. For example, businesses based in an office environment will suffer some theft of stationery, including paper, envelopes and pens. The cost of eliminating this petty theft may be very large and so it becomes cost effective for the organization to accept that these losses will occur. The approach to theft in shops may be very different in different retail sectors, as illustrated by the example below.

Shop security standards

A security-conscious jewellery shop may only allow customers into the shop one at a time. They will be recorded on CCTV as they wait to enter. Items will be held securely, and customers will need to ask to see specific items under the watchful eye of shop assistants. Of course, some customers may be put off, but equally the shop will suffer negligible rates of shoplifting.

Contrast this with a supermarket, where there are no barriers on entry and customers are allowed to handle all of the items. There is CCTV monitoring the shops, and there are likely to be store detectives patrolling. Shoplifting is likely to occur, but at rates that are acceptable to the supermarket. Conversely, few potential customers are put off visiting the shop because of the measures.

When considering the changing nature of risk and risk management in the digital age, the above example should be seen in the light of a new supermarket business model. In 2021 Amazon opened a supermarket in London that allowed entry to those with a particular smartphone application. The customers can place any item of stock in their bag and depart without needing to use a checkout till. This is due to continuous monitoring by sensors throughout the store and an automatic invoicing

and payment systems. Clearly these approaches to selling goods will affect the risks and risk management in the retail sector.

The range of hazard risks that can affect an organization needs to be identified. Hazard risks can result in unplanned disruption for the organization. Disruptive events cause inefficiency and are to be avoided.

Table 2.2 provides a list of the events that can cause unplanned disruption or inefficiency. These events are divided into categories: people, premises, processes and products. For each category of hazard risks, the organization needs to evaluate the types of incidents that could occur, the sources of those incidents and their likely impact on normal efficient operations.

Management of hazard risks involves analysis and management of three aspects of the hazard risk, which include the necessary actions to prevent the loss occurring, limit the damage that the event could cause and contain the cost of recovering from the event. This is discussed in more detail in Chapter 16.

Organizations will have a tolerance of hazard risks. Their approach should be based on reducing the likelihood and impact of hazard losses. One approach to hazard management is to use insurance to transfer or limit the financial cost of losses. When an organization considers the level of insurance that it will purchase, the hazard tolerance of the organization needs to be fully analysed. Organizations may be willing to accept a certain number of motor accidents as a financial cost that will be funded from the day-to-day profit and loss of the organization. This will only be tolerable up to a certain level, and the organization will need to determine what level is acceptable. Insurance should then be purchased to cover losses that are likely to exceed that level. Organizations need to take care because poor risk management may result in higher insurance premiums, thus negating the benefits of risk transfer.

Table 2.2 Categories of operational disruption

Category	Examples of disruption
People	Lack of people skills and/or resources Inappropriate behaviour by a senior manager Unexpected absence of key personnel Ill health, accident or injury to people
Premises	Inadequate, insufficient or denial of access to premises Damage to or contamination of premises Damage to and breakdown of physical assets Theft or loss of physical assets

(continued)

Table 2.2 (Continued)

Category	Examples of disruption
Processes	Poor maintenance of production equipment Disruption by software failure, hacker or computer virus Inadequate management of information Failure of communication or transport systems
Products	Poor product or service quality Disruption caused by failure of supplier Delivery of defective goods or components Failure of outsourced services and facilities

Some hazard risks will be associated with regulatory requirements and may be considered to be compliance risks. Most organizations will seek to minimize compliance risks.

Manage uncertainty (or control) risks

The nature of control risks and the appropriate responses depend on the level of uncertainty and the nature of the risk. Uncertainty represents a deviation from the required or expected outcome. When an organization is undertaking a project such as a process enhancement, the project has to be delivered on time, within budget and to specification. Also, the enhancement has to deliver the benefits that were required. Deviation from the anticipated benefits of a project represents uncertainties that can only be accepted within a certain range.

Control management is the basis of the approach to risk management adopted by internal auditors and accountants. The risk management requirements of the UK corporate governance code concentrate on internal control with little reference to risk assessment. Control management is concerned with safeguarding company assets and reducing the uncertainty associated with significant risks to minimize the variability of outcomes.

There are dangers if the organization becomes too concerned with control management. It is sometimes suggested that over-focus on internal control and control management suppresses the entrepreneurial effort. This is where risk tolerance and risk appetite (both discussed later) come to the forefront.

The example below considers risk factors by classifying them as controllable and uncontrollable. Consideration of whether business risks are within the control of the organization or not is an important component of successful business risk management.

Geopolitical change

If an organization operates in more than one country it will be exposed to geopolitical risk. For example, its operations in one country (country A) will have to comply with regulations in that country which may not apply in the other countries in which it operates (countries B and C). The organization will have no control over the regulation in country A (other than limited input through consultation processes) but may wish to alter its operations so as to be in compliance with the regulations in countries B and C regardless of the legal requirement in those countries. This would mean that its operations were globally applicable and more easily managed.

When undertaking projects and implementing change, an organization can expect a level of uncertainty. Uncertainty or control risks are an inevitable part of undertaking a project. A contingency fund to allow for the unexpected will need to be part of a project budget, as well as contingent time built into project schedules. When looking to develop appropriate responses to control risks, the organization must make the necessary resources available to identify the controls, implement the controls and respond to the consequences of any control risk materializing.

Embrace opportunity risks

As stated in the opening to this chapter, risk managers will be required to advise on opportunity risk much more as organizations develop greater abilities to create meaningful information, which will enable the uncertainty of future plans to be minimized. This section discusses the basic nature of opportunity risk and in Chapter 14 this is discussed in more detail.

In order to achieve its mission, an organization must take risk, however small or controlled. These risks are often marketplace or commercial risks that have been taken in the expectation of achieving a positive return. These opportunity risks can otherwise be referred to as commercial, speculative or business risks. Opportunity risks are the type of risk with potential to enhance the achievement of the mission of the organization. These risks are the ones associated with embracing business opportunities.

Organizations have an appetite for seizing opportunities and are willing to invest in them. Organizations cannot remain static for long, as referred to in Chapter 1. There will always be a desire for the organization to have effective and efficient operations, tactics and strategy and to maximize the opportunities presented in their

environment, whether commercial or otherwise. Opportunity risks are normally associated with the development of new or amended strategies, although opportunities can also arise from enhancing the efficiency of operations and implementing change initiatives.

Organizations will need to decide what appetite they have for seizing new opportunities, and the level of investment that is appropriate. For example, an organization may realize that there is a requirement in the market for a new product that its expertise would allow it to develop and supply. However, if the organization does not have the resources to develop the new product, it may consider it is unable to implement that strategy and may forego the opportunity. Using the tools provided as risk managers we might analyse the issue and advise that a mitigating action could include seeking a partner with which to create a joint venture and so transfer part of the risk and reduce the gross value at risk for the organization so that this value becomes tolerable and falls within risk appetite. Other options may be available if a thorough analysis is conducted through a risk management lens. This is also discussed in Chapter 22.

It will be for the management of the company to decide whether they have an appetite for seizing the opportunity. However, just because the organization has that appetite, it does not mean that it is the correct thing to do. The board of the company should therefore be aware of the fact that, in order to meet their appetite for seizing the opportunity, actions are required to address the capacity of the organization to support that course of action.

Opportunity management is the approach that seeks to maximize the benefits of taking entrepreneurial risks. Organizations will have an appetite for investing in opportunity risks. There is a clear link between opportunity management and strategic planning. The desire is to maximize the likelihood of a significant positive outcome from investments in business opportunities.

Managing risk 03

The background, principles and aims of risk management

Origins of risk management

Risk management has a variety of origins and as a result can mean different things in different areas of practice. In respect of compliance, UK governments have regulated working conditions since the earliest Factory Acts in the 19th century, but the introduction of the Health and Safety at Work Act in 1974 gave regulators more authority to apply the principles of a risk-based approach in relation to these risks.

As far as hazard risks are concerned, insurance firms increasingly imposed risk mitigation and control standards from the early 19th century if they were required to underwrite the risk. For example, insurers provided their own fire brigades and provided their clients with marks to identify which houses should be saved in the event of a fire. Similarly, marine insurers championed the use of the 'Plimsoll line' to indicate the level of cargo that a ship could safely transport without being dangerously overloaded.

Importance of risk financing

A brief timeline has been produced by Felix Kloman¹ and refers to the development of the practice from insurance purchasing, with Massey Ferguson introducing the concept of 'cost of risk' as being more than just buying insurance in the 1960s. In the USA the insurance function of organizations includes health-care provision for employees, and as a result that function was well resourced and received considerable attention from management on costs. Their approach was based on earlier studies which argued the teams that managed insurance purchases would be better engaged if they re-focused efforts on managing risk. Kloman's analysis follows the development of the practice through a risk financing lens and demonstrates how financial concerns were at the root of changes in emphasis in the earliest days of the study and practice of risk management.

The linkage of insurance, or risk financing, with risk control was developed in Europe during the 1970s, building on the concept of total cost of risk championed by Massey Ferguson. This concept is explained further in Chapter 18. As this approach became established, it also became obvious that there were many risks facing organizations that were not insurable. The tools and techniques of risk management were then applied to other disciplines, as discussed later in this chapter.

Education, formal training and standards

As risk management became more mature, education programmes emerged to support the development of risk management as a profession, which in turn led to the development of risk management qualifications in the 1980s. Risk management regulations associated with corporate governance were introduced and regulators became increasingly concerned with control risks in relation to particular business sectors, for example in financial institutions.

The development of education and qualifications in risk management, as well as the more structured approach of regulators, led to the emergence of risk management standards. Risk management standard AS/NZS 4360:1995 was one of the early examples of a comprehensive approach to the management of risk. As well as the generic risk management standards applicable to all industries, specific risk management approaches also emerged in particular sectors, including the finance sector. The emergence of regulated capital requirements for banks and insurance companies indicated the increased level of risk management maturity required of financial institutions.

Widening the scope of risk

The corporate risk management role started to extend beyond insurance purchase and into contingency planning, which became more important to organizations. There was increased emphasis on loss prevention and safety management, which developed from the 1960s when commercial organizations started to form their own (or captive) insurance companies to obtain more competitive insurance rates. During the 1970s and 1980s this trend expanded globally and places like Bermuda, the Cayman Islands, Guernsey and the Isle of Man developed legislation to attract the formation of such entities.

At the same time, during the 1960s and 1970s there were considerable developments in the risk management approach adopted by occupational health and safety practitioners. During the 1980s the application of risk management techniques to project management developed substantially. Financial institutions continued to develop the application of risk management tools and techniques to market risk and

credit risk. During the 1990s, the financial institutions further broadened their risk management initiatives to include structured consideration of operational risks.

Also during the 1980s, treasury departments began to develop the financial approach to risk management. There was recognition by finance directors that insurance risk management and financial risk management policies should be better co-ordinated. During the 1990s, risk financing products emerged that combined insurance with derivatives. At the same time, corporate governance and listing requirements encouraged directors to place greater emphasis on enterprise risk management (ERM), and the first appointment of a chief risk officer (CRO) occurred at that time.

Uniting into a single function

During the 2000s, financial services firms have been encouraged to develop internal risk management systems and capital models. There has been a rapid growth of CRO positions in energy companies, banks and insurance companies. Boards are now investing more time in ERM due to the Sarbanes–Oxley Act of 2002 in the United States. More detailed risk reporting and other corporate governance requirements have also been introduced.

Despite these trends, the financial crisis of 2008 called into question the contribution that risk management can make to corporate success, especially in financial institutions. There is no doubt that risk management failed to prevent the global financial crisis. This failure was, however, due to the failure to correctly apply effective risk management processes and procedures, rather than inherent defects in risk management as a discipline, as can be seen by the HBOS case study.

HBOS failure to act on risk management advice

It is a matter of public record that the risk manager of HBOS, Paul Moore, warned senior management, including the chair and chief executive officer (CEO), of the dangers of misalignment of rewards to management and the over-emphasis on meeting aggressive sales targets. James Crosby, then the CEO, dismissed Mr Moore in 2004, disregarding his clear warnings, and replaced him with a sales manager who was unqualified in risk management. In 2008 HBOS required £21 billion of UK taxpayers' money to remain afloat, and in 2012, in anticipation of the Parliamentary Inquiry, Mr Crosby resigned as the Deputy Chair of the Financial Services Authority (a position he had subsequently been awarded) and surrendered the knighthood he had received in 2006.

The maturity of the risk management discipline is now such that the links with insurance are much weaker. Insurance is only one of the risk control techniques, only applicable to a portion of hazard risks, and is irrelevant to the majority of risks facing an enterprise. The range of different approaches to risk management is illustrated by the definitions of risk management as set out in Table 3.1.

Taking calculated risks

Risk management is about helping leaders to learn to take more risk and to accept failure. To perform better than its competitors an organization must take more risk, but it should be calculated risk. The risk that is taken should be known and understood; it is not acceptable to take risks unwittingly. This applies across different sectors. For example, *The Orange Book* states:

Public sector organizations cannot be risk averse and be successful... Effective and meaningful risk management in government remains as important as ever in taking a balanced view to managing opportunity and risk. It must be an integral part of informed decision making.²

Providing a suitable definition of risk management is as difficult as providing a suitable and universally accepted definition of risk. Because it is commonly accepted that risk management should be concerned with hazards, uncertainty and opportunities, a description and definition is required that reflects the broad scope of risk management activities (Table 3.1).

Table 3.1 Definitions of risk management

Organization	Definition
ISO Guide 73	Co-ordinated activities to direct and control an organization with regard to risk.
Institute of Risk Management	Process which aims to help organizations understand, evaluate and take action on all their risks with a view to increasing the probability of success and reducing the likelihood of failure.
HM Treasury	The co-ordinated activities designed and operated to manage risk and exercise internal control within an organization
London School of Economics	Selection of those risks a business should take and those that should be avoided or mitigated, followed by action to avoid or reduce risk.

Table 3.2 Importance of risk management

Managing the organization	<ul style="list-style-type: none"> ● Variable cost or availability of raw materials ● Cost of retirement/pension/social benefits ● Desire to deliver greater shareholder value ● Greater transparency required from organizations ● Pace of change in business ever increases ● Impact of e-commerce on all aspects of business life ● Increased reliance on information technology systems ● Increasing importance of intellectual property ● Greater supply chain complexity/dependency ● Reputation becomes more and more important ● Contributing to carbon reduction and supporting climate change initiatives ● Regulatory pressures continue to increase ● Changes/variation in national legislative requirements ● Joint ventures becoming more common
Changes in the marketplace	<ul style="list-style-type: none"> ● Digital approaches disrupting the commercial and marketplace environment ● Globalization of customers, suppliers and products ● Greater customer expectations, often led by competitors ● Need to respond more rapidly to stakeholder expectations ● Constant need to make bold strategic decisions ● Short-term success required, without long-term detriment ● Product innovation and continuous improvements ● Rapid changes in (consumer) product technology ● Threats to world/national economy ● Threat of more pandemics in future caused by zoonotic diseases ● Increasing occurrences of civil unrest/political risks ● Extreme weather events resulting in population shift

The practice of risk management can have a bearing on the list of issues set out in Table 3.2. Insurance has very few solutions for the majority of these issues and this list demonstrates that the application of risk management has moved a long way from its origins in the insurance world and currently is relevant only to the approach to hazard management. This chapter considers the nature of risk management and the established stages that build into the risk management process.

Specialist areas of risk management

Risk management is a constantly developing and evolving discipline. As well as having its origins in the insurance industry and in other branches of hazard management, risk management has strong connections with credit and treasury functions. Many functions within large organizations will have a significant risk management component to their activities, such as tax, treasury, human resources, procurement and logistics. However, it is unlikely that specialists in those areas will consider their activities as simply a branch of the risk management discipline.

Perhaps one of the best known and specialist areas of risk management is that of health and safety at work. Another specialist area is that of business continuity management, which includes disaster recovery planning and business continuity planning. Also, there is no doubt that quality management is a very well-developed branch of risk management, given the high profile attached to quality management systems, such as ISO 9000. Other specialist areas of risk management have developed over the past decades, including:

- project risk management;
- clinical/medical risk management;
- energy risk management;
- financial risk management;
- IT risk management;
- information security risk management.

All of the above specialist areas of risk management have contributed considerably to the development and application of risk management tools and techniques. Project risk management is an area where the application of risk management tools and techniques is particularly well developed. As discussed earlier, project risk management has its emphasis on the management of uncertainty or control risks.

Clinical risk management has been developing for some time. This area of risk management is primarily concerned with patient care, especially during surgical operations. The cost of medical malpractice claims has increased because the medical profession has increased the number of diseases they can improve combined with an increase in life expectancy. This means that not only can medicine improve more people's lives but its application to more ailments will inevitably result in some injury. Any subsequent payout for negligence will be multiplied by the 15 to 20 years' increase in life expectancy that medicine has enabled since the 1950s. This means that claim payments have increased disproportionately, resulting in risk management systems being introduced.

Particular aspects of clinical risk management include the reporting of incidents that occur during surgery. Considerable emphasis has been placed on the need to report, in an accurate and timely manner, details of any incidents that occur in the operating

theatre. This includes details of ‘near misses’ and has required a change of culture amongst medical professionals. There are many publications available on clinical risk management, and a great deal of work has been put into establishing the necessary systems and procedures to cover this specialist area of risk management. Further aspects of clinical risk management include greater attention to making patients aware of the risks that may be associated with the procedure they are about to undertake.

As well as project and clinical risk management, risk management tools and techniques have been applied in a range of specialist industries. In particular, risk management techniques have been applied in the finance sector, focusing on operational risks, as well as market, credit and other types of financial risks. Finance and insurance are highly regulated business sectors, governed by international standards such as Basel III and Solvency II. It is in the finance sector that the title of chief risk officer was first developed. Chapter 31 considers the importance of operational risk management within the finance sector.

The energy sector has also seen an increase in the application of risk management techniques. Techniques around the processing of volatile material were, of course, developed in the energy sector and the DuPont corporation introduced clear health and safety techniques in the 1990s that were demonstrably superior to their peers. Now risk management has extended to sustainability of energy production, the future price of energy and exploration risk.

Information technology (IT) and information security risk management is another well-developed branch. The increasing importance of information to organizations, in terms of the management of and security of data, has resulted in the development of specific standards applicable to IT risk management. Amongst the best established of these standards is COBIT, which is similar in many regards to the COSO ERM cube discussed in Chapter 4.

Enterprise risk management

What distinguishes enterprise risk management (ERM) from the specific types of risk management mentioned is the more integrated or holistic approach that is taken in ERM. In many ways, it can be considered to be a unifying philosophy that draws together management of all types of risks, rather than a new or different approach.

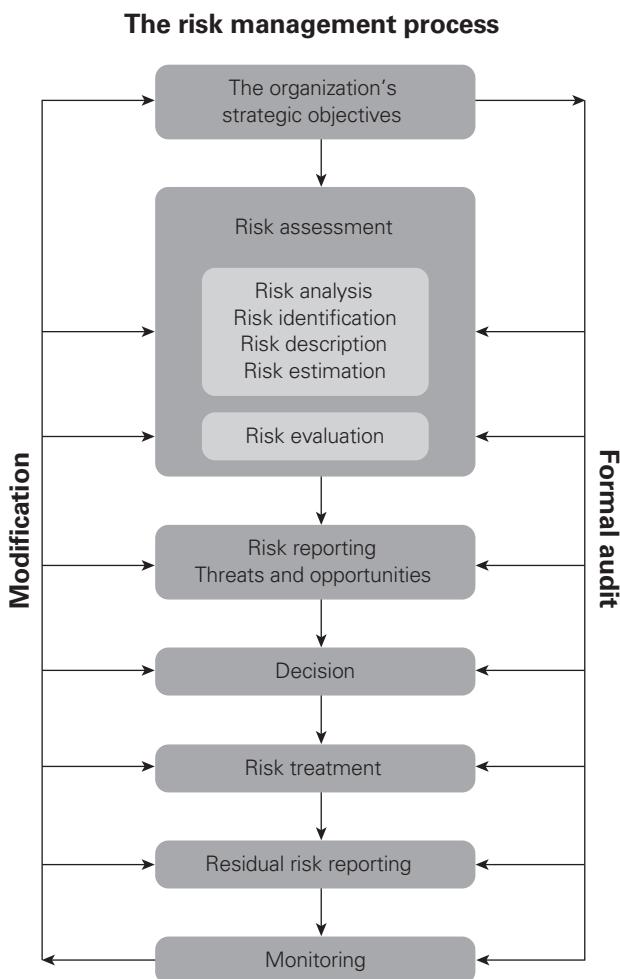
When an organization considers all of the risks that it faces and how these risks could impact its strategy, projects and operations, then the organization is embarking on an ERM approach. The US risk management association, the Risk and Insurance Managers Society, defines enterprise risk management as:

a strategic business discipline that supports the achievement of an organization’s objectives by addressing the full spectrum of its risks and managing the combined impact of those risks as an interrelated risk portfolio.³

An enterprise-wide approach has considerable advantages, because it analyses the potential for disruption to the overall stakeholder expectation. Health and safety, for example, is then viewed as a component in ensuring that staff are always available so that the overall operational core process will not be disrupted, rather than (or perhaps as well as) a separate hazard management issue.

The risk management process is shown graphically in Figure 3.1. Risk management has well-established principles that make up the risk management process, as described in Table 3.3. These principles underpin valuable risk management activities, each of which makes an important contribution. There are many ways of representing

Figure 3.1 Risk management process



SOURCE IRM/Airmic/Alarm (2002)

the risk management process, and each of the standards mentioned in Chapter 4 provides a slightly different description.

Risk management can improve the management of the core processes of an organization by ensuring that key dependencies are analysed, monitored and reviewed. Risk management tools and techniques will assist with the management of the hazard risks, control risks and opportunity risks that could impact these key dependencies. Organizations should ensure that the risk management process is repeated as often as necessary, to overcome the difficulty of a static snapshot of the status of the risks facing the organization. This will ensure that risk management remains a dynamic activity.

Levels of risk management sophistication

More professions and disciplines are now involved in risk management than in previous years. This adds diversity to the development of the risk management discipline. An organization needs not only to be sophisticated in its approach and expectations of risk management, but also mature in the way it conducts its risk management activities. The importance of risk maturity is considered in Chapter 25.

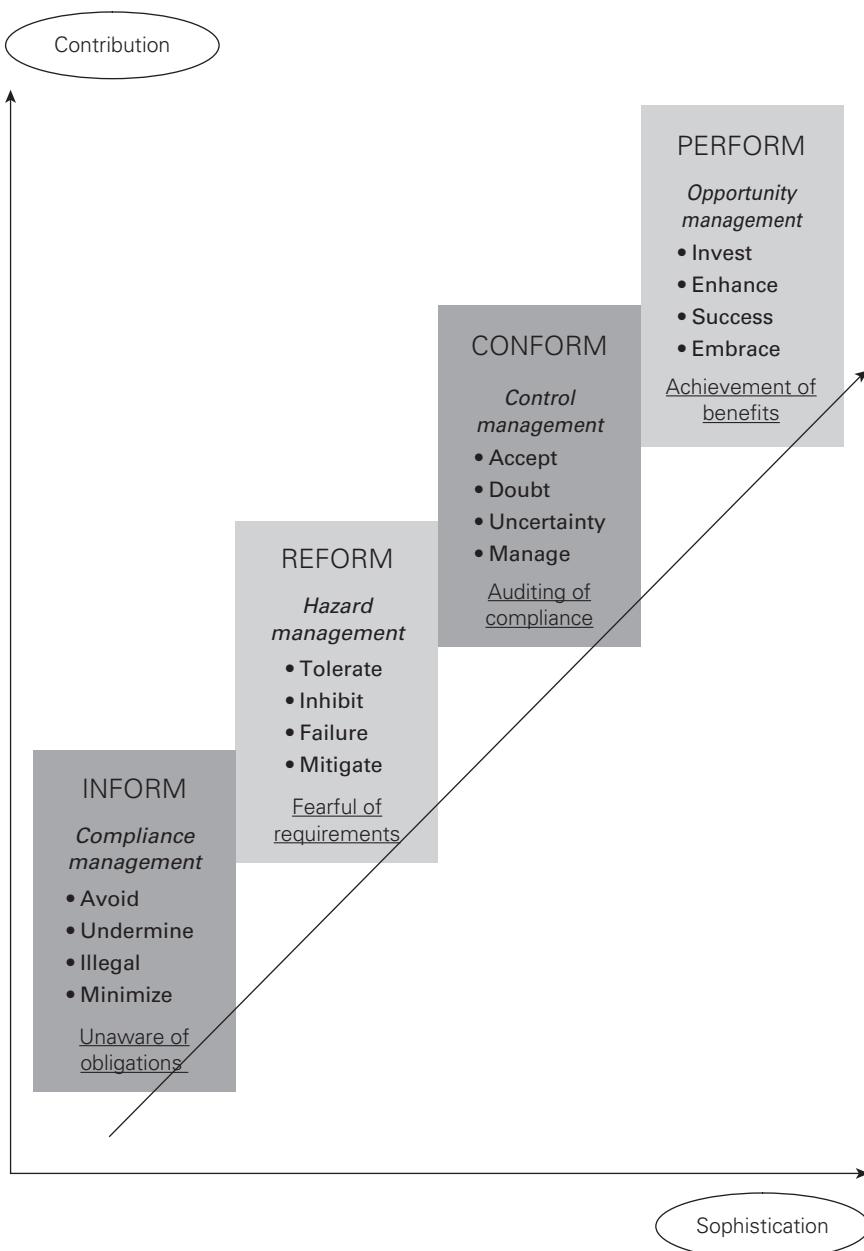
At first, an organization may be unaware of the legal and contractual obligations that it faces. In that case, it will be necessary to inform the organization of its obligations in relation to the risk. As the level of sophistication develops, the organization will become aware of the need to comply with obligations and the more general need for improved risk management. Once the organization is aware of its obligations, there will be a need for it to reform in response to the hazard risks. As the organization responds to the risk, it will seek to conform to the appropriate risk control standards.

After this stage, the organization may realize that there are benefits to be obtained from the risk. The organization will then have the ability to perform and view the risk as an opportunity risk, as illustrated in Figure 3.2.

As a simple example, a magazine publisher might realize that it was not fully complying with equal opportunities legislation because there was no ethnic minority representation within the workforce. The company will identify the actions necessary in order to reform its procedures, so that it conforms to legal requirements. Having achieved compliance, the publisher should seek to perform better in the marketplace by exploring opportunities to produce and publish new magazines that appeal to a more ethnically diverse readership.

The stages of reform to conform to perform represent levels of risk management sophistication. However, it is not necessary for a risk or the practice of risk management to progress from hazard to control to opportunity. In fact, risks can regress in certain circumstances. At any one time, a particular risk will be of a specific type in an organization. Benefits can be obtained from the successful management of that risk at whatever level of sophistication is appropriate at the time. In summary, risk

Figure 3.2 Risk management sophistication



management need only be as sophisticated as the organization requires in order to bring benefits.

Although the four levels of risk management sophistication illustrated in Figure 3.2 represent an improved approach to risk management, there is a danger that

organizations apply risk management techniques too negatively to the point that important decisions are not taken. In this case risk and risk management will ‘disable’ activity, rather than enable improved activity. It will cause the organization to deform its operations. In summary:

- **inform:** unaware of obligations;
- **reform:** awareness of non-compliance;
- **conform:** actions to ensure compliance;
- **perform:** achieve business opportunities;
- **deform:** inactivity caused by obsession.

Principles of risk management

The main principle of risk management is that it delivers value to the organization by applying practices designed to achieve the best possible outcome, reducing volatility or uncertainty. This is achieved through the application of a broader set of aims and principles. There have been several attempts to define these principles. ISO 31000 includes a detailed list of the suggested principles of risk management, which are shown in Chapter 4.

In Table 3.3 the acronym ‘PACE’ combines the eight principles in ISO 31000 to provide five attributes of effective risk management, which are the foundations of a successful approach to risk management within any organization. Some lists of principles also include information on what risk management should do or deliver.

Table 3.3 Principles of risk management

Principle	Description
Proportionate	Risk management activities must be proportionate to the level of risk faced by the organization.
Aligned	Risk management activities need to be aligned with the other activities in the organization.
Comprehensive	In order to be fully effective, the risk management approach must be comprehensive.
Embedded	Risk management activities need to be embedded within the organization.
Dynamic	Risk management activities must be dynamic and responsive to emerging and changing risks.

SOURCE Institute of Risk Management (2018) *Standard Deviations: A risk practitioner’s guide to ISO 31000*, www.theirm.org/media/6907/irm-report-iso-31000-2018-v2.pdf

Objectives of risk management

The five objectives for risk management (mandatory, assurance, decision making, effective and efficient core processes) provide the acronym MADE2, denoting less disruption to normal operations, improved decisions in relation to evaluation and selection of alternative strategies and a reduction of uncertainty in relation to tactics. In other words, a key part of risk management is improved organizational decision making.

The resources available for managing risk are finite, so risks should be evaluated and actions prioritized accordingly. The appropriate range of responses will depend on the nature, size and complexity of the organization and the risks it faces.

As well as assisting with better decision making and improved efficiency, risk management also contributes to the provision of greater assurance to stakeholders through a formal process to identify risk and the consistent application of responses. This in turn allows for better reporting of information by organizations, including risk information. The Sarbanes–Oxley Act of 2002 (SOX) in the United States has accuracy of financial reporting as its main requirement. It brings the issue of the accurate reporting of results to a higher priority (section 404), whilst also requiring full and accurate disclosure of all information about the organization (section 302).

Although SOX is a specific piece of legislation that only applies in certain circumstances, the principles it contains are vitally important to all risk management practitioners. Accordingly, Chapters 34 and 35 of this book consider risk assurance and accurate reporting as integral components of the overall risk management process.

Table 3.4 Risk management objectives

Objective	Description
Mandatory	The basic objective for any risk management initiative is to ensure conformity with applicable rules, regulations and mandatory obligations.
Assurance	The board and audit committee of an organization will require assurance that risk management and internal control activities comply with PACED.
Decision making	Risk management activities should ensure that appropriate risk-based information is available to support decision making.
Effective and efficient core processes	Risk management considerations will assist with achieving effective and efficient strategy, tactics, operations and compliance to ensure the best outcome with reduced volatility of results.

When deciding the importance of risk management in the organization, the design of the risk management initiative and the risk management framework must reflect the reasons why risk management is being undertaken in the organization, in terms of MADE2. These decisions will need to be taken with due regard to the risk management drivers for the particular organization. The drivers may be related to a particular consideration within MADE2, such as the effectiveness and efficiency of operational core processes.

Some organizations have appointed a loss control manager with specific responsibility for reducing the frequency and cost of accidents to people and of damage to plant and equipment. Sometimes, the initiative will be based on the desire to improve the reputation of the organization by enhanced compliance with applicable rules and regulations, or the ability to demonstrate more ethical behaviour – including in the supply chain.

Risk management activities

Risk management is a process that can be divided into several stages, as described in the various standards that are considered in more detail in Chapter 4. Within this book, the risk management process is taken as a set of activities that identify, analyse, evaluate, treat, monitor and review risk. This provides a clear distinction between the process and the framework that implements and supports the process.

There are a number of options when responding to hazard risks. These are often represented as the 4Ts of hazard risk management, and these risk response options are considered in more detail in Chapter 15. In summary, the options for responding to hazard risks are:

- tolerate;
- treat;
- transfer;
- terminate.

Effective and efficient core processes

Insurable or hazard risks can have an immediate impact on operations. Therefore, the initial application of risk management principles was to ensure continuation of normal efficient operations.

As risk management has developed, emphasis has been placed on providing enhancements to core business processes. Processes must be effective in that they

deliver the results that are required, as well as being efficient. For example, there is limited value in having a software program that is efficient if it does not deliver the range of functions that are required.

Strategic decisions are arguably the most important that an organization has to make. Risk management delivers improved information so that strategic decisions can be made with greater confidence. The strategy that is decided by an organization must be capable of delivering the results that are required. There are many examples of organizations that selected an incorrect strategy or failed to successfully implement the selected strategy. Many of these organizations suffered corporate failure.

Strategy should be designed to take advantage of opportunities. For example, in terms of growing revenues, sports clubs may identify the possibility of selling more products to their existing customer base. Some clubs will establish a travel agency for fans of the club who travel overseas, together with the provision of associated travel insurance. Also, there is the possibility of creating a club credit card that will be managed by a new finance subsidiary.

Having identified these possibilities, clubs will need to look at the uncertainties associated with these investments and devise suitable projects to implement the selected strategies. Ensuring that adequate account is taken of risk during all of these activities will increase the chances of selecting the correct strategy. It is worth noting that projects and programmes of work represent the tactics by which strategy is implemented.

Organizations that have effective and efficient tactics, operations and compliance but an incorrect overall strategy will fail. This will be the case however good the risk management activities are at operational and project level. Incorrect strategy has resulted in more corporate failures than ineffective or inefficient operations and tactics. Nevertheless, the importance of compliance activities cannot be over-emphasized as failure to comply could result in the complete shutdown of operations.

The importance of compliance

HSBC had been dogged by stories of money laundering across its global operations and faced legal actions in USA and Switzerland throughout the 2010s. In 2015 it paid £28 million to the Swiss financial authorities, a record at the time, for the 'organizational deficiencies' which allowed HSBC to bank the illegal proceeds of its clients, including political corruption and arms trafficking – essentially a failure of its compliance team.

This was followed in 2019 by an agreement to pay US regulators \$1.9 billion and enter a deferred prosecution agreement because of similar allegations. By paying the fine HSBC avoided the revocation of its charter to continue doing business in the USA.

Implementing risk management

In a rapidly developing discipline like risk management, there is scope for different practitioners to become intolerant towards the approach adopted by others. Internal control specialists focused on the management of uncertainty and the achievement of corporate objectives may be intolerant of the more traditional insurance risk management approach. This can lead to destructive attitudes where a more collaborative approach would benefit the organization.

There is no single style of specialist risk management or approach to risk management that offers all the answers. Clearly, the various styles that can be adopted should operate as complementary approaches within an organization. The integrated or enterprise-wide approach to risk management accepts that the organization must tolerate certain hazard risks and must have an appropriate appetite for investment in opportunity risks. Risk management tools and techniques should be used to achieve the following:

- compliance management provides risk governance;
- hazard management makes outcomes less negative;
- control management reduces the range of possible outcomes;
- opportunity management maximizes the benefits of possible outcomes.

Within the context of hazard management, insurance represents the mechanism for restricting the financial cost of losses when a risk materializes. Risk control and loss management techniques will reduce the expected losses and should ensure that the overall cost is contained. The combination of insurance and risk control/loss management will reduce the actual cost of hazard losses and this will inevitably (and correctly) cause the hazard tolerance of the organization to decline. More of the risk capacity of the organization will then be available for opportunity investment.

Control management reduces the range of possible outcomes from an event. Control management is based on the established techniques of internal financial control, assured by internal auditors. The main intention is to reduce losses associated with inadequate control management at the same time as reducing the range of possible outcomes. This is the contribution that internal control should make to the overall approach to risk management within an organization.

Opportunity management seeks to make positive outcomes more likely and more substantial. As part of the opportunity management approach, the organization should also look at possibilities for increasing the revenue from the product or service. In not-for-profit organizations, opportunity management should facilitate the delivery of better value for money.

Achieving benefits

This chapter has considered the background and principles of risk management that describe the origins of risk management, what risk management should be and what it should deliver. Although organizations may realize that there are benefits from implementing risk management, its successful implementation has to be undertaken as a programme. Chapter 7 sets out the stages involved in successful enterprise-wide risk management.

There is a more detailed consideration of the barriers to and enablers for implementation of risk management in Chapter 27. The most important point to make is that the support of senior management and (ideally) the sponsorship of the board are essential. Also, as part of the programme the concerns of employees and other stakeholders need to be considered. This is normally included within the communication element of the programme. Although risk management is vital to the success of an organization, it is equally vital to communicate the benefits of the approach in order to persuade managers to implement the approach.

It is important to note that not all activities and functions undertaken by managers should be claimed by the risk manager as being undertaken in the name of risk management. Not all activities in the organization will be driven by risk management, even if all decisions, processes, procedures and activities have risks embedded within them.

Risk management drives and enables activities

Risk management enables operations, tactics and strategy in the same way the three pedals in a car enable it to drive at speed. Risk management acts as an accelerator to help the car go faster by helping the organization embrace strategic opportunities and seek rewards. It operates as a clutch to change gears by enabling the successful management of tactical change and the reduction of the associated uncertainty. Finally, it will act as a brake by mitigating operational hazards and avoiding disruption, thereby enhancing operational efficiency.

Much of this book is concerned with risk management input to operational activity. It is likely that this will be impacted by hazard risks and so the focus of risk management in relation to operations is on hazard management, which will involve a combination of loss prevention, damage limitation and cost containment.

Risk management input into strategy focuses on the risk assessment of the various strategic options available to an organization and assists in making optimal decisions. Figure 15.3 illustrates the 5Es of opportunity management (explore, exit or expand, exploit and exist) and plots risk exposure against potential reward.

Organizations undertaking strategic risk management will complete a careful review of viable new business prospects and undertake detailed risk assessment before making strategic decisions.

Notes

- 1 F Kloman (2009) A short history of risk management, Risk Journal, <https://riskjournal.blogspot.com/2009/02/short-history-of-risk-management.html> (archived at <https://perma.cc/HYN2-L7PU>)
- 2 HM Government (2020) *The Orange Book: Management of risk – principles and concepts*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866117/6.6266_HMT_Orange_Book_Update_v6_WEB.PDF (archived at <https://perma.cc/R73D-TKQF>)
- 3 RIMS – the Risk Management Society (2021) About strategic and enterprise risk management (SERM), www.rims.org/resources/strategic-enterprise-risk-center/about-serm (archived at <https://perma.cc/5WJ4-TQGN>)

Risk management 04 standards

Risk management standards set out the overall approach to the successful management of risk, including a description of the risk management process, together with the suggested framework that supports that process. There are a number of established risk management standards and frameworks issued by various global bodies such as the International Organization for Standardization (ISO) based in Switzerland, which is an overarching and co-ordinating body for various national standards bodies, including the British Standards Institute and Standards Australia. In addition to ISO, we shall also consider the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which is largely US based and which has issued comprehensive standards on risk management.

In this chapter we shall principally consider the International Standard ISO 31000 in its updated 2018 version and the COSO standard of 2013. ISO 31000 is internationally recognized, and is a highly influential risk management standard. COSO have applied standards to two concepts and it is important to be clear which one is used and for which purpose. The COSO internal control cube provides a standard against which to measure internal control frameworks and has become most widely used in the United States. Given the spread and influence of US companies, the standard has therefore been adopted and/or adapted by numerous countries and businesses around the world. COSO also provide a standard for ERM. This was released as a framework called the Rainbow Double-Helix published in 2017. We consider the standards elements of both in this chapter but discuss the context of risk in more detail in Chapter 8.

Although some standards are better recognized than others, organizations should select the approach that is most relevant to their particular circumstances. The standards considered in this chapter are designed for use primarily by specialist risk management practitioners.

The standards are reviewed and updated at regular intervals, so we shall also review what changed to get to the most recent versions, particularly with regard to COSO. This provides a good indication of the ‘direction of travel’ for risk management.

Before going any further, it is important to distinguish between a risk management standard and a risk management framework. In simple terms, a risk management standard is the combination of a description of the risk management process,

Table 4.1 Risk management standards

Standard	Description	Reference
ISO 31000	Standard published by the International Standards Organization (2018)	Figure 4.2
COSO ERM frameworks	Framework produced by the Committee of Sponsoring Organizations of the Treadway Commission (2013 and 2017)	Figure 4.3

together with the recommended framework. The key features of a risk management framework are described later in this chapter. Table 4.1 provides a summary of the most widely used risk management standards and frameworks.

Use of risk management standards for listed companies

Risk management standards are widely used as a way of measuring how an organization is managing their risk, particularly for listed companies that are publicly traded. For organizations listed on the New York Stock Exchange, the COSO ERM framework is the preferred risk management standard, along with the COSO internal control framework, which is a requirement of the Sarbanes–Oxley Act of 2002 (SOX). SOX also applies to subsidiaries of US-listed companies around the world. Therefore, the COSO approach is internationally recognized, and in many circumstances is mandated.

For many stock exchanges, the greater emphasis in the listing requirements and associated corporate governance code is on internal control, rather than risk management. This emphasis is maintained in the UK Corporate Governance Code, although there were several enhanced specific requirements in the updated version in 2018.

Apart from the ISO and COSO frameworks, a number of others are also well regarded and in widespread use. The *Guidance on Risk Management, Internal Control and Related Financial and Business Reporting* from the UK's Financial Reporting Council was updated in 2014 and is considered by the Securities and Exchange Commission in the United States to be an acceptable alternative to the COSO internal control framework for SOX compliance. The updated risk guidance can be found as a free download from the website of the Financial Reporting Council (www.frc.org.uk).

As well as the established standards and frameworks, a considerable amount of guidance on risk management has been published by various government departments.

HM Treasury in the UK has updated the highly respected *Orange Book*, with many of its ideas and concepts referenced throughout this volume.

Some of the available standards were developed by risk management professionals, whilst others were developed by accountants or auditors. There are three distinct approaches followed in the various standards:

- ‘risk management’, followed by ISO 31000;
- ‘internal control’, developed by COSO internal control framework and by the FRC risk guidance;
- ‘risk-aware culture’, developed by the Canadian Institute of Chartered Accountants, known as the criteria of control (CoCo) framework.

Risk management process

All established risk management standards have similar processes. Many of the standards distinguish between the risk management process and the framework that implements and supports the process. The risk management standards referred to in Table 4.1 provide a description of a risk management framework, but more emphasis is placed on the risk management process in ISO 31000. The COSO approach does not provide the same clear distinction between the framework and the risk management process itself and is mainly concerned with framework considerations.

Although there are many ways of representing the risk management process, the basic steps are all similar. There can be difficulties with the terminology that is used to describe the various steps, and Appendix B provides definitions of basic terms, as well as cross-referencing the different terminologies that can be used. Chapter 7 describes the stages involved in achieving successful enterprise risk management and this is structured in a plan, implement, measure and learn (PIML) format. This is very similar to the plan–do–check–act format followed in several international standards and often referred to as PDCA. PIML is intended to indicate a more structured and analytical approach.

Context

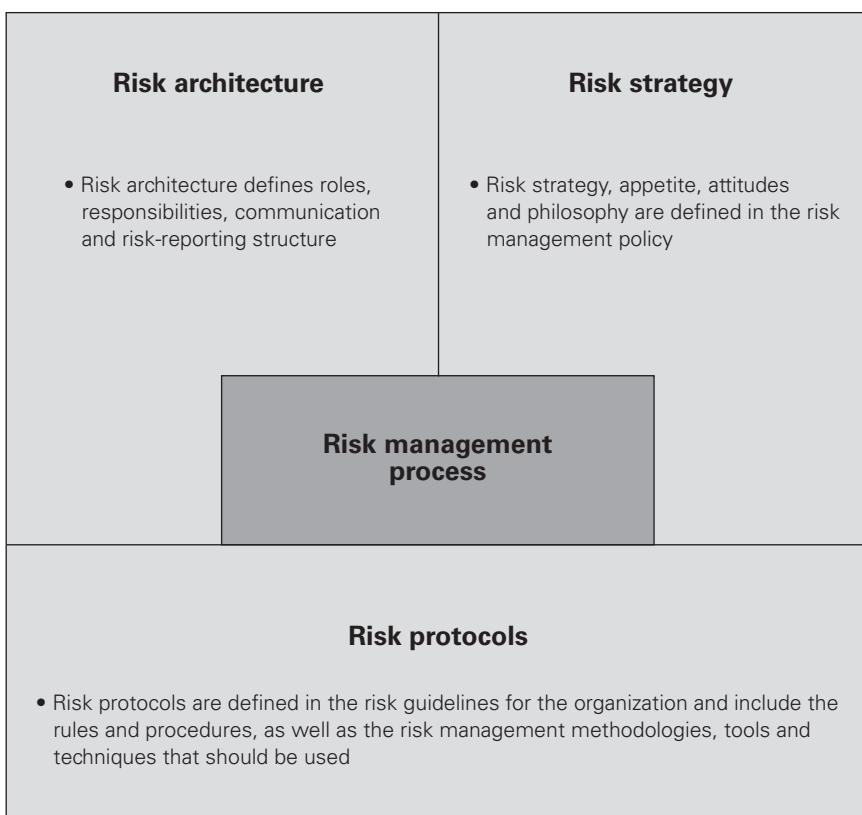
In many risk management standards it is stated that risk management activities should take place within the context of the business environment, the organization and the risks faced by the organization. In order for the context to be described and defined, a framework is required to implement and support the risk management process. ISO 31000 places particular emphasis on context and states that

consideration should be given to the internal context, external context and risk management context when undertaking risk management activities.

All of the established risk management standards refer to the risk management framework, although this is represented in different ways. In order to provide a simple explanation of the scope of the risk management framework, the acronym risk architecture, strategy and protocols (RASP) has been developed. Figure 4.1 illustrates the key features of a risk management framework that is built around and supports the risk management process. The RASP approach is entirely consistent with the concept of the risk management context or risk management framework described in ISO 31000.

Part Six of this book describes RASP in more detail. It is these elements that define the framework within which the risk management process takes place. These three components of risk architecture, strategy and protocols are required for successful risk management activities. There needs to be a thorough understanding of the risk

Figure 4.1 Components of the RM context



management process, followed by a clear definition of the framework that supports the process. Because the framework is a supportive structure, it is shown in Figure 4.2 as a series of components built around and supporting the risk management process.

The risk management framework has two separate considerations. Firstly it must be supportive of the risk management process, and secondly it must ensure that the outputs from the process are communicated into the organization and achieve the anticipated benefits for the organization. The framework should then include the structure, responsibilities, administration, reporting and communication components of risk management. All these components would then be recorded in a ‘manual’ for risk management.

The standards in more detail

ISO 31000

ISO 31000:2018 is in the same format as the previous version of ISO 31000 dated 2009. The standard provides a statement of risk management principles, as well as a description of the risk management framework and process all based around the central purpose of risk management, which is stated as the ‘creation and protection of value’. A summary of these eight principles is set out below and can be seen to be closely aligned to the PACED model set out previously:

- 1** Framework and processes should be customized and proportionate.
- 2** Appropriate and timely involvement of stakeholders is necessary.
- 3** A structured and comprehensive approach is required.
- 4** Risk management is an integral part of all organizational activities.
- 5** Risk management anticipates, detects, acknowledges and responds to changes.
- 6** Risk management explicitly considers any limitations of available information.
- 7** Human and cultural factors influence all aspects of risk management.
- 8** Risk management is continually improved through learning and experience.

This standard also provides information on the development of a risk management framework. The framework is presented as a continuous improvement model similar to the PIML model discussed throughout this book. The detailed information in the standard describes the necessary features of the risk management framework that are required in order to achieve continuous improvement.

Establishing the context is the first stage of the risk management process. Risk assessment is the next step, and comprises risk identification (what are the risks), risk analysis (how big or small are they) and risk evaluation (so what). At this point, the

risk treatment step considers what controls can be put in place to modify the risks, and the implementation of these controls. Surrounding these core steps there is communication and consultation (actually the first step in the standard), monitoring and review, and recording and reporting. These are all important steps in checking, informing and giving assurance that the risks to the organization are being managed effectively, to support decision making at all levels of the organization.

The diagram used to illustrate the risk management process in ISO 31000 is reproduced in Figure 4.2. This contains elements of the risk management framework, as well as the key stages of the risk management process. ISO clearly recognizes the interlinkage of the component parts, similar to the COSO ERM cube, by stating the following: ‘Although the risk management process is often presented as sequential, in practice it is iterative.’

COSO ERM framework

The COSO ERM framework is commonly referred to as the COSO ERM cube. It is a very influential risk management framework that was first produced in 2004. Details of the COSO ERM cube are provided on the COSO website (www.coso.org), where there is a free download of the executive summary of the COSO ERM cube, reproduced here as Figure 4.3. A brief description of the risk management process within the ERM cube is set out in Table 4.2.

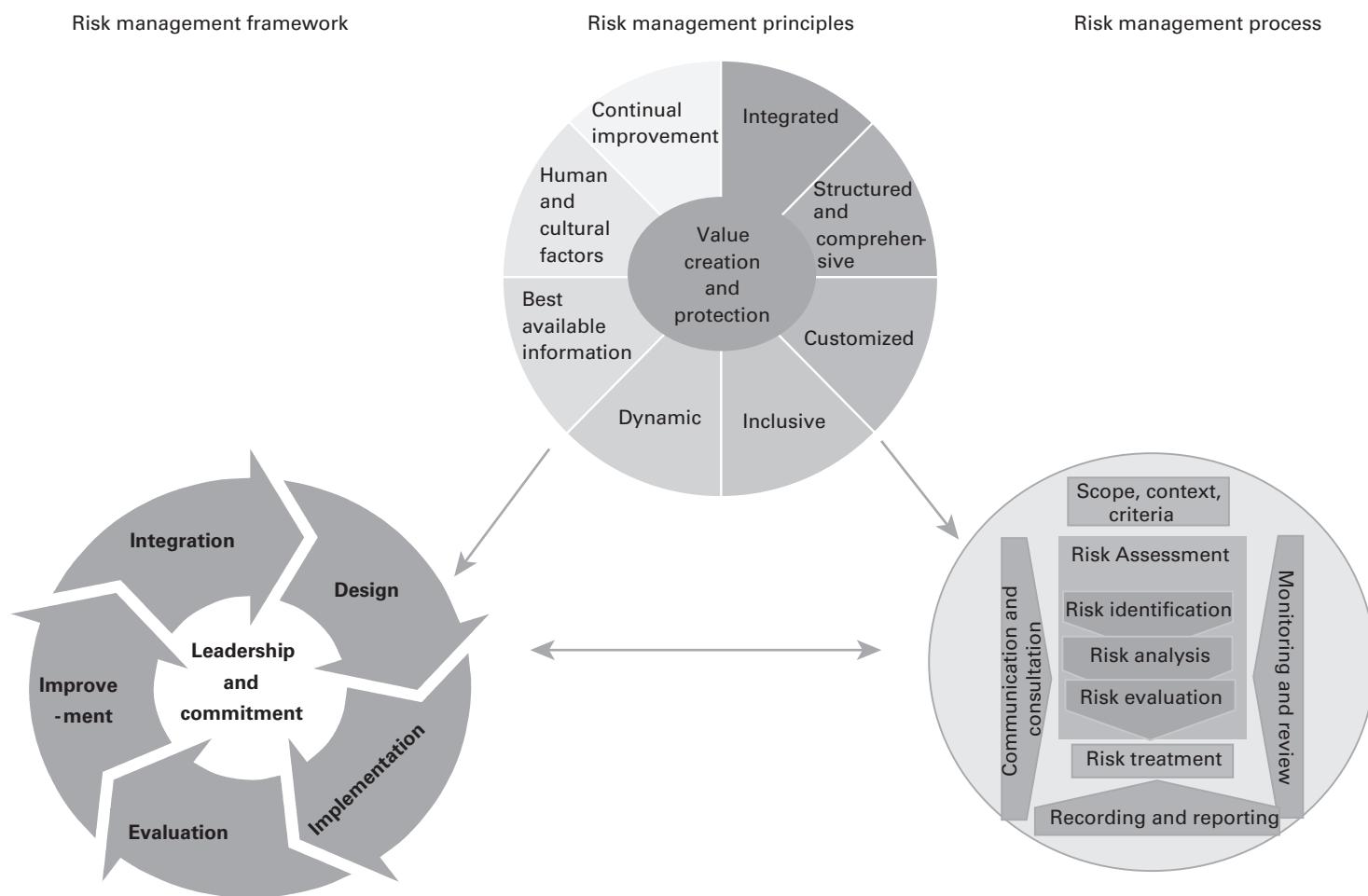
The approach adopted by COSO suggests that enterprise risk management is a multidirectional, iterative process in which almost any component can and does influence all other components. In simple terms, this standard suggests that in order to achieve a successful ERM initiative an organization needs to implement all eight components shown on the front of the cube in relation to each of the four categories of objectives indicated across the top, in all parts of the organization, as indicated on the side of the cube.

At the time of writing, the COSO ERM cube has not been withdrawn by COSO and it provides background to the 2017 rainbow double helix framework considered below. It is noted by COSO that the updated framework is not mandatory, so companies can still utilize the cube, but COSO reserves the right to supersede or retire the cube in the future.

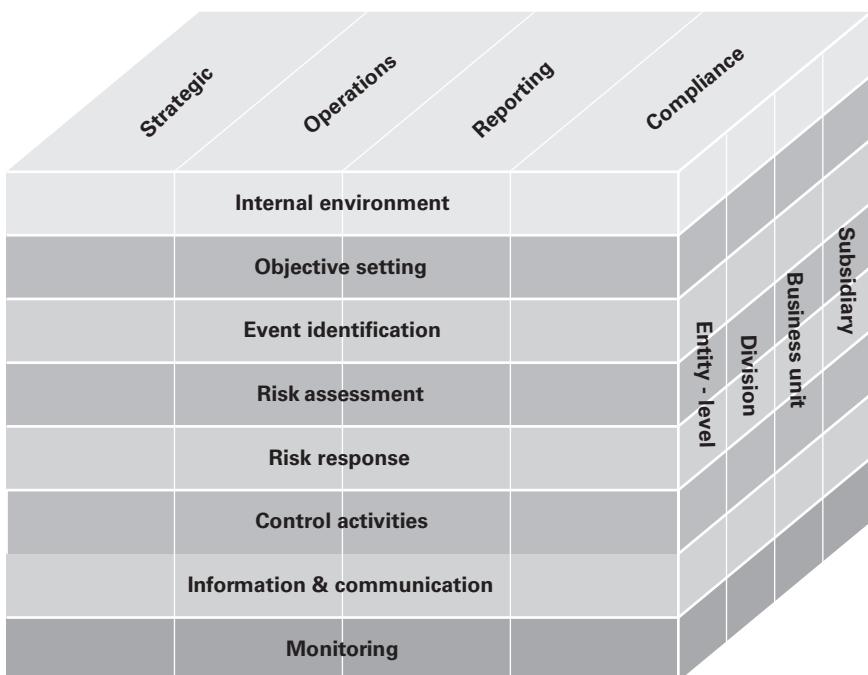
COSO ERM rainbow double helix

In 2017 COSO published additional guidance on ERM and how it can be integrated with strategy and performance. This guidance is reviewed in Chapter 8. The update brings greater focus to the positive contribution to performance that can be made by enterprise risk management.

Figure 4.2 ISO 31000 principles, framework and risk management process



SOURCE Permission to reproduce extracts from ISO 31000 is granted by BSI.

Figure 4.3 COSO ERM cube

SOURCE COSO Enterprise Risk Management: Integrated Framework, © 2004, Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used with permission

Table 4.2 COSO ERM cube

Internal environment – The internal environment encompasses the tone of an organization and sets the basis for how risk is viewed and addressed.

Objective setting – Objectives must exist before management can identify potential events affecting their achievement.

Event identification – Internal and external events affecting achievement of objectives must be identified, distinguishing between risks and opportunities.

Risk assessment – Risks are analysed, considering likelihood and impact, as a basis for determining how they should be managed.

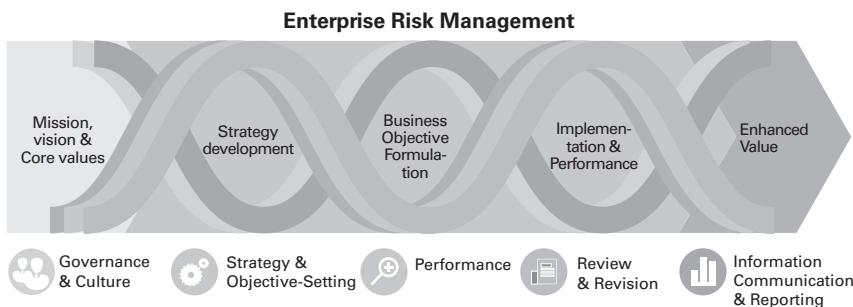
Risk response – Management selects risk responses: avoiding, accepting, reducing or sharing risk.

Control activities – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.

Information and communication – Relevant information is identified, captured and communicated so that people can fulfil their responsibilities.

Monitoring – The entirety of enterprise risk management is monitored and modifications made as necessary.

Figure 4.4 COSO ERM rainbow double helix



The basis of the 2017 COSO guidance is that ERM should be embedded into the activities of an organization, including the mission, vision and core values. In developing strategy, business and performance objectives, an organization should consider the implications of the selected strategy, the risks to strategy and performance, and the possibility of the strategy not aligning with core values.

As previously stated, it is instructive to consider the changes or trends that were considered in the design and reissue of this approach. The revision emphasizes that organizations need to become more adaptive to change. In that sense, it reflects the approach to risk stated at the outset in Chapter 1 where risk management is required because of the fast-paced nature of change as a result of digital transformation. The revision declares that leaders need to adopt better thinking on how to manage the increasing volatility, complexity and uncertainty in the marketplace. The updated framework is designed to meet the needs of executive management and the board with a principles-based approach that integrates risk with strategy and performance.

Updating of RM terminology

There is considerable benefit in adopting a risk management standard, but it is undoubtedly the case that organizations will need to change and adapt the detailed requirements of that standard to their specific circumstances and/or external, internal and risk management contexts. Greater acceptance of a risk management approach within an organization will be achieved when the approach has been customized specifically for the organization by the organization itself.

An important part of customizing the approach to risk management is to establish the risk terminology to be used throughout the organization. There is considerable variation in the terminology used in different branches of the risk management profession and Appendix B includes alternative definitions for many terms. ISO itself

has published two separate guides to risk-related vocabulary: *ISO Guide 73:2009 Risk Management – Vocabulary* and *ISO/IEC Guide 51:2014 Safety aspects – Guidelines for their inclusion in standards*.

As various organizations update their terms and definitions, there is a clear shift towards ensuring that any definition of risk includes a consideration of opportunities or the upside of risk. This is reflected in King IV (2016), which states that ‘risk thus balances the traditional, negative view of risk with one that recognizes the potential opportunities inherent in some risks’.¹ The COSO 2017 guidance states that organizations need to identify the best framework for optimizing strategy and performance in order to integrate ERM throughout the organization to achieve benefits, including (inter alia) identifying new opportunities.

In addition to risk management standards, there are also a number of internal control standards in existence. These internal control frameworks have a different emphasis and are outside the scope of this book, with the exception of the CoCo framework produced by the Canadian Institute of Chartered Accountants. The approach in CoCo is based on the evaluation of the culture or the internal control environment of the organization and is considered in more detail in Chapter 33.

As well as developing ISO 31000 and the guide to risk management terminology ISO Guide 73, work has also been completed on a guide to risk assessment techniques. *IEC 31010:2019: Risk management – Risk assessment techniques* is a very comprehensive publication and it reflects current good practice in the selection and utilization of risk assessment techniques. Further standards in the ISO 31000 ‘suite’ will be issued in coming years; 31022 provides guidelines for management of legal risks, and 31050 is due to be released, offering guidance for managing emerging risks to enhance resilience.

Standards institutions around the world have a requirement for routine review of standards, typically every four years. Therefore, the existing standards, as well as those additional standards that are being developed, will be subject to review on a regular basis. This will ensure that the advice and guidance given in the various standards will remain up to date and in line with current practice.

Note

- 1 Institute of Directors in Southern Africa (2016) *King IV Report on Corporate Guidance for Southern Africa*, https://cdn.ymaws.com/www.iods.co.za/resource/collection/684B68A7-B768-465C-8214-E3A007F15A5A/IoDSA_King_IV_Report_-_WebVersion.pdf (archived at <https://perma.cc/3FYE-WSTS>)

Risk management 05 in context

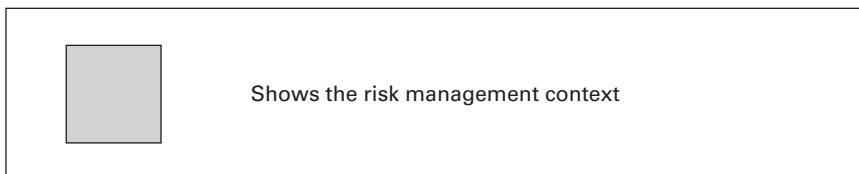
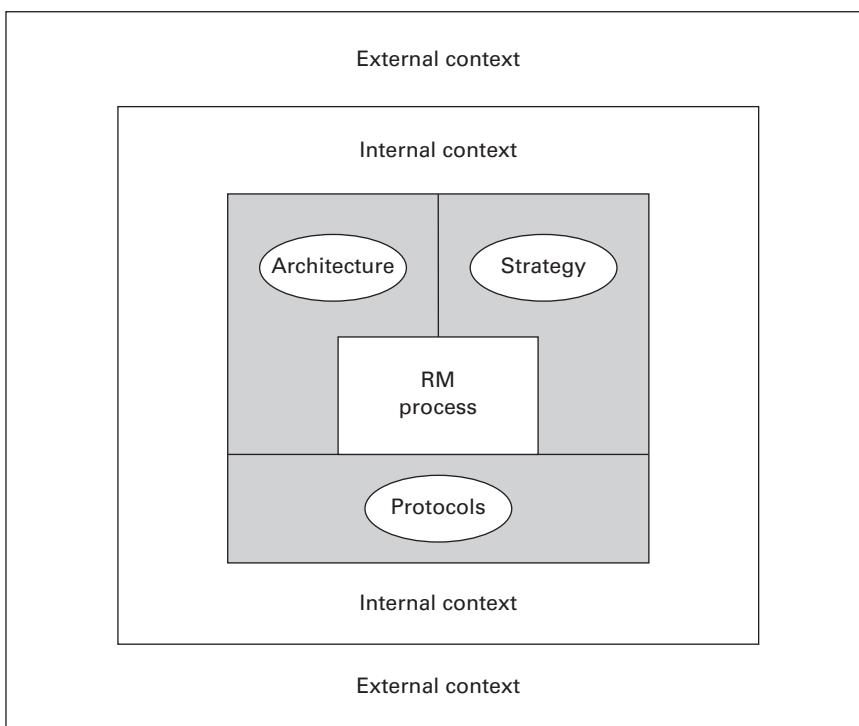
Scope of the context

ISO 31000 states that the first stage in the risk management process is to establish the context, which is shown in Figure 4.2 as ‘scope, context, criteria’. Other standards have referred to context as having three components: the external context, internal context, and risk management context. The relationship between the three contexts is illustrated in Figure 5.1.

The three components of context may be considered as follows:

- The external context is the environment within which the organization exists. This environment will include stakeholder expectations, industry regulations and regulators, the behaviour of competitors and the general economic environment within which the organization operates. The external context also considers the drivers and trends that can affect the success of the organization and its ability to achieve objectives. These are the opportunities and threats facing the organization.
- Internal context refers to the organization itself, the activities it undertakes, the range of skills and capabilities available within the organization, and how it is structured. Internal stakeholders and their expectations are part of the internal context and operate within the culture of the organization. The internal context concerns objectives, the capacity and capabilities of the organization, as well as the business core processes that are in place. An important consideration regarding the internal context is how the organization makes decisions. These are the strengths and weaknesses within the organization and provide internal opportunities and threats.
- The risk management context has already been described as the risk architecture, strategy and protocols or the risk management framework within the organization. As noted earlier, this framework must fulfil two functions: firstly, provide support for the risk management process within the organization; and secondly ensure that the outputs from the risk management process are communicated to internal and external stakeholders.

Figure 5.1 Three components of context



The nature and extent of the risk management process itself is a major consideration when establishing the context for risk management. The key question is what the risk management process is expected to achieve, or to answer the question of why the organization has risk management activities in place. The risk management context also includes consideration of who will be responsible and identifies the resources that will be required in order to fulfil risk management activities.

Another important consideration within the risk management context is the establishment of risk appetite or risk criteria. This will help the organization decide what controls should be put in place and whether the residual or current level of risk is acceptable. The risk management context should also provide a means of

establishing the overall total risk exposure so that this can be compared with the risk appetite of the organization and the capacity of the organization to withstand risk.

External context

Risk management standard ISO 31000 identifies ‘establish the context’ as the first stage in the risk management process, represented in the ISO 31000 diagram, and reproduced as Figure 4.2, as ‘scope, context, criteria’. Establishing the context is a fundamentally important aspect of successful risk management, and it is also identified by other international standards as an essential early stage in implementing risk management.

Establishing the external context must take account of the expectations of external stakeholders. The critical importance of stakeholder expectations is considered in more detail in Chapter 30. For many organizations, the most important group of external stakeholders will be customers. The external context for an organization will be significantly influenced by the nature of the customers and the products or services that they are being offered. Consideration of customers and the customer offering form an important part of the business model for the organization and the relevance of the business model to risk management is considered in more detail in Chapter 20.

Having identified the expectations of external stakeholders, an organization can then view, in more detail, the factors that influence the external context for the organization. Many organizations use the political, economic, social, technological, legal and environmental/ethical (PESTLE) risk classification system. The PESTLE risk classification system is considered in more detail in Chapter 11.

The finance, infrastructure, reputation, marketplace (FIRM) risk scorecard provides a structure for carrying out a detailed evaluation of the context of the organization. This is discussed further in Chapter 14 where Table 14.2 provides a detailed checklist of questions relating to the development of a riskiness index based on the structure of the FIRM risk scorecard.

In summary, the reputational component of the external context for an organization defines the external perception of the organization, the desire of customers to trade with the organization and the level of customer retention. In particular, when evaluating the reputational component of the external context, the following issues should be addressed:

- public perception of the industry sector in which the organization operates;
- corporate social responsibility standards achieved by the organization;
- governance standards and whether the sector is highly regulated;
- quality of products or services and/or after-sales service standards.

The other component of the FIRM risk scorecard relevant to the external environment is the marketplace and the level of presence of the organization within the marketplace. This will impact the level of customer trade or expenditure. In particular, when evaluating the marketplace component of the external environment, the following issues should be addressed:

- level of revenue generation in the marketplace and return on investment;
- presence of aggressive competitors and/or high customer expectations;
- level of economic stability, including exposure to interest rates and foreign exchange rates;
- complexity of the supply chain and volatility of raw material costs;
- exposure to disruption through either technology or geopolitical reasons (political risks, war and terrorism).

The overall purpose of evaluating the external context is to determine the level of riskiness associated with the external environment within which the organization operates. This will enable the organization to validate the existing business model and develop strategy for the future, together with the tactics for implementing that strategy.

External stakeholders

Good stewardship by the board should not inhibit sensible risk taking that is critical to growth. However, the assessment of risks as part of the normal business planning process should support better decision taking, ensure that the board and management respond promptly to risks when they arise, and ensure that shareholders and other stakeholders are well informed about the principal risks and prospects of the company. The board's responsibility for the organization's culture is essential to the way in which risk is considered and addressed within the organization and with external stakeholders.

SOURCE FRC (2014) *Guidance on Risk Management and Internal Control and Related Financial and Business Reporting*, www.frc.org.uk/getattachment/d672c107-b1fb-4051-84b0-f5b83a1b93f6/Guidance-on-Risk-Management-Internal-Control-and-Related-Reporting.pdf

Internal context

Establishing the internal context of an organization must take account of the expectations of internal stakeholders. There will be a range of internal stakeholders, but the most important group will be the people on whom the organization directly

depends. This will include members of staff and people providing services on an outsourced, contracted and/or supplier basis.

Having identified the expectations of internal stakeholders, including the importance of these stakeholders to the operations and compliance activities of the organization, it will then be possible to view in more detail the factors that influence the internal context. Using the FIRM risk scorecard, the financial and infrastructure components are primarily related to the internal context.

In summary, the financial component of the internal context of an organization defines the financial procedures and the means by which money is managed and profitability is achieved. In particular, when evaluating the financial component of the internal context, the following issues should be addressed:

- availability of adequate funds and future flows of funds to fulfil strategic plans;
- existence of robust procedures for correct allocation of funds for investment;
- nature of internal financial control environment to prevent fraud;
- availability of funds to meet historical and anticipated future liabilities.

The other component of the FIRM risk scorecard relevant to the internal context is infrastructure, as this influences the nature of the processes undertaken within the organization. Infrastructure risks define the level of inefficiency and dysfunction that may arise during internal processes. In particular, when evaluating the infrastructure component of the internal context, the following issues should be addressed:

- senior management structure and the nature of the risk culture;
- availability of adequate people resources and skills, including intellectual property;
- availability of adequate physical assets to support operational activities;
- information technology infrastructure sufficient to achieve resilience and protect data;
- business continuity plans in place to ensure continuity of activities following major disruption;
- arrangements for service delivery and/or transportation and reliable communication infrastructure.

The FIRM risk scorecard offers one mechanism for evaluating the internal context of an organization, but other approaches may be employed, including a SWOT analysis.

There are many checklists available that will enable an organization to identify the nature of the external and internal context within which it operates. Which classification system or checklist of questions is used is less important than the need to identify the full range of risk issues faced by the organization. This will enable the organization to validate the existing business model, the resources required to deliver the business model, as well as the level of resilience within the existing business model.

Risk management context

Chapter 23 considers the risk management context in detail, in terms of the risk architecture, strategy and protocols (RASP) developed by the organization. The RASP of an organization defines the structure of the risk management context and how the components of that context are implemented to achieve the desired benefits from the enterprise risk management initiative.

It is important that the risk management context of an organization is capable of delivering the required risk management strategy and developing the necessary risk-aware culture. The components of a satisfactory risk-aware culture are leadership, involvement, learning, accountability and communication (LILAC), as considered in more detail in Chapter 25.

An important component of the risk management context is the mandate provided by senior management that provides the scope and level of authority for undertaking risk management activities in the organization. The mandate provided to the risk manager, head of internal audit and others involved in the risk management initiative should be defined in the risk management policy for the organization.

The risk attitude and risk appetite of the organization, as defined by the risk criteria for different types of risks, helps to establish the risk management context of the organization and to provide the basis for undertaking risk assessments and recording the results in a risk register, as discussed below. The nature and extent of communication of the information contained in a risk register throughout the risk architecture of the organization also helps define the risk management context.

Perhaps the most important feature of the risk management context that will determine the success of the enterprise risk management initiative relates to how the initiative is implemented. Chapter 7 discusses implementation for an enterprise risk management initiative in more detail.

The risk management context must contribute to the success of the organization and be supportive of the delivery of stakeholder expectations, both external and internal. A requirement of the risk management context is that it should identify emerging risks and support the response to changes in the external and internal context of the organization. The nature of emerging risks can be complex and, by definition, highly unpredictable.

In helping the organization identify the nature of emerging risks, the risk management context should provide the mechanism for providing early warning. This has been described as the ‘risk radar’ of the organization and it must include timely review and evaluation of information relating to emerging risks. In order to comprehensively determine the specific impact and consequences for the organization, the mechanism for identifying emerging risks should also include provision for identifying opportunities that may be exploited in the future.

In summary, the organization is required to identify each specific external, internal and risk management context issue that could impact the organization, acquire and evaluate timely knowledge and information about them, evaluate the risks and opportunities that these context factors present and take appropriate actions to mitigate the risks and embrace the opportunities.

Once the external, internal and risk management contexts have been established, the risks that have been identified should then be documented within the scope of RASP. This is usually performed by a risk register.

Designing a risk register

Once identified through establishing their context, risks should be documented in some form. Documentation can be as simple as a spreadsheet or table of risk but it is more likely to involve, in most organizations, some form of technology that enables manipulation of the data in various ways. Its form will depend upon the maturity of the organization, the resources available to the risk management function, who is to use it and what it will be used for.

The register of these documented risks will be the repository for risk management knowledge for the organization. A risk register is defined in ISO Guide 73 as the ‘record of information about identified risks’. The guide adds that the purpose of the risk register is to facilitate ownership and management of each risk.

Typically, the risk register will identify all risks and contain sufficient information to support the ranking of each risk into broad categories of likelihood and impact to allow the significant risks to be identified from this universe of identified risk. For example, it will record the results of the risk assessment related to the process, operation, location, business unit or project under consideration.

Although there is no fixed format for this document (and in practice much of this will be driven by the software used) the detail will include category, cause, source, risk, consequence, inherent/current/target ratings, existing controls, new controls, risk owner, control owner, new control review date, objective at risk, and similar detail in as much granularity as is appropriate for the organization.

The purpose of the risk register is to form an agreed record of the significant risks that have been identified, and the control activities that are currently undertaken. It is also a record of the additional actions that are proposed to improve the control of the particular risk. The risk register has three functions:

- Collecting the risk information requires engagement from the organization and will establish the risk function credentials. Input will vary and can include workshops, incidents, other datasets, etc.

- To maintain the data in a form that enables manipulation to establish trends or relationships. It should be possible to identify possible actions (and unintended consequences) if the data allows building a network of risk for the organization. Documenting the components using appropriate software can establish complex linkages between various relationships.
- To provide the source material to establish actions, and communicate risk information to stakeholders, including escalating risk issues when appropriate.

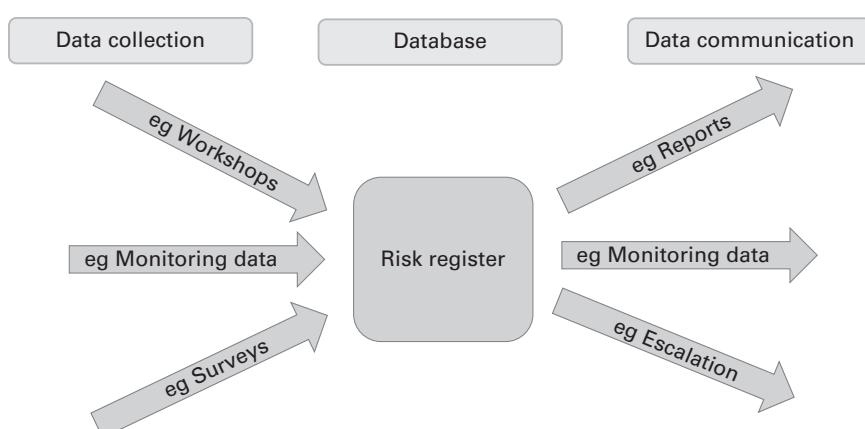
These are shown in Figure 5.2

Using a risk register

A well-constructed and dynamic risk register is at the heart of a successful risk management initiative. For example, output from the risk register may form the centrepiece of discussion in a risk committee and be the subject of detailed discussion and challenge, requiring supporting information as back-up. The risk register itself should not form a risk report directly, without some form of interpretation.

The output will need to be tailored to the function or person receiving the report and whether the reports require an action, control or escalation so that the message, purpose and reasoning is clear. The communication from the risk function is likely to be judged by the operation, and a well-constructed report will enable better engagement with the function so that the value of risk management becomes more compelling.

Figure 5.2 Components of a risk register



SOURCE Satarla (reproduced with permission)

In some organizations, the risk register is given the status of a controlled document to be used by internal audit as one of the key reference documents for undertaking an audit of risk management activities. Risk control activities should be described in sufficient detail for the controls to be auditable. This is especially important when the risk register relates to the routine operations undertaken by the organization. It will, for example, probably provide a record of the critical controls that are in place, together with the details of any additional controls that need to be introduced. This detail can form a risk action plan and clearly establish the responsibility for undertaking the actions identified.

A risk register can be used to inform strategy and provide input to the range of strategic options that can be undertaken. The risk assessment this produces could include both the risks of undertaking the strategy and an analysis of the risks associated with not undertaking the proposed strategy. Certainly, the output should be attached to a business plan as a record of the risks that could impact the achievement of that plan.

Finally, the board will probably wish to see a risk report generated by the register on at least a quarterly basis, and more frequently if significant changes occur. This will ensure that the risk register remains a dynamic document and is kept fully up to date. It will also ensure the necessary actions are taken and reported to the board.

The future for risk registers

It should be clear from the discussion above that technology has a large part to play in the future of risk registers. The increased ability to collect data and analyse streams of information in real time will develop into bringing these registers into a more dynamic environment.

At the time of writing, it is recognized that there are disadvantages associated with the use of risk registers; the information needs to be correct, updated and to the right level of detail. Manually operated risk registers can become unwieldy if they contain too much detail, and open to criticism if they contain too little. Senior management may consider they have fulfilled their obligation to risk management by attending a risk assessment workshop and producing a risk register, without the need for further engagement in the risk management process.

Without the benefit of technology to manipulate and analyse the complex array of information the maintenance of risk registers can become a focus of activity such that it becomes the process rather than a tool to achieve improvements. More importantly, unless supported by technology, it is difficult for a risk register to be a collaborative tool that exists in real time.

There are many different types of software solutions in use and being designed. It is likely that new technology will allow greater integration of different datasets and

live streams of information from, for instance, remote operating monitors. These new forms of register will provide near instant analysis and probably have the ability to generate some form of quantification and aggregation technique to establish greater levels of numeracy.

The enhanced technology will embrace machine learning (or other forms of artificial intelligence) at all levels of digital information. This may include taking those risk registers that are currently less well structured in a digital fashion and transforming them into datasets which can become more meaningfully analysed. In other words, risk registers need to be ready to become more digitally enabled as technology proceeds.

PART TWO

Enterprise risk management

LEARNING OUTCOMES

Having studied this section readers will be able to:

- Explain the features of an enterprise-wide approach to risk management and the various available definitions of ERM.
- Outline the steps required in order to achieve successful implementation of an enterprise risk management initiative.
- Consider the changing face of risk management and the increasing importance of managing emerging risks.
- Outline the concept of 'emerging risks'.
- Outline the difference between resilience and risk management.
- Outline some alternative approaches to risk management.
- Outline the need to set performance objectives.
- Explain the importance of reviewing the progress of a risk management function.

Further reading

- Bernstein, P (1998) *Against the Gods: The remarkable story of risk*, Wiley, Hoboken, NJ
- BSI (2011) *BS 31100:2011 Risk Management: Code of practice and guidance for the implementation of BS ISO 31000*, British Standards Institution, London
- Calvert, J and Arbuthnot, G (2020) *Failures of State: The inside story of Britain's battle with Coronavirus*, Mudlark, London
- COSO (2004) *Enterprise Risk Management: Integrated framework*, www.coso.org/pages/erm-integratedframework.aspx
- COSO (2017) *Enterprise Risk Management: Integrating with strategy and performance*, www.coso.org/documents/2017-coso-erm-integrating-with-strategy-and-performance-executive-summary.pdf
- Institute of Operational Risk (2021) Sound practice guidance, www.ior-institute.org/sound-practice-guidance
- ISO (2009) *ISO Guide 73:2009 Risk Management – Vocabulary*, www.iso.org/standard/44651.html
- ISO (2018) *International Standard ISO 31000:2018 Risk Management – Guidelines*, www.iso.org/standard/65694.html

CASE STUDIES

The student can review the following examples to illustrate further the areas discussed in Part Two and throughout this book.

bp: Integrated approach to risk management

bp is a global energy supplier that has experienced some catastrophic losses (Deepwater Horizon) and is focused on continuing to manage its traditional customer base whilst moving its business to a more sustainable footing and delivering renewable energy. They carry out their risk management activities in three ways:

- Day to day: Where ‘management and staff seek to identify and manage risk, promoting safe, compliant and reliable operations’. These are focused on ‘reduc[ing] risk and deliver[ing] safe, compliant and reliable operations as well as greater efficiency and sustainable financial results’.
- Business and strategy: Where their ‘businesses integrate risk management into key business processes such as strategy, planning, performance management, resource and capital allocation, and project appraisal’. They achieve this by ‘collating risk data, assessing risk management activities, making further improvements and in connection with planning new activities’.

- Oversight and governance: Where ‘management, the leadership team, the board and relevant committees provide oversight of how significant risks to BP are identified, assessed and managed’.

They make specific mention of climate-related risks and state that ‘these risks are considered through key business processes including the strategy, annual plan, capital allocation and investment decisions. The outputs of these key business processes are reviewed in line with the cadence of these activities.’

Edited extracts from: bp (2020) bp Annual Report 2020, www.bp.com/en/global/corporate/investors/results-and-reporting/annual-report.html

Lincolnshire County Council: Strategic approach to risk management

This English local authority provides services to its community as varied as education, social care, roads and highways. They have a particularly clear statement as to how they deal with risk in a strategic fashion, which explicitly discusses making informed decisions and realizing opportunities. Their communication is well set out and designed for use by all stakeholders, including both employees and residents. They state that their approach includes:

- ‘Setting the “tone from the top” on the level of risk we are prepared to accept on our different service delivery activities and priorities. [This] incorporates a new “opportunist” category, acknowledging that how we “think about risk” will be different depending on the context of corporate impact and sensitivity.’
- ‘Acknowledging that even with good risk management and our best endeavours – things can go wrong. Where this happens we use the lessons learnt to try and prevent it from happening again.’
- ‘Developing leadership capacity and skills. Risk management should be integral to how we run council business/services.’
- ‘Supporting a culture of well measured risk taking throughout the council’s business, including strategic and operational.’
- ‘Ensuring our approach to risk management is proportionate to the decision being made.’

Edited extracts from: Lincolnshire County Council (2018) Thinking About Risk: Our risk management strategy 2018–2020, www.lincolnshire.gov.uk/downloads/file/1925/risk-management-strategy

DP World: Enterprise approach to risk management

DP World is a global logistics operator ultimately owned by Dubai Holdings. They operate ports and transport systems globally and have a section in their annual report headed ‘Effective risk management’, which discusses their approach to ERM. The approach is in two stages: firstly, each business reports its own individual risk assessment (which they

call a 'bottom-up' approach); and then the second stage is a strategic view across all their businesses, or a 'top-down' approach. They clearly set out responsibilities and their four-stage approach involving:

- 1 Risk identification.
- 2 Risk assessment and prioritization.
- 3 Risk monitoring and reporting.
- 4 Risk treatment and response.

There is an expanded section in the 2020 report discussing the response to Covid-19. As well as describing their operational response they state that:

Covid-19 is not an isolated risk, it is enterprise-wide and is a key consideration that needs to be reflected in our business unit, regional and corporate risks. Accordingly, the associated impacts, trends and responses have been incorporated across our principal risks

*Edited extracts from: DP World (2020) *The Smarter Trade Report: Annual report and accounts 2020*, www.dpworld.com/-/media/project/dpwg/dpwg-tenant/corporate/global/media-files/investor-relations/financials-and-presentation/financial-reports/annual-results/2020/dpw-36032-annual-report-2020-eng-web.pdf?rev=3d0a53fb14094deda745a3426e4c9d74*

Enterprise risk management

06

Enterprise-wide approach

Risk management has developed over the course of the last 50 years and has been practised and improved in specialist areas such as portfolios, programmes, projects, energy, finance, operational and clinical risk management. This has delivered benefits in these distinct areas but it does not benefit the organization as a whole if some areas of risks are well managed within a ‘silo’ at the expense of the organization as a whole. There are many examples of organizations that have well-developed and in some cases leading-edge risk management practices in, for instance, health and safety risk management areas, but ultimately have failed due to the absence of financial or strategic risk management. For this reason, organizations have embraced the desire to take a broader approach to the practice of risk management.

Various terms have been used to describe this broader approach, including holistic, integrated, strategic and enterprise-wide risk management. It is the term enterprise or enterprise-wide risk management (ERM) that is now the most widely used and generally accepted terminology for this broader approach.

ERM takes a unifying, broader and more integrated approach. The ERM approach means that an organization looks at the uncertainties that it faces across all of the operations that it undertakes. ERM is concerned with the opportunities and threats that can impact the objectives, key dependencies or core processes of the organization.

The ERM approach addresses the fact that many risks are interrelated. Specialist areas of risk management fail to address the relationship between risks in their field and other internal, or external, risks. With the ERM approach, the relationship between risks is identified by the fact that two or more risks can have an impact on the same activity or objective. Many disasters have arisen in the past because of the failure to address the interconnectivity of risks. The ERM approach is based on looking at the objective, key dependency or core process and evaluating all of the risks that could impact the item being evaluated.

Organizations practise risk management in a number of different ways. However, there are many common features to most of these approaches. Table 6.1 gives an overview of the features of enterprise risk management as a comparison to the silo-based approach whereby risk management tools and techniques are applied to different types of risks independently. ERM allows the organization to gain an overview of all the risks that it faces so that it can take co-ordinated actions to manage these risks. Nevertheless, the specialist risk management functions, such as health and safety and business continuity, continue to make a valuable contribution.

An example of the ERM approach is to consider a sports club where the key objective is to maximize attendance at games. This process is made up of several activities, including marketing, advertising, allocation and sale of tickets as well as logistical arrangements to ensure that the experience at the game is as good as possible. Part of maximizing attendance at games will be to ensure there are adequate parking and transport arrangements, together with suitable catering and other welfare arrangements in the ground.

Table 6.1 Features of an enterprise-wide approach

- | | |
|----|---|
| 1 | Encompasses all areas of organizational exposure to risk (financial, operational, reporting, compliance, governance, strategic, reputational, etc). |
| 2 | Prioritizes and manages those exposures as an interrelated risk portfolio rather than as individual 'silos' of risk. |
| 3 | Evaluates the risk portfolio in the context of all significant internal and external contexts, systems, circumstances and stakeholders. |
| 4 | Recognizes that individual risks across the organization are interrelated and can create a combined exposure that differs from the sum of the individual risks. |
| 5 | Provides a structured process for the management of all risks, whether those risks are primarily quantitative or qualitative in nature. |
| 6 | Seeks to embed risk management as a component in all critical decisions throughout the organization. |
| 7 | Provides a means for the organization to identify the risks that it is willing to take in order to achieve strategic objectives. |
| 8 | Constructs a means of communicating on risk issues, so that there is a common understanding of the risks faced by the organization, and their importance. |
| 9 | Supports the activities of internal audit by providing a structure for the provision of assurance to the board and audit committee. |
| 10 | Views the effective management of risk as a competitive advantage that contributes to the achievement of business and strategic objectives. |

By identifying the key activities that deliver the selected core process, the club is able to identify the risks that could impact both these activities and the core process. Targets can then be set for increased attendance at future games, and responsibility for the success of this core process has been allocated to the commercial director of the club. A consideration of the opportunities for increasing attendance at games can also be included in this broader approach.

Definitions of ERM

Table 6.2 presents a number of suggested definitions of enterprise risk management. There are three components that are required in a comprehensive definition of the ERM process. These are: 1) the description of the process that underpins enterprise risk management; 2) identification of the outputs of that process; and 3) the impact (or benefit) that arises from those outputs.

Many of the definitions concentrate on the process by describing the activities that make up the ERM approach. This is a good starting point, but the outputs from that process are more important than the process itself. Some of the definitions do include reference to the outputs from the process, such as being able to manage risks within the risk appetite of the organization and provide reasonable assurance regarding the achievement of objectives.

Table 6.2 Definitions of enterprise risk management

Organization	Definition
RIMS	Enterprise risk management is a strategic business discipline that supports the achievement of an organization's objectives by addressing the full spectrum of its risks and managing the combined impact of those risks as an interrelated risk portfolio.
COSO (2017)	The culture, capabilities, and practices that organizations integrate with strategy setting and apply when they carry out that strategy, with the purpose of managing risk in creating, preserving and realizing value.
IIA	A rigorous and co-ordinated approach to assessing and responding to all risks that affect the achievement of an organization's strategic and financial objectives.
<i>The Orange Book</i>	The co-ordinated activities designed and operated to manage risk and exercise internal control within an organization.

The following is offered for the sake of clarification. Enterprise risk management:

- involves the identification and evaluation of uncertainties that matter to the organization, both upside and downside;
- uses processes that assign ownership to implement and monitor actions to manage these uncertainties;
- assigns a formal risk appetite to the risk of the organization;
- produces information to help management improve business decisions, reduce uncertainty and provide reasonable assurance regarding the achievement of the objectives of the organization;
- improves the efficiency and delivery of services, improves allocation of resources (capital) to business improvement, creates shareholder value and enhances risk reporting to stakeholders.

ERM in practice

By taking a comprehensive approach to enterprise risk management, a wide range of benefits can be delivered, and these are set out in Table 6.3 and considered in detail in Chapter 22. It is for each organization to decide how the enterprise risk management initiative will be structured and how these benefits will be achieved.

The developing role of the risk manager is discussed in Chapter 24. Their position within the organization will be proportionate to the risks that the organization faces. For many organizations a board-level risk director is often appropriate, who is often referred to as a chief risk officer (CRO). These appointments originated in the energy and finance sectors, but are becoming established in a wider range of organizations.

The seniority of the CRO is just one example of how ERM can be achieved in practice. The actual position within the organization will be set according to what is appropriate to the risk; in other words it will be proportionate, aligned, comprehensive, embedded and dynamic (PACE).

The key feature of ERM is that the full range of significant risks facing the organization is evaluated. The interrelationship between risks should be identified, so that the total risk exposure of the organization may be compiled. Having measured the total risk exposure of the organization, that level of risk exposure can then be compared with the risk appetite of the board and the risk capacity of the organization itself.

Table 6.3 Benefits of enterprise risk management

FIRM risk scorecard	Benefits
Financial	Reduced cost of funding and capital Better control of Capex approvals Increased profitability for organization Accurate financial risk reporting Enhanced corporate governance
Infrastructure	Efficiency and competitive advantage Resilience Improved supplier and staff morale Targeted risk and cost reduction Reduced operating costs
Reputational	Regulators satisfied Improved utilization of company brand Enhanced shareholder value Good reputation and publicity Improved perception of organization
Marketplace	Commercial opportunities maximized Better marketplace presence Increased customer spend (and satisfaction) Higher ratio of business successes Lower ratio of business disasters

ERM and business continuity management

There is an important relationship between enterprise risk management (ERM) and business continuity management. The risk assessment required as part of the risk management process and the business impact analysis that is the basis of business continuity planning (BCP) are closely related. The concept of BCP additionally feeds into the idea of ‘resilience’, which is a concept that is further discussed in Chapter 8.

The normal approach to risk management is to evaluate objectives and identify the individual risks that could impact these objectives. The output from a business impact analysis is the identification of the critical activities that must be maintained for the organization to continue to function.

Based on the definition of ERM set out above and the fact that it applies to core processes, key dependencies, stakeholders’ expectations and protection of the business

model, it can be seen that the ERM approach and the business impact analysis approach are very similar; both approaches require the identification of functions that must be in place for the continuity and success of the business.

Where ERM and BCP differ is in timing and structural elements. ERM is concerned with the management of risks that could impact core processes and looks across the organization in an integrated fashion. Business continuity is concerned with actions that should be taken to maintain the continuity of individual activities. The business continuity approach has the very specific function of identifying responses that should be taken after the risk has materialized in order to minimize its impact. BCP relates to resuming operations with as minimal an impact on the organizations as possible, eg cost containment and customer retention, as described in Chapter 13.

Over the longer term, ERM will enhance enterprise resilience – the ability to anticipate and respond to change. It helps organizations identify factors that represent not just risk, but change, and how that change could impact performance and necessitate a shift in strategy. All organizations need to set strategy and periodically adjust it, always staying aware of both ever-changing opportunities for creating value and the challenges that will occur in pursuit of that value.

Integrating strategy and performance

The COSO internal control model and ERM frameworks of 2004 and 2017 were discussed in Chapter 4. The COSO 2017 framework was a response to the recognition that there needed to be stronger links between strategy, risk and performance. This later ERM framework clearly connects ERM stakeholder expectations, positions risk in the context of an organization's performance, and enables organizations to better anticipate risk.

COSO's *Enterprise Risk Management: Integrating with strategy and performance* was published in June 2017 and provides a framework to enhance management of risk for all types and sizes of organization. It puts forward the argument that integrating ERM practices throughout an entity will help to accelerate growth and enhance performance. The advice is to build on the current level of risk management that already exists in the normal course of business.

This updated COSO ERM framework (2017) adopts a components and principles structure. It clearly differentiates between ERM and internal control, and enhances the references to risk appetite and risk tolerance. The intention of the revised framework is to elevate discussion of strategy, enhance the alignment between performance and ERM, and more explicitly link ERM into decision making. There is greater emphasis on the relationship between risk and value. Also, the benefits of integration of ERM are emphasized. Finally, the revised framework underlines the role of culture in the achievement of successful enterprise risk management.

The framework outlines principles that can be applied from strategic decision making through to performance. It includes a set of principles organized into five interrelated components:

- 1 Governance and culture: Governance sets the tone for the organization and establishes oversight responsibilities for ERM. Culture relates to ethical values, desired behaviours and understanding of risk.
- 2 Strategy and objective setting: ERM, strategy and objective setting work together in the strategic planning process. Risk appetite should be aligned with strategy and business objectives to successfully implement strategy.
- 3 Performance: Risks that can impact achievement of strategy and business objectives need to be identified, assessed and prioritized by severity in the context of risk appetite, so that risk responses can be selected.
- 4 Review and revision: By reviewing entity performance, an organization can consider how well the ERM components are functioning over time and following substantial changes, and what revisions are necessary.
- 5 Information, communication and reporting: ERM requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization.¹

Organizations need to identify the best framework for optimizing strategy and performance in order to integrate ERM throughout the organization to achieve benefits, including:

- Increase the range of opportunities: Identify new opportunities and unique challenges associated with current opportunities.
- Identify and manage risk entity-wide: Identify and manage enterprise-wide risks to sustain and improve performance.
- Increase positive outcomes and reduce negative surprises: Identify responses, reduce surprises and related costs or losses, while profiting from advantageous developments.
- Reduce performance variability: Anticipate the risks that would affect performance and put in place the actions needed to minimize disruption and maximize opportunity.
- Improve resource deployment: Assess overall resource needs, prioritize resource deployment and enhance resource allocation.
- Enhance enterprise resilience: Anticipate and respond to change, not only to survive but also to evolve and thrive.

Note

1 COSO (2017) *Enterprise Risk Management: Integrating with strategy and performance*, www.coso.org/documents/2017-coso-erm-integrating-with-strategy-and-performance-executive-summary.pdf (archived at <https://perma.cc/4KFC-9BYN>)

Implementing enterprise risk management

07

This book is concerned with taking an enterprise-wide approach to risk management and this chapter will take a high-level view of the implementation of the ERM approach in practice. Whilst much of this book considers specific individual risks or approaches to risk management, this is done in order to provide the foundation for the wider ERM philosophy that consolidates the management of individual risks into a unified and consistent approach to risk across the whole enterprise.

The high-level approach taken in this chapter is intended to provide an overview from which the reader can develop their own investigations but with the context of the overall process clearly in mind. To that extent, what follows should be seen as a roadmap for the remainder of the book, as a pointer to further topics, as well as a high-level plan for the implementation of ERM.

Investment in change

Before considering the actions required to implement an ERM approach, it will be necessary to gain senior management approval and support. The full nature of the changes required to implement an ERM approach will depend upon how the organization is currently structured. Moving to a fully mature ERM approach from a risk management style that was, perhaps, more siloed will require cultural as well as organizational change, requiring investment of time and, probably, investment in technology to upgrade recording and analytical processes.

The largest investment to be made is likely to be that of employing a risk manager or a risk management function that will design, facilitate and drive the implementation and running of an ERM framework. In some business sectors, particularly banking and finance, and in some countries of the world, the employment of a chief risk officer (CRO) is becoming a regulatory requirement.

A fully functioning ERM programme will have an impact across the entire organization and, depending on the sector, size, complexity and geographies in which the organization operates, it will take time to be accepted by those actors involved in running the organization. The commitment from the board and extent of active engagement by the leadership of the organization will determine the speed of that acceptance. A period of between three and ten years has been suggested as a reasonable timeframe in which to implement ERM fully.¹ Given the speed of change brought on by technology and shifts in ways of working, it is unlikely that an organization that takes ten years to implement such change will be in existence at the end of that time.

Along with the leadership's commitment, the extent of the investment required to implement the ERM approach should be governed by a sense of proportionality. In the previous chapter the PACED principle was discussed; the ERM approach will need to be proportionate, aligned, comprehensive, embedded and dynamic.

A worthwhile change

Implementing an ERM approach will affect the culture of the organization and the ERM approach will seek to monitor and address aspects of the culture that may require behavioural modification. This can be seen from the lessons learned in the financial crisis, illustrated by the HBOS case study in Chapter 3.

The extent of the impact and changes sought will depend upon the start point, but in order for ERM to be fully embedded and its benefits fully realized the organization will require process and behavioural change from everyone involved. The benefits of an ERM approach are outlined in Chapter 22.

Integrating processes, reviewing and improving

Successful implementation of ERM that brings about cultural change within the organization will, as we have seen, take time to implement. It is likely to be an ongoing process that involves applying an initial methodology and through iterations continuously improving the process, to enable as mature and embedded an approach as possible within the organization.

Whilst ERM is an embedded process in some organizations, and being adopted by others, there is no single, combined or overwhelmingly accepted methodology that forms ERM. It will vary between organizations, based in part on the context of the risks to be managed and in part on the culture and existing processes into which ERM is to be applied.

This isn't about adding new processes; it is about ensuring that effective risk management is integrated in the way we lead, direct, manage and operate. As an integrated part of our management systems, and through the normal flow of information, an organization's risk management framework harnesses the activities that identify and manage the uncertainties faced and systematically anticipate and prepare successful responses.

SOURCE HM Government (2020) *The Orange Book: Management of risk – principles and concepts*, p 6, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866117/6.6266_HMT_Orange_Book_Update_v6_WEB.PDF

Academics have found it difficult to agree a consistent method of application for ERM since the ERM approach has been implemented to overlay against many of the existing processes that the organization undertakes. In other words, its application has been moulded to the existing organization, and not imposed in a pre-determined fashion. This is in accordance with the PACED principle that 'proportionality' is important.

Regulators will rarely impose a precise form in which ERM must be implemented. They will advise which areas they expect to be managed and will judge the appropriateness of that management, but it will remain up to the organization itself how to implement ERM.

The variation in practical application of the methodology contributes to what has been termed an 'ERM mix'² and makes it difficult to characterize the imperatives that must be used. What this book will explain in more detail is that successfully implementing ERM requires the interlinking of two components: the technical aspects of risk management and the practical understanding of the organization into which ERM is to be embedded. The true skill of the ERM implementer is to be able to blend technical knowledge with organizational knowledge.

Plan, implement, measure and learn (PIML)

In Chapter 4 the concept of applying a consistent methodology to change, the PIML approach, was mentioned. The PIML structure is very similar to plan–do–check–act (PDCA). The PDCA construct emanates from the 'quality' management process and can be traced to the 1920s. It is sometimes called the 'Deming' cycle and has had some additions in the intervening years, including 'Observation' as an initial step and 'Study' as an interim step. Regardless of whether it is OPDCA (for observation) or PDSA (with S for study), the main idea is that it is a consistent way of analysing an issue and, through taking planned steps, making an improvement to a process which can be reviewed and then, after further planning, itself improved upon.

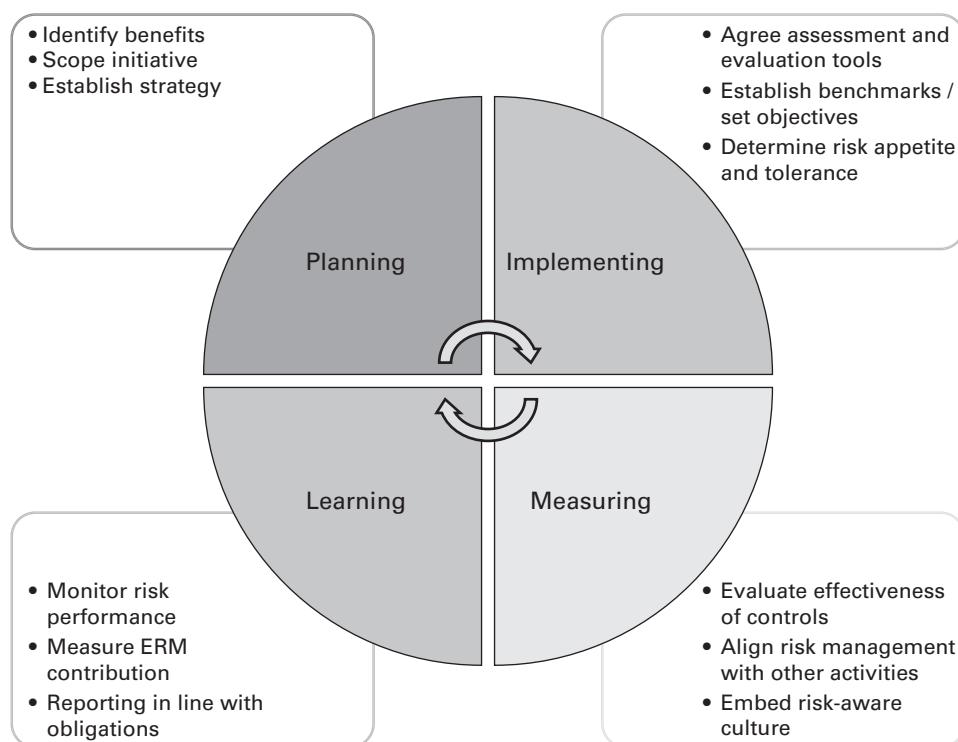
The PIML acronym is preferred in risk management for two reasons. Firstly, it implies a structured and proactive approach that places specific emphasis on measuring and learning, and secondly it distinguishes risk management from quality management.

The key steps to implementing a risk management process are shown in Figure 7.1.

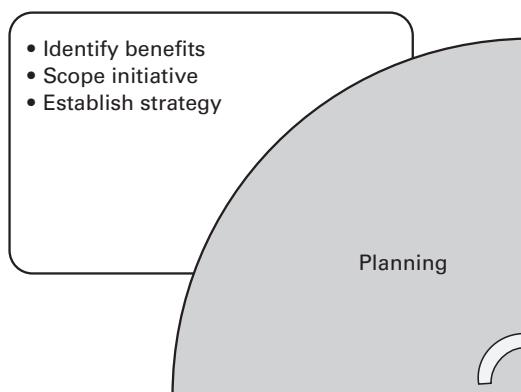
Below is an outline of each stage of the process. The centre arrows indicate that the process is continuous, in that once the process has been completed, from planning through to learning, the final phase leads into a further round of planning improvements after an appropriate time, and regular review is required.

This is more necessary than ever in fast-moving times, given external pressures on an organization, whether brought about through technology improvements, demographic changes, changes to working patterns, the Covid-19 pandemic, or other external changes. For example, a risk management framework that was designed and implemented in the last few years may require revision and update in light of the need to build the risks of climate change into the ERM system. A look at the top ten risks from the World Economic Forum's report of 2020 shows how risks are changing. In the discussion of each stage in the cycle that follows, illustrations of how this might apply to this climate change example have been provided.

Figure 7.1 Implementing risk management by PIML



Planning



In the initial part of the process, it is important to identify and assess the benefits that will arise as a result of the change to be made, either in implementing a new risk management process or by iterations seeking an improvement to the existing process. These benefits can be identified in numerous ways within the context of the organization but suggestions can be made through reviewing the business model, taking into account the interests of all stakeholders (see Chapter 30), which will include external pressures imposed by regulators or the need to contribute to carbon neutrality or other benefits that may be identified in terms of the value added by the ERM approach (Chapter 22).

It is important to identify and have a clear view of the benefits in order to gain acceptance and sponsorship from the board or controlling powers in the organization. Once benefits are established, the planning phase will lead to more detailed scoping of the ERM initiative itself. This may require the development of a common taxonomy or defining improvements within the existing and well-understood language of the organization itself. Using existing phraseology often enables greater traction for the exercise through easier acceptance of the change required.

Simply controlling or eliminating risk from the organization is not taking an enterprise-wide (ERM) approach, but may be more commonly found in a health and safety or compliance regime. A key difference of an ERM approach is that it seeks to exploit the advantages of taking risk, where the ambition is not to just maintain value, but also to create and add value to the organization.

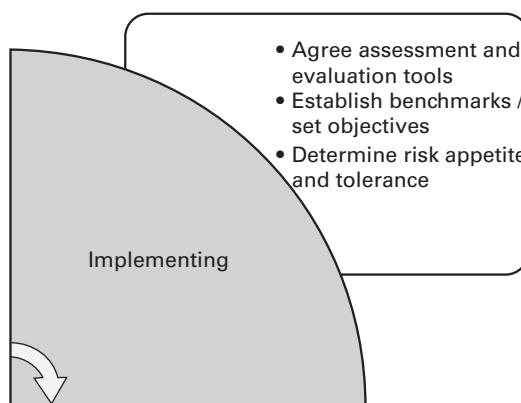
The final element of this phase will be to establish the strategy, framework and the roles and responsibilities of the people who will implement the change required. This is discussed in Chapter 23 and may involve outlining documentation such as the risk management manual, or establishing new procedures that need to be accepted. This documentation, along with other risk management tools, will be used in the next phase of the process.

For example, if improving an embedded risk management system to cater for climate change, issues that may have emerged may require an agreed taxonomy of risk. For climate change, three risk categories have been identified: physical, legal and transition risk. These will need to be defined specifically for the organization itself.

Gaining acceptance and sponsorship from the board may require providing evidence from other sectors, for example the finance sector, of the drive to encourage decarbonization. This may for instance focus on the probable inability to access adequate insurance capacity to satisfy the demands of investors by 2025 if the activity includes the mining of fossil fuels.

Lastly, identifying the benefits of incorporating climate change into the ERM process might focus on being a more attractive proposition for the investment community and as a result reducing the costs of capital. This benefit might arise if the organization was the first in the sector to provide meaningful measures that institutional investors could assess, and by doing so create a higher demand to invest in their stock, reducing the requirement to deliver higher returns.

Implementing



This is the main phase of the change programme and will involve adopting or adapting some of the key technical features of ERM discussed in more detail in later chapters. For example, the production of risk management guidelines (see Chapter 23), risk classification systems (see Chapter 11), and risk protocols (see Chapter 10), using different protocols such as FIRM, PESTLE or SWOT.

This phase may also involve undertaking exercises within the organization to gain information or initiate the process of gaining acceptance to the initiatives that are

being implemented. This may involve risk assessment workshops, producing and agreeing risk registers, or designing or improving risk management information systems (RMIS) (see Chapter 27).

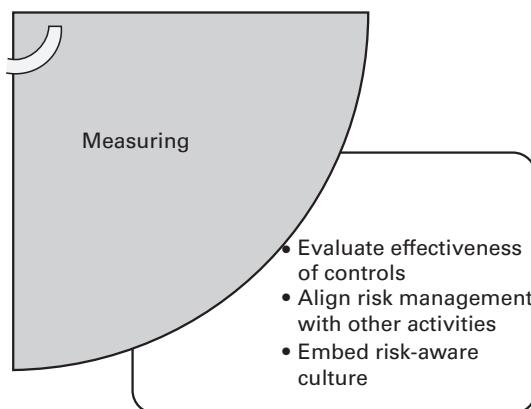
The final element will involve designing or setting some measurements, such as determining and agreeing the organization's risk appetite and risk tolerance levels, or evaluating the existing controls.

In the example of implementing a risk management system to cater for climate change issues, this may involve amending the risk management guidelines to include principles around activities requiring environmental assurance or carbon reduction protocols.

It could also, for example, involve running risk assessment workshops with managers, informed by details of recent or upcoming legal challenges expected from activists in other sectors to assess the likelihood such challenges might transfer across sectors.

Lastly, it is likely that the board will need to consider and agree a statement of its attitude to climate change and the activities it will undertake to become carbon neutral by a certain date. The risk function will need to build these statements into an action plan that can be monitored and reviewed.

Measuring



The emphasis on measurement is perhaps a main feature of risk management and goes beyond the 'check' phase of PDCA in the sense that it will overlap with internal audit in terms of measuring the effectiveness of existing controls and introducing improvements.

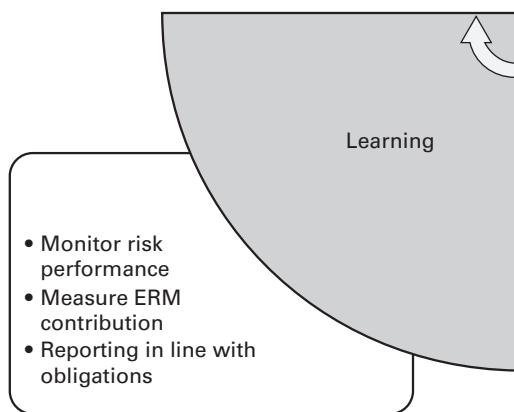
To become embedded in the organization's activities, the processes should have been designed to be aligned as far as possible with the existing processes taking place within the organization. This phase may involve monitoring in more detail the risk improvement plans or reaction planning such as business interruption analysis (See Chapter 19).

Within this phase, if RM activities are aligned with others in the organization then the ERM will start to embed a risk-aware culture within the organization and it will become 'second nature' in terms of resource allocation and wider communications within the organization.

For example, measurement of the risk management system that has been altered to cater for climate change issues will require analysis of the carbon footprint and performing risk impact analyses on activities that may reduce the footprint.

It may involve measuring how the organization's activities will be changed as a result of different scenarios of temperature increase. An example can be seen in the UK National Trust's analysis in March 2020 of the threat to their estate at a 'worst-case model of no intervention'. They will use the analysis to establish actions that can be taken to mitigate the physical risk they have identified.³

Learning



The final phase before again reviewing the phases, involves learning from the measurement activity. This will take the form of monitoring and reviewing risk performance indicators to measure ERM contribution. It may involve work with an internal audit team to contribute to the audit plan or reviewing a learning from any self-assessment (control risk self-assessment – CRSA) forms that have been completed (see Chapter 34).

Included within this phase will be reporting of risk performance internally to the board. External stakeholders such as listing bodies like the London Stock Exchange or the New York Stock Exchange will require reports on the ERM processes to be published. Additionally, many rating agencies will specifically consider the ERM processes of an organization before assigning a credit score. In our climate change example, this might involve producing reports for external stakeholders on the risks that have been identified or alerting investors to the processes that are in place in respect of climate change activities.

The ERM process might also take the measures of output from the activities and identify ways in which the organization might benefit from further modification of the ERM process, for example by investing in technology to enable more granular assessment of outputs to establish defences to possible future legal challenges.

Notes

- 1 Shortreed, J (2010) ERM frameworks, in *Enterprise Risk Management*, ed J Fraser and B Simkins, John Wiley & Sons, New York; Association of Federal Enterprise Risk Management (2021) How long does it take to implement a fully compliant ERM program? www.aferm.org/ask-the-expert/how-long-does-it-take-to-implement-a-fully-compliant-erm-program/ (archived at <https://perma.cc/R2KB-TK28>)
- 2 Mikes, A and Kaplan, R (2014) Towards a contingency theory of enterprise risk management, Working Paper 13-063, Harvard Business School, www.hbs.edu/ris/Publication%20Files/13-063_5e67dffe-aa5e-4fac-a746-7b3c07902520.pdf (archived at <https://perma.cc/8ASN-TBGZ>)
- 3 National Trust (2021) National Trust maps out climate threat to coast, countryside and historic places, www.nationaltrust.org.uk/press-release/national-trust-maps-out-climate-threat-to-coast-countryside-and-historic-places (archived at <https://perma.cc/VS9M-KNSH>)

The context for ERM

08

Changing face of risk management

As with any management initiative that becomes embedded within the way the organization operates, a successful risk initiative should develop and become more sophisticated over time. Developments in the discipline of risk management, especially during the past 10 years, have been dramatic; technology has enabled better reporting, recording, analysis and quantification of risk. Regulation, which has forced some sectors to introduce new risk techniques such as enhanced accountability, could be said to have 'seeped' into other sectors, in particular for listed companies, and has driven the requirement for more extensive risk management reporting and transparency. In the UK, the Wates principles require boards to have a clear understanding of the views of shareholders, including those with a minority interest; larger companies must report on their stakeholders.

The universally accepted terminology for the broad application of risk management across the whole organization is enterprise risk management. Similarly, operational risk management (ORM) has been established and developed very substantially. The risk management discipline as a whole continues to develop and derive opportunity from newly available techniques, brought about by enhanced availability of data sources and rapidly advanced processing power.

There is a need for the continued education and training of boards and senior members of those boards to maintain knowledge of the changing basis on which risk management analysis and advice is offered. Without 'laying the groundwork', the risk management department could stand accused of changing the nature of the risk management process and sow confusion and lack of interest amongst the senior board members.

Lessons from the past: Financial and health crises

Any review of the changing face of risk management has to acknowledge two global crises: the Covid-19 pandemic originating in China in 2019 and the global financial

crisis (GFC) of 2008/9. These global events have similarities but can also show us how the risk management practice has developed over the intervening years.

The argument might be offered that risk management failed to adequately prevent the financial crisis and also failed to mitigate the effect of the pandemic. In some circles a cynicism may have arisen as to the application of ERM processes, and the risk manager needs to be aware of evidence to rebut these ideas and to argue their case for resources.

Firstly, as to risk identification, both Covid-19 and the GFC were foreseen events. For example, the warning from Mr Moore to HBOS (in Chapter 3) was not the only counsel to go unheeded in the financial services sector prior to 2008. The probability of a pandemic had been identified as a likely global risk event, and indeed it had been foreshadowed by the SARS, Ebola, and Zika viruses. Risk management responses had been applied to the extent that the USA set up the Directorate of Global Health Security and Biodefense (DHSB) in 2016 specifically to respond to these events. The UK had run Exercise Cygnus in 2017 to identify any weaknesses in their health preparedness for similar events.

Secondly, in terms of actions to limit loss (the inherent and residual risk), it is instructive to note how these events were handled differently in different regions. For Covid-19 in particular, some countries took little coherent action, Brazil being a case in point, which may be our best example of an inherent risk without any control measures. In the East, governments had experience of health crises (for example, SARS) and had better-developed and recently deployed systems to use to protect their citizens. Here we might see a target risk after control measures taking place.

There had also been a banking crisis, ‘the Asian contagion’ in 1997, which meant action was taken swiftly to provide liquidity in Asian economies, which was not replicated in the West. Whilst interconnectedness meant Covid-19 and the GFC impacted both regions, the East could be said to have mitigated the effects of both better than the West.

Lastly, both events can provide learning points for the impact of timely actions. During the GFC, governments acted quickly and in a co-ordinated fashion to provide immediate relief, albeit that the West required this to a greater extent. Regulators followed with new rules on capital building and management behaviour.

In the aftermath of Covid-19 lessons will be learnt, but it could be said that most governments acted quickly and science resources were co-ordinated to speed vaccine development. The country with the highest health spend and seemingly best prepared to provide mitigating actions, the USA, failed to act in a concerted fashion, with the resultant negative impact on its citizens. In the UK the government failed to take the threat seriously at an early stage, was consistently poor in implementing actions in a timely manner, and has been said to have repeated the same mistakes time after time.

For the risk management profession there are lessons on how risk management was deployed. In the GFC the example from HBOS in Chapter 3 is clear that technically qualified risk managers are important. In respect of Covid-19 the USA would

undoubtedly have been better off if they had not dismantled the DGHSB in 2018 for political reasons. Both of these examples indicate that risk management messages are sometimes disregarded with calamitous consequences. Senior risk managers need to provide compelling evidence and argument to enable the deployment of effective and well-resourced risk management practices, and sometimes need to show courage to make sure their messages are heard.

The power of taking risks

It is undoubtedly the case that taking too much risk may be inappropriate and can result in the failure of the whole organization. However, for many organizations, losses caused by aggressive risk taking are survivable. Understanding the level of risk embedded in an organization should not put a stop to all bold strategic decisions. Risk awareness should not prevent an organization embarking on a high-risk strategy, but should enable decisions to be taken on an informed basis.

Organizations should continue to look for opportunities and, from time to time, acknowledge that there is a good opportunity that is high risk. The organization can still embark on that strategy, but should understand how to manage the risks so as to remain within appetite, and measure the risks so that the board is aware of the actual exposure.

Figure 26.1 illustrates where an organization's risk appetite and capacity might fall within a risk matrix. If the organization is risk aggressive and operates in the 'critical zone' identified in Figure 26.1 they should identify ways to increase their risk capacity in that specific instance, or stand accused of being reckless rather than risky. For example, risk may be transferred through contractual means, diminished by establishing a joint venture or through financial means such as insurance. The board will need to revisit risk assessments, challenge the scope and results of risk analysis activities, and ensure that a highly dynamic approach to risk management is maintained at all times and at all levels in the organization.

As a general principle, a risk matrix helps to prioritize risks and show which are considered the most significant. It should be noted that risk appetite and capacity can change over time so that at some point risks in the comfort zone might subsequently fall outside of appetite.

Managing emerging risks

All organizations are concerned about changes in the external and internal context that give rise to new challenges. These changes can be considered to be the emerging

risks facing the organization. The International Risk Governance Council defines these risks as:

a risk that is new, or a familiar risk in a new or unfamiliar context or under new context conditions (re-emerging). Emerging risks are issues that are perceived to be potentially significant but which may not be fully understood and assessed, thus not allowing risk management options to be developed with confidence.¹

Consideration of these risks can be difficult unless the organization clearly understands the nature of the emerging risks that it faces. Following the above definition emerging risks can be divided into three categories:

- new risks that have emerged in the external environment, but are associated with the existing strategy of the organization – new risks in a known context;
- existing risks that were already known to the organization, but have developed or changed circumstances have triggered the risk – known risks in a new context;
- risks that were not previously faced by the organization, because the risks are associated with changed core processes – new risks in a new context. This last category is where the risk manager will have the least confidence and will need to actively seek further information.

The level of risk faced by organizations is constantly shifting, caused by increased interconnectedness, new technology and increasingly complex supply chains. Some of these increasing risks will be under the control of the organization itself but many emerging risks will not be within the control of an individual organization, including:

- government direction;
- climate change;
- sovereign debt;
- national security;
- changing demographics.

When seeking to manage these changes in context, an organization should evaluate whether the risks are to be treated as hazard, control or opportunity risks. Depending on the activities of the organization, many of these emerging risks may simply be threats to the organization or represent opportunities for future development. In some cases, the emerging risks will simply represent additional uncertainties that need to be managed.

An important consideration when thinking about emerging risks is the speed at which they can become significant. Some risk management practitioners refer to the speed of development and change of risks as the risk velocity.

A good example of emerging risk is nanotechnology.

The risks of nanotechnology

Nanotechnology is used extensively in the medical and, to some extent, cosmetics industry to improve the effectiveness of cosmetic treatment of skin conditions. Whether any long-term risks will emerge from the use of nanotechnology has not yet been fully established. As nanotechnology is an emerging field, there is great debate regarding the extent that it will benefit or pose risks for human health. Nanotechnology's health impact can be split into two aspects: the potential for medical applications to cure disease, and the potential health hazards posed by exposure to nano-materials.

The extremely small size of nano-materials means that they are much more readily taken up by the human body than larger-sized particles. How these nanoparticles behave inside the organism is not fully resolved and cannot be without being applied at some scale. Health and environmental issues combine in the workplace of companies engaged in producing or using nano-materials and in the laboratories engaged in nano-science and nanotechnology research.

Increasing importance of resilience

In recent years, there has been an increasing interest in the topic of resilience. Governments and local or municipal authorities recognized during the 1990s and 2000s that society in general, and communities in particular, had to become more resilient to cope with civil emergencies, as well as natural catastrophes such as earthquakes and extreme weather events. Although the initial concern with resilience may have started with the consideration of how to respond to wide area events, broader concerns have developed.

The increasing awareness and concern in relation to resilience was demonstrated by the replacement of the 2006 British Standard *BS 25999-1:2006 Business Continuity Management: Code of practice* with ISO 22301. Standards for these areas are set out in *ISO 22316:2017 Security and Resilience: Organizational resilience — Principles and attributes*. Chapter 19 discusses resilience in greater detail.

This ASIS standard takes an enterprise-wide view of risk management, enabling an organization to develop a comprehensive strategy to prevent when possible, prepare for, mitigate, respond to, and recover from a disruptive incident. This allows integration with ISO 31000. It is also compatible with existing ISO management system standards (such as ISO 9001, ISO 14001, ISO 27001 and ISO 28000). The overall approach is that a resilient organization needs to ‘prevent, protect and prepare’ in relation to resources and assets, and at the same time be able to ‘respond, recover and review’ when a crisis occurs.

When seeking to make an organization more resilient, it is essential to have a definition of the desired state of resilience that is being sought. It has been defined as the ‘ability to absorb and adapt in a changing environment’. This is a useful definition, but resilience is often associated with crisis management, and this definition does not explicitly address the behaviour of an organization during a crisis. Perhaps a better definition would be the ‘capacity of an organization to consistently achieve a desired state following a change in circumstances’. This definition is more inclusive of the management of a crisis, as well as the ability to successfully respond to less dramatic or disruptive events.

The emergence of resilience is an opportunity for risk management and business continuity management specialists to work more closely together to ensure a more co-ordinated approach to enterprise risk management, emergency management, crisis management, disaster management and business recovery. There are three behaviours that should be achieved by an organization if it is to achieve increased resilience:

- awareness of changes in the external, internal and risk management environments, so that constant attention to resilience is ensured;
- ‘prevent, protect and prepare’ in relation to all types of resources, including assets, networks, relationships and intellectual property;
- ‘respond, recover and review’ in relation to disruptive events, including the ability to respond rapidly, review lessons learnt and adapt.

As the increasing importance of resilience is recognized, advice on achieving resilience is becoming more widespread.

Note

- 1 IRG (2019) Governance of emerging risks, <https://irgc.org/risk-governance/emerging-risk> (archived at <https://perma.cc/XTE9-GV7T>)

Setting objectives 09 for ERM

Setting objectives for the ERM approach is intrinsically associated with the objectives for the organization as a whole. Making sure that the ERM objectives are aligned with the organization's objectives is therefore critical if the ERM approach is to be embedded correctly.

In terms of the risks to be managed, Figure 1.2 showed where risks attach in terms of the mission of the organization and flowing down from the strategic plan. Here it could be considered that certain risks 'attached' to aspects of the business in terms of key dependencies, core processes, stakeholder expectations or, finally, corporate objectives. It can be seen therefore that both the risk management process and the identification of the risks themselves are intimately related to the objectives of the organization.

Therefore, a clear understanding of the organization's objectives is critical. Any misalignment of these objectives could be a risk in itself, as this could mean the risk management activity may support incorrect, unclear or vague objectives, leading to excellent risk management but of the wrong risks. In this section we consider the aspect of risks attaching to the objectives of the organization.

Risk management standards and objectives

The various risk management standards that have been discussed all consider objective setting to be important. Both COSO and ISO have statements that are concerned with objective setting.

In 2004 COSO issued its 'cube' (see Figure 4.3), which has objective setting in the second row after the internal environment. The text states that 'the board should set objectives that support the mission of the organization that are consistent with its risk appetite.' If the board is to set objectives effectively, it needs to be aware of the risks arising if different objectives are pursued.

The COSO framework was supplemented in 2017 with the rainbow double helix, which states: 'Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.' It further states that 'There

is a direct relationship between objectives, which are what an entity strives to achieve, and enterprise risk management components, which represent what is needed to achieve them'.¹

Strategy and objectives in standards

It can be seen by considering these standards that ERM, strategy and objective-setting are closely aligned and need to be integrated to work together in the strategic planning process. The ERM approach should ensure that the organization takes into account its risk appetite when framing its strategy. The strategy will in turn enable objectives to be designed and implemented and these objectives in turn will serve as a basis for identifying, assessing and responding to risk.

Again, in COSO 2017 the Executive Summary states, 'Enterprise risk management is as much about understanding the implications from the strategy and the possibility of strategy not aligning as it is about managing risks to set objectives'. Overall, therefore, the strategy is paramount: the ERM approach will inform strategy but strategy must come first. Whilst easily said, this can still be challenging for the risk management practitioner for the following reasons.

Firstly, we should assume the organization has a consistent mission which is agreed upon by all senior management. From this it will be necessary to choose a range of suitable objectives that support the mission. This can be more challenging and will require consensus between senior management and the various stakeholders whose expectations need to be met. At this stage risk appetite will be an important factor in both making the choice of strategy and communicating that strategy to stakeholders.

Secondly, strategy does not exist in isolation: it will have been set according to the context of the organization at a point in time. That context will change, either gradually or through some form of disruptive activity caused by events such as technology failure. So, there will need to be a review of strategy at appropriate intervals, at which point it will be necessary to update and align the ERM approach to any newly aligned strategy.

Thirdly, in some organizations, and particularly large, geographically dispersed organizations, there may be different interpretations of the mission, and from that there may be a difference in the implementation of the strategy. This is where the culture of the organization will play a part and, as Peter Drucker the management educator said, 'culture eats strategy for breakfast'! By this he was meaning that the organization's culture is the dominant factor in its success and is clearly critical in terms of an agreed interpretation of the mission.

Fourthly, and linked to both the cultural issue discussed above and the requirement for consensus amongst management to the strategy, there is a need for the strategy to be accepted by all. There will be different agendas amongst management who have to deliver on the objectives that have been set and it will be important that those ‘informal’ objectives are aligned as far as possible to the formal objectives of the organization. Where they are not it can become toxic for an organization and at the extreme may need some ‘fresh thinking’ to deliver the objectives.

Lastly, it is important that the ERM approach does not overwhelm the setting of strategy, and therefore objectives. If ERM plays too great a role in the activity it may lead to the organization becoming overly risk averse and reducing its exposure to risk by being less ambitious in its strategy and setting too easily achievable targets.

Implementing objectives

The objectives once agreed will need to be cascaded in some form from the centre to each division or business unit that delivers the output of the organization and from there to each team or individual. It will be necessary to set some form of time period within which the objectives are to be achieved, and this should also be communicated at the organizational, divisional and team or individual level. Typically, organizations will seek to implement objectives over a one- to-three-year time horizon depending upon complexity. That time period will shorten as objectives are cascaded downwards, as shown in Figure 9.1.

Along with time period in which to achieve objectives, it is important that there is a way of determining whether an objective has been achieved, and if so by how much. In other words, to be able to measure its realization some way. This may be challenging in an ERM setting where the ERM practitioner is being set objectives and at a strategic level the objective is to reduce risk.

From the tactical level this may be translated into quantitative terms in order to provide a measurability. This may not be available for all objectives, however, and more qualitative aspects of reducing risk may have objectives set around specific tasks to accomplish in a set period. For example, improving culture as a strategic objective may be translated to tactics such as running training or workshops. Measurability may be provided by some form of feedback scores from attendees. Care needs to be taken in more qualitative areas as they can provide an opportunity for ‘gaming’ the system by that individual, which would not achieve the stated intention of reducing risk.

Figure 9.1 Three levels of objective setting



Objectives need to be set in reality and with sufficient resources available to achieve them. And, finally, there must be a specific outcome to be achieved. The objectives will need to meet the SMART test as shown here. SMART objectives are:

- Specific
- Measurable
- Achievable
- Realistic and resourced
- Time limited

Aligning objectives to risk management principles

In Figure 9.1 it is noted that there needs to be alignment between each level of objective and the risk management perspective. This is because objectives are delivered by individuals, and different individuals respond to different criteria. There needs to be alignment between the longer- and shorter-term objectives, and between individual actions and organizational outcomes.

For example, how staff are rewarded according to the achievement of their objectives can have a significant effect on risk culture. Rewards that provide immediate and large bonus payments for the achievement of short-term gains may promote a culture of excessive risk taking, for instance by the aggressive selling tactics of banks prior to the global financial crisis. It was for this reason that ‘clawbacks’ were introduced to many financial services bonus arrangements in order to promote a longer-term perspective on risk taking. These clawbacks allow an organization to recover some element of previously paid bonuses should outcomes change over the longer term.

The Institute of Operational Risk recommends that ‘relevant professionals, from the operational risk function and the HR function, should be consulted about the organization’s performance management and appraisal strategy to ensure that it promotes an appropriate risk culture’.² They recommend, for example, that to help promote an appropriate risk culture, rewards are based on longer-term performance criteria such as customer satisfaction and retention, or profits over periods longer than one year, and that appraisals should reflect concern for operational risk and its management, as well as profit and sales growth.

Notes

- 1 COSO (2017) *Enterprise Risk Management: Integrating with strategy and performance*, www.coso.org/documents/2017-coso-erm-integrating-with-strategy-and-performance-executive-summary.pdf (archived at <https://perma.cc/DV2C-EDT5>)
- 2 Institute of Operational Risk (2021) Sound practice guidance, www.ior-institute.org/sound-practice-guidance (archived at <https://perma.cc/RT4C-WX6K>)

THIS PAGE IS INTENTIONALLY LEFT BLANK

PART THREE

Assessment

and analysis

LEARNING OUTCOMES

Having studied this section readers will be able to:

- Describe the importance of risk assessment as a critically important stage in the risk management process.
- Summarize the most common risk assessment techniques, plus the advantages and disadvantages of each technique, including SWOT.
- Explain the importance of the long-term attitude of an organization to risk and how that affects the perception of risk.
- Describe options for classifying risks according to the nature, source, timescale, impact and consequences of the risk.
- Describe the importance of risk classification systems and describe the features of the established systems, including PESTLE, FIRM and the 4Ps.
- Explain the attributes of each risk characteristic and illustrate by means of a risk matrix the nature and attributes of a risk in terms of likelihood and impact.
- Illustrate, by using a risk matrix, the risk attitude of an organization and the importance of the concept of the ‘universe of risk’.
- Provide examples of the use of a risk matrix, including using it to indicate the dominant risk response in each quadrant: tolerate, treat, transfer and terminate (the 4Ts).

- Describe the main components of loss control as loss prevention, damage limitation and cost containment, and provide practical examples.
- Summarize the alternative approaches to defining the upside of risk and the application of these approaches for core processes.

Further reading

- Government of Western Australia (2011) *Western Australia's Risk Management Policies and Insurance Strategies for Essential Public Assets*, www.wa.gov.au/sites/default/files/2020-02/western-australias-risk-management-policies-insurance-strategies-essential-public-assets.pdf
- Hillson, D (2016) *The Risk Management Handbook: A practical guide to managing the multiple dimensions of risk*, Kogan Page, London
- Hillson, D (2020) *Capturing Upside Risk: Finding and managing opportunities in projects*, Routledge, Abingdon
- HM Government (2020) *The Orange Book: Management of risk – principles and concepts*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866117/6.6266_HMT_Orange_Book_Update_v6_WEB.PDF
- Institute of Risk Management (2011) Risk appetite and tolerance, www.theirm.org/what-we-say/thought-leadership/risk-appetite-and-tolerance/
- ISO (2009) *IEC 31010:2019: Risk management – Risk assessment techniques*, www.iso.org/standard/72140.html
- Taylor, E (2014) *Practical Enterprise Risk Management*, Kogan Page, London

CASE STUDIES

The student can review the following examples to illustrate further the areas discussed in Part Three and throughout this book.

British Land: Risk assessment

British Land is a large UK-based property developer and owner of real estate, mainly London-based office and retail, with a move into residential. Their 2020 accounts have a large section on how Covid-19 has affected their operations to the date of reporting, and clearly outline the effects on their customers leasing their properties and the rental payments flow.

Their risk management section discusses their 'top down' and 'bottom up' approach, and follows a similar path to that of DP World. Of interest in Part Three is their risk

assessment analysis, where they graphically show the change in risks over the course of the year. They noted increases in risk due to economic outlook, office and retail investment and occupier markets, their investment strategy and sustainability of income. This was tracked against their strategic priorities and displayed as a 'heat map', which shows risks moving substantially up the scale of increased likelihood and impact.

*Edited extracts from: British Land (2020) *Places People Prefer: Annual report and accounts 2020*, www.britishland.com/sites/british-land-corp/files/investors/results-reports-presentations/2020/annual-report-and-accounts-2020.pdf*

Softcat plc: Risk appetite

Softcat is a leading supplier of IT infrastructure focused on: cyber security, IT intelligence, hybrid infrastructure and digital workspace tools. Its strategy is centred on leveraging data to make systems more efficient, navigating the on-premise data centre versus cloud computing conundrum, and helping to facilitate remote working.

In a discussion of risk management, which has a focus on security as an IT company, they discuss their generally low risk appetite but state:

we... have a strong desire to grow our technical capabilities, our customer base and our income. As a result, we rely on our open culture to empower our employees to develop the business and will review individual opportunities as they arise. In situations where our financial and/or reputational exposure is limited or can be mitigated, our appetite for risk in order to achieve strategic growth may be higher.

After a discussion of the architecture of their risk management framework, they outline their principal risk and uncertainties, which are clearly aligned to the strategy of the company.

Their operations benefitted from the rapid move to off-premises working during the Covid-19 pandemic and they discuss how they managed their exposures, particularly to credit risk.

*Edited extracts from: Softcat plc (2020) *Care: Annual report and accounts 2020*, https://d2v35wnqk1ks61.cloudfront.net/3416/1417/4247/Softcat_plc_Annual_Report_and_Accounts_2020.pdf*

Darktrace: Governance of risk management

Darktrace is a privately held company which uses artificial intelligence as a way of neutralizing cyber threats to an organization. It relies heavily on mathematically based learning behind its algorithms, which supports the software used to continuously scan customer IT systems for cyber threats. It has 1,500 employees, is headquartered in Cambridge, UK and operates globally.

As a private company, it is not required to present a full outline of its risks and systems but it does reveal on its website details of its governance systems and what its risk management committee does. This includes advising ‘the board on the company’s overall risk appetite, tolerance and strategy, and the principal and emerging risks the company is willing to take in order to achieve its long-term strategic objectives’.

It takes an enterprise-wide approach to risk as the risk committee’s remit extends to advising its board:

on the risk aspects of proposed changes to strategy and strategic transactions including acquisitions or disposals, ensuring that a due diligence appraisal of the proposition is undertaken, focusing in particular on implications for the risk appetite, tolerance and strategy of the company, and taking independent external advice where appropriate and available.

Edited extracts from: Darktrace website (www.darktrace.com/en) and terms of reference: Darktrace (2021) Governance, <https://ir.darktrace.com/governance/documents>

Assessing risks

10

Considerations, causes and consequences

Importance of risk assessment

Risk recognition and risk rating together form the risk assessment component of the risk management process. Risk assessment involves the recognition of risks and the rating of them to determine the significant risks facing the organization, project or strategy. It is defined in British Standard BS 31100 as the overall process of risk identification, risk analysis and risk evaluation. Because the risk management input into strategy focuses on improved decision making, risk assessment is the main risk management input into strategy formulation.

Risks may be attached to corporate objectives, stakeholder expectations, core processes and key dependencies. Whichever of these features is selected as the starting point, risk assessment can be undertaken. The purpose of risk assessment is to identify the significant risks to an organization. A risk is significant if it could have an impact in excess of the benchmark test for significance for that type of risk. Identification of potentially significant risks will be undertaken during a risk recognition exercise. It is necessary to decide the:

- magnitude of the event should the risk materialize;
- size of the impact that the event would have on the organization;
- likelihood of the risk materializing at or above the benchmark;
- scope for further improvement in control.

Although risk assessment is vitally important, it is only useful if the conclusions of the assessment are used to inform decisions and/or to identify the appropriate risk responses for the type of risk under consideration. It should be considered as the starting point of the risk management process and it is certainly not an end in itself. Managing risk is the priority rather than simply recording risk.

An important feature of undertaking a risk assessment is to decide whether the identified risk is going to be evaluated at the inherent level or at the current (or residual) level. Assessment of inherent risk is undertaken without taking account of the controls that are currently in place. Once assessed without controls, the further assessment of risk with controls in place, or planned controls, enables benefits to be revealed. This topic is discussed in more depth in Chapter 12.

Approaches to risk assessment

There are a number of approaches that can be taken when planning how to undertake risk assessment. Before conducting the risk assessment, it is important to determine the participants in the risk assessment exercise. This can be achieved in one of two ways:

- senior management leading the process with information passed downwards for validation, as a top-down exercise; or
- by involving individual members of staff and local departmental management, as a bottom-up approach.

The opinion of the chief executive officer (CEO) is critically important, especially as it helps to define the overall attitude of the organization to risk. The CEO will be able to provide a structured view of the significant risks faced by the organization but the CEO's focus is likely to be on external risks.

In general, the overall approach by the organization to risk assessments will be heavily influenced by the risk assessment techniques that are selected. It is important that the approach that is adopted is consistent with the culture of the organization. For example, it should be considered whether an organization processes information best through workshops, or through written and structured reports.

Technology such as 'crowd sourcing' software has become available in recent times and offers benefits of speed and a more dynamic approach to updating risks and monitoring emerging trends. Technology can provide additional information in the assessment of risk from different areas of the organization. If there is a broad spread of opinions, this needs to be explored, because it could represent a possible misunderstanding of the nature of the risk being discussed.

Table 10.1 provides examples of advantages and disadvantages of undertaking a top-down risk assessment exercise. A top-down risk assessment exercise will tend to focus on risks related to strategy, tactics, operations and compliance (STOC), in that order.

Table 10.2 provides examples of advantages and disadvantages of undertaking a bottom-up risk assessment exercise. A bottom-up risk assessment exercise will tend to focus on risks identified as compliance, hazard, control and opportunity in that order.

For most organizations, a combination of top-down and bottom-up risk assessments will be undertaken, with the risk manager collecting information from as many stakeholders as possible. Often, the main constraint in undertaking a bottom-up exercise is the greater time commitment that is required from the risk management department to attend and/or facilitate a series of risk assessment exercises.

Table 10.1 Top-down risk assessment

Advantages	Disadvantages
Likely to result in an enterprise-wide approach – the risks at the top will have impacts throughout the business.	Senior managers and directors tend to be more focused on risks external to the organization.
The most significant strategic risks for the organization can be captured quickly and there will be a manageable number.	Limited awareness of internal operational risks or interdependencies of risks within the business.
Shows risk management buy-in from the top, resulting in acceptance of risk management activities at all levels.	Danger that the approach becomes too superficial, because senior managers believe they can manage crises.
Since it originates from the top, there is likely to be consistent methodology throughout the organization.	New risks emerging from the operational activities of the organization might not be fully identified.

Table 10.2 Bottom-up risk assessment

Advantages	Disadvantages
Significant buy-in at all levels of the organization should be achieved.	There will be little focus on external risks or strategic risks.
Can be mirrored to an existing organization chart, and risk impacts beyond immediate operational risks can be discussed.	Time-consuming and may demotivate, if it takes longer to develop the overall enterprise results.
Operational staff have great awareness of local risks and their causes, which might elude higher levels of management.	Danger that the approach becomes too detailed and blinkered, resulting in a silo approach to risk assessment.
Methodology can be varied according to local norms and culture and this is useful for a multinational organization.	New risks emerging from the operational activities of the business might not be reported by operational staff.

Risk assessment techniques

There is a wide range of risk assessment techniques available. The ISO International Standard *IEC 31010:2019: Risk management – Risk assessment techniques* was published in 2009 and provides detailed information on the full range of risk assessment

techniques that can be used. Table 10.3 lists the main risk assessment techniques that are commonly used and provides a brief description of each of these techniques. A widespread form of risk assessment is the use of checklists/questionnaires and the use of brainstorming sessions, normally during risk assessment workshops.

Checklists and questionnaires have the advantage that they are usually simple to complete and are less time-consuming than other risk assessment techniques. However, this approach does have the potential disadvantage that any risk not referenced by appropriate questions may not be recognized as significant. A simple analysis of the advantages and disadvantages of each of the most common risk assessment techniques is set out in Table 10.4.

Given that risks can be attached to other aspects of an organization as well as or instead of objectives, a convenient and simple way of analysing risks is to identify the key dependencies faced by the organization. Most people within an organization will be able to identify the aspects of the business that are fundamentally important to its future success. Identifying the factors that are required for success will give rise to a list of the key dependencies for the organization.

Key dependencies can then be further analysed by asking what could impact each of them. If a hazard analysis is being undertaken then the question is: ‘What could undermine each of these key dependencies?’ If control risks are being identified, then the question can be asked: ‘What would cause uncertainty about these key dependencies?’ For an opportunity risk analysis, the question would be: ‘What events or circumstances would enhance the status of each of the key dependencies?’

Table 10.3 Techniques for risk assessment

Technique	Brief description
Questionnaires and checklists	Use of structured questionnaires and checklists to collect information that will assist with the recognition of the significant risks.
Workshops and brainstorming	Collection and sharing of ideas at workshops to discuss the events that could impact the objectives, core processes or key dependencies.
Inspections and audits	Physical inspections of premises and activities and audits of compliance with established systems and procedures.
Flow charts and dependency analysis	Analysis of the processes and operations within the organization to identify critical components that are key to success.
Crowdsourcing technology	Use of mobile applications to enable individuals to upload their views on risks to a data platform.

Table 10.4 Advantages and disadvantages of risk assessment techniques

Technique	Advantages	Disadvantages
Questionnaires and checklists	Consistent structure guarantees consistency Greater involvement than in a workshop	Rigid approach may result in some risks being missed Questions will be based on historical knowledge
Workshops and brainstorming	Consolidated opinions from all interested parties Greater interaction produces more ideas	Senior management tends to dominate Issues will be missed if incorrect people involved
Inspections and audits	Physical evidence forms the basis of opinion Audit approach results in good structure	Inspections are more suitable for hazard risks Audit approach tends to focus on historical experience
Flow charts and dependency analyses	Useful output that may be used elsewhere Analysis produces better understanding of processes	Difficult to use for strategic risks May be very detailed and time-consuming
Crowd sourcing technology	Speed of collection of data Analysis of responses enables a dashboard approach Diverse input enabled Encourages visual representation	Individuals may abuse the system maliciously, or find other ways to affect the system to produce incorrect outcomes

For many organizations, quantification of risk exposure is essential and the risk assessment technique that is chosen must be capable of delivering the required quantification. Quantification is particularly important for financial institutions and the style of risk management employed in these organizations is frequently referred to as operational risk management (ORM).

Risk workshops are probably the most common of the risk assessment techniques. Brainstorming during workshops enables opinions regarding the significant risks faced by the organization to be shared and a common view and understanding of each risk is achieved. However, the disadvantage can be that the more senior people in the room may dominate the conversation, and contradicting their opinions may be difficult and unwelcome.

In order to have a structured discussion at a risk assessment workshop, several brainstorming structures are commonly used. These may be qualitative or quantitative, depending on the level of analysis of the risk that is required. The most common of the qualitative brainstorming structures are the SWOT and PESTLE analyses. SWOT is an analysis of the strengths, weaknesses, opportunities and threats faced by the organization.

The SWOT analysis has the benefit that it also considers the upside of risk by evaluating opportunities in the external environment. One of the strengths of the SWOT analysis is that it can be linked to strategic decisions. However, because it is not a structured risk classification system, there is a possibility that not all of the risks will be identified.

The other common qualitative approach is the PESTLE analysis that considers the political, economic, social, technological, legal and environmental/ethical risks faced by the organization. Table 11.3 considers the PESTLE risk classification system in more detail. PESTLE is a well-established structure with proven results for undertaking brainstorming sessions during risk assessment workshops.

Many organizations will wish to undertake a quantitative evaluation of the possibility of a risk event occurring. There are several techniques available for undertaking these quantitative evaluations. The most common are hazard and operability (HAZOP) studies and failure modes effects analysis (FMEA). Both of these techniques are structured approaches that ensure that few risks are omitted. However, the involvement of a wide range of experts is required in order to undertake an accurate quantitative analysis.

HAZOP and FMEA techniques are most easily applied to manufacturing operations. HAZOP studies are often undertaken of hazardous chemical installations and complex transport structures, such as railways. Also, HAZOP studies of complex installations, such as nuclear power stations, are often undertaken. They can also be applied to the analysis of the safety of products. In both cases, these are very analytical and time-consuming approaches, but such an approach will be necessary in a wide range of circumstances.

Nature of the risk matrix

When a risk has been recognized as significant, the organization needs to rate it so that the priority significant risks can be identified. Techniques for rating risks are well established, but there is also a need to decide what scope exists for further improving control. Consideration of the scope for further cost-effective improvement is an additional consideration that assists in the clear identification of the priority significant risks.

An organization will need to establish the measures of risk likelihood and risk impact that will be used throughout the organization. Table 10.5 provides a typical list of definitions in relation to risk likelihood. Table 10.6 sets out definitions of impact that would be used in a typical organization. In both cases, four different definitions are provided and this will avoid any tendency for persons undertaking a risk rating exercise to select the middle option. However, many organizations decide to have more than four options available both for likelihood and impact. The number of options available will depend on the nature, size and complexity of the organization.

There are many different styles of risk matrix. The most common form is one that demonstrates the relationship between the likelihood of the risk materializing and

the impact of the event should the risk materialize. As well as likelihood and impact, other features of the risk can be represented on the risk matrix. For example, the scope for achieving further risk improvement is often represented using a risk matrix. In this case, the risk matrix will demonstrate the level of risk in relation to the additional measures that can be taken to improve the management of that risk, and thereby set a target level for it.

The risk matrix can be used to record the outcome of the risk rating exercise and this will provide a simple visual presentation of the significant risks that have been

Table 10.5 Definitions of likelihood

Likelihood	Frequency
Unlikely	Can reasonably be expected to occur, but has only occurred 2 or 3 times over 10 years in this organization or similar organizations.
Possible	Has occurred more than 3 times in the past 10 years in this organization, or occurs regularly in similar organizations, or is considered to have a reasonable likelihood of occurring in the next few years.
Likely	Occurred more than 7 times over 10 years in this organization or in other similar organizations, or circumstances are such that it is likely to happen in the next few years.
Almost certain	Has occurred 9 or 10 times in the past 10 years in this organization, or circumstances have arisen that will almost certainly cause it to happen.

Table 10.6 Definitions of impact – example hospital risks

Descriptor	Definition
Small	No impact on patient health; minor reduction of reputation in the short run; no violation of law; negligible economic loss which can be restored.
Moderate	Minor temporary impact on patient health; small reduction of reputation that may influence trust for a short time; violation of law that results in a warning; small economic loss that can be restored.
Severe	Serious impact on health; serious loss of reputation that will influence trust and respect for a long time; violation of law that results in a fine or penalty; large economic loss that cannot be restored.
Catastrophic	Death or permanent reduction of health of patient; serious loss of reputation that is devastating for trust; serious violation of law; considerable economic loss that cannot be restored.

recognized or identified. In undertaking a risk assessment exercise, it is also necessary to rank the risks against the risk appetite of the organization or the risk criteria that have been established. The stage of risk rating is referred to in ISO 31000 as risk analysis and the stage of risk ranking is described as risk evaluation.

This will lead to the clear identification of the priority of significant risks. Most organizations will find that the total number of risks identified in a workshop is between 100 and 200. After the risk rating has been completed, it is typical for the number of priority significant risks faced by the organization to be identified as between 10 and 20. The terminology used in Guide 73 is a combination of likelihood and impact of a risk, and is considered to be the level of risk, sometimes referred to by risk practitioners as the risk severity.

There are many alternative versions of tables that provide definitions for terms used to describe likelihood and impact. An organization will need to produce its own definitions, based on the size, nature and complexity of that organization. Table 10.5 provides generic definitions of likelihood in terms of the number of occasions when the event is likely to occur over a 10-year period. Table 10.6 provides definitions of impact that could be used in a hospital where patient safety is the primary consideration.

Risk perception

When undertaking risk assessment exercises, it is often the case that different attendees at the workshop will have different views of the risk. There are several ways of accommodating differing opinions, either through use of technology or through wider discussion of the different views of a risk. The perception of risk by individuals will be affected by a number of factors. The following are considered to increase concern amongst the general public in relation to a specific risk to health:

- involuntary (pollution) rather than voluntary (dangerous sports);
- inequitably distributed (some benefit while others suffer);
- inescapable by taking personal precautions;
- arising from an unfamiliar or novel source;
- resulting from human-made, rather than natural, sources;
- causing hidden and irreversible damage, perhaps years after exposure;
- posing particular danger to small children or pregnant women;
- threatening form of death (or illness/injury) arousing particular dread.

Different views on the importance of a risk can be present at different levels of seniority within the organization. It is useful for the risk assessment process to draw opinions

from all levels of management, so that different perspectives of a risk can be identified. Again, the benefits of this approach are better risk communication, fuller risk understanding and the identification of appropriate and practical control measures.

In order to understand the risks facing an organization and be able to undertake an accurate risk assessment, extensive knowledge of the organization is required. To complete an accurate risk assessment that correctly identifies the significant risks and then goes on to identify the critical controls is a time-consuming and resource-intensive exercise.

In relation to the public perception of risk, members of the public often only have access to incomplete information and are subject to strong arguments from lobbying and other special interest groups. Therefore, the public understanding and perception of risk may not be sufficiently informed or entirely objective. Journalists and news reporters have a duty to present news stories in an objective and unbiased manner, which may not be easy when the people receiving the information do not have a full understanding of the risks involved.

Government risk assessments

Government will make available its assessments of risks that affect the public, how it has reached its decisions and how it will handle the risk. It will also do so where the development of new policies poses a potential risk to the public. When information has to be kept private, or where the approach departs from existing practice, it will explain why. Where facts are uncertain or unknown, government will seek to make clear what the gaps in its knowledge are. It will be open about where it has made mistakes and what it is doing to rectify them.

SOURCE HM Treasury (2005) *Managing Risks to the Public: Appraisal guidance*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/191518/Managing_risks_to_the_public_appraisal_guidance.pdf

Attitude to risk

Figure 10.1 provides an illustration of risk attitude using a standard risk matrix. It represents the risk attitude of a risk-averse organization. It is becoming more common for a risk attitude matrix to contain four sections. These sections can be represented by the 4Cs of comfort, cautious, concerned and critical. Risk attitude represents the long-term approach of the organization to risk. These descriptors can also be attached

to the four sections on a risk appetite matrix to describe the approach to short-term risk taking. The relationship between risk attitude and risk appetite is discussed further in Chapter 25.

The darkest area in Figure 10.1 represents the critical risks for the organization. For a risk-aggressive organization, the lower portion of the graphic, the comfort zone, will be larger than for a risk-averse organization. The ‘universe of risk’, or those risks of real significance to the board, will be very restricted for such a risk-aggressive organization. The phrase ‘universe of risk’ is often used by internal auditors to identify audit priorities. Working with such a closed or restricted ‘universe of risk’ will increase the chances of an unidentified significant risk impacting the organization. Each different stakeholder will have a different ‘universe of risk’ and the risk manager is likely to have a ‘universe of risk’ that includes all of the risks that have already been identified, plus any emerging risks that are starting to appear.

Figure 10.1 Risk attitude matrix

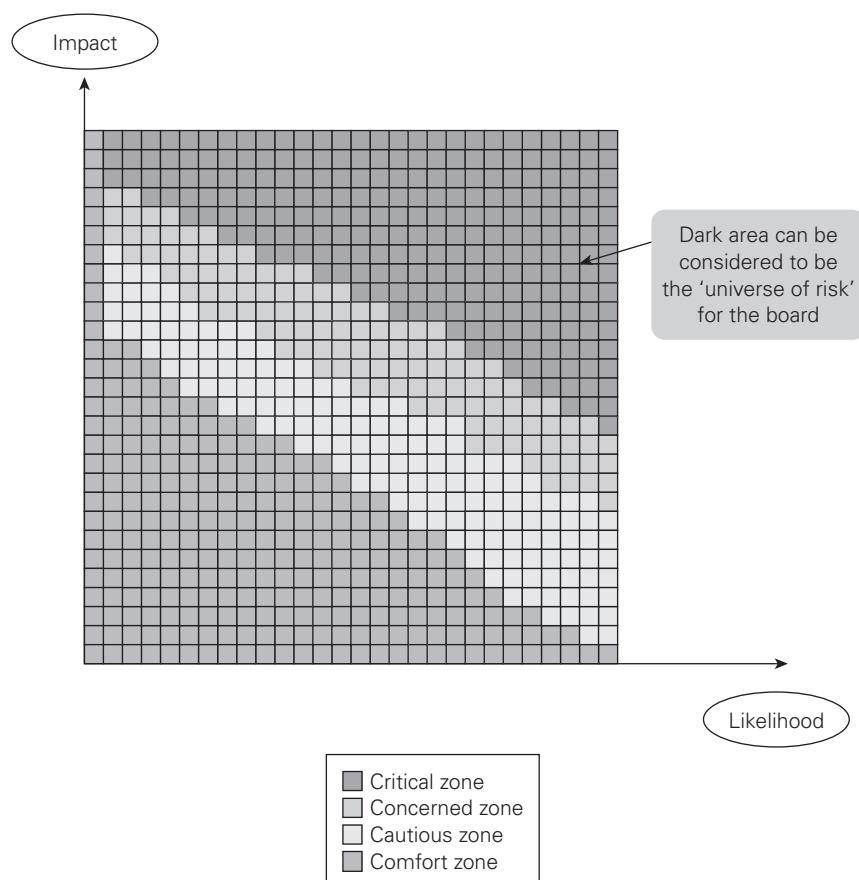


Figure 10.1 illustrates that there will be a level of risk that the organization feels comfortable taking and embedding into core processes. This is because, regardless of the likelihood of the risk materializing, the impact is so small that it would not be significant if it did materialize. Likewise, there will be a likelihood of a risk materializing that is considered so remote that it is assumed that it will not occur, even though it would be very serious if it did. For example, most organizations do not consider the consequences of a jumbo jet crash-landing on their site.

Above these minimum levels of tolerable likelihood and impact, a range of risks can arise. Generally speaking, low-likelihood/low-impact risks will be tolerable; medium-likelihood/medium-impact risks will require some judgement before acceptance; and high-likelihood/high-impact risks will be intolerable. The overall attitude of an organization to risk can be described by a set of 'risk criteria' and this is the approach taken by ISO 31000. It is worth noting that there is no specific mention of risk appetite in ISO 31000 in favour of discussion of the risk criteria. The difference between risk attitude and risk appetite can be described as follows: risk attitude is concerned with the criteria surrounding risk, and risk appetite is concerned with the amount of risk required to achieve objectives.

Organizations will need to take a risk-by-risk approach when deciding whether a risk is acceptable. Different organizations will set tolerance levels differently and this will be an indication of risk attitude. Many organizations will take a cumulative review of risk where all risk exposures are added together, and this is a feature of the enterprise risk management approach. The organization will then be able to decide whether the overall exposure to risk is acceptable and consistent with the risk attitude of the organization.

When considering risk attitude, perception and appetite, it is worth reflecting that individuals may be more alert to low-impact risk with a high probability of occurrence (slips and trips) than they will a high-impact risk that is unlikely to happen (such as an earthquake). This difference in approach is often reflected in the risk assessment process and can affect the way in which significant risks are prioritized but is capable of being quantified using data analytics.

When all the potentially significant risks have been identified, one approach is to ask how likely it is that each of those risks will materialize above the threshold test for significance. The risks can then be prioritized as high likelihood, medium likelihood and low likelihood. The alternative approach is to prioritize the potentially significant risks in order of the impact at the same likelihood. The risks will then be presented as high impact, medium impact and low impact.

There is a difference in attitude and perception in these approaches. The first approach is based on how likely it is that the risk will be significant while the second is based on how much the risk will impact when it happens. Neither of these approaches is better than the other, and which approach an individual board member

(or the collective board itself) may prefer is related to attitude to risk, as stated in the risk criteria for the organization. The impact associated with a risk is usually measured in terms of the effect on finances, infrastructure, reputation and/or marketplace (FIRM). One of the main requirements of risk management is that the consequences of high-impact events for the strategy, tactics, operations and compliance (STOC) of the organization are successfully managed.

Classifying risks 11

Risk classification systems

There will be many identified risks facing an organization. The volume of these identified risks means there will be too many risks to focus on any particular area and a structure to classify them will be required. Formalized risk classification systems enable the organization to identify where similar risks exist within the organization. Classification of risks also enables the organization to identify who should be responsible for setting strategy for management of related or similar risks. Appropriate classification of risks will enable the organization to better identify the risk appetite, risk capacity and total risk exposure in relation to each risk, group of similar risks or generic type of risk.

There are a number of classification systems available. They may sort the risks according to timescale of their impact or according to the nature of the risk, the source of the risk and/or the nature of the impact or size and nature of the consequences. The different systems have been devised in different circumstances and by different organizations; therefore, the categories are similar but not identical. For example, operational risk is referred to as infrastructure risk in the FIRM risk scorecard and COSO takes a narrow view of financial risk, with particular emphasis on reporting.

In describing different risk classification systems, Table 11.1 illustrates that many classification systems offer a combination of source, event, impact and consequences categories.

British Standard BS 31100 sets out the advantages of having a risk classification system, such as helping to define the scope of risk management in the organization, providing a structure and framework for risk identification, and giving the opportunity to aggregate similar kinds of risks across the whole organization. It states that the number and type of risk categories employed should be selected to suit the size, purpose, nature, complexity and context of the organization. The categories should also reflect the maturity of risk management within the organization.

The advantages of having a risk classification system include:

- Accumulations of risk that could undermine a key dependency or business objective and make it vulnerable can be more easily identified.
- Responsibility for improved management of each different type of risk can be more easily identified/allocated if risks are classified.

- Decisions and knowledge about the type of control(s) that will be implemented can be taken on a more structured and informed basis.
- Circumstances where the risk appetite of the organization is being exceeded (or the risk criteria not being implemented) can be more readily identified.
- Categorizing risks according to a single risk classification system may not be sufficient to reveal all risks. Therefore, a combination of systems can be used to provide a complete picture.

Time to impact

Although it is not a formalized system, the classification of risks into short, medium and long term helps to identify risks as being related (primarily) to operations, tactics and strategy, respectively. This distinction is not clear-cut, but it can assist with further classification of risks. There is always the requirement to ensure compliance in operations, tactics and strategy.

A short-term risk can impact the objectives, key dependencies and core processes instantly. These risks can cause disruption to operations immediately the event occurs. They are predominantly hazard risks, although this is not always the case and they are often associated with unplanned disruptive events, but may also be associated with cost control in the organization. Short-term risks usually impact the ability of the organization to maintain effective and efficient core processes that are concerned with the continuity and monitoring of routine operations. There is a need to mitigate short-term risks.

A medium-term risk can impact the organization following a (short) delay after the event occurs. Typically, the impact of a medium-term risk would be apparent within months, or at most a year after the event. Medium-term risks usually impact the ability of the organization to maintain effective and efficient core processes that are concerned with the management of tactics, projects and other change programmes. These medium-term risks are often associated with projects, tactics, enhancements and other developments. There is a need to manage these medium-term risks. In information security risk, the phrase ‘zero-day attack’ indicates the day a system was breached and counting from that day to when organizations were aware of the breach can be between three and nine months.

A long-term risk can impact the organization between one and five years (or more) after the event. Long-term risks usually impact the ability of the organization to maintain the core processes that are concerned with the development and delivery of effective and efficient strategy. Risks that have the potential to undermine strategy can destroy more value than risks to operations and tactics. Although long-term

risks can undermine an organization, there is a need to embrace the appropriate level of risk embedded in the strategy.

Figure 11.1 illustrates short-term, medium-term and long-term risks in terms of the source of these risks. The risks arise from the operations, tactics and strategy adopted by the organization. For the sake of completeness, the category of compliance risks is also included, since this is an additional category to operations, tactics and strategy. The need to respond to risks according to whether they arise from strategy, tactics, operations or compliance (STOC) is summarized by embrace, manage, mitigate and minimize (EM3) respectively.

Examples of risk classification systems

Perhaps the most commonly used risk classification systems are those offered by the COSO ERM cube by the IRM risk management standard and using the FIRM framework. The COSO risk classification system contains some weaknesses. For example, strategic risks may also be present in operations and in reporting and compliance, but it remains in widespread use since it is explicitly recognized by the Sarbanes–Oxley Act.

It is for the organization to decide which risk classification system most fully satisfies its needs and requirements, or to tailor elements of systems into an individual framework. For example, banks and other financial institutions almost universally classify risks as market, credit and operational risks. Another commonly used risk classification system that can also be employed to provide structure to risk assessment workshops is the PESTLE analysis.

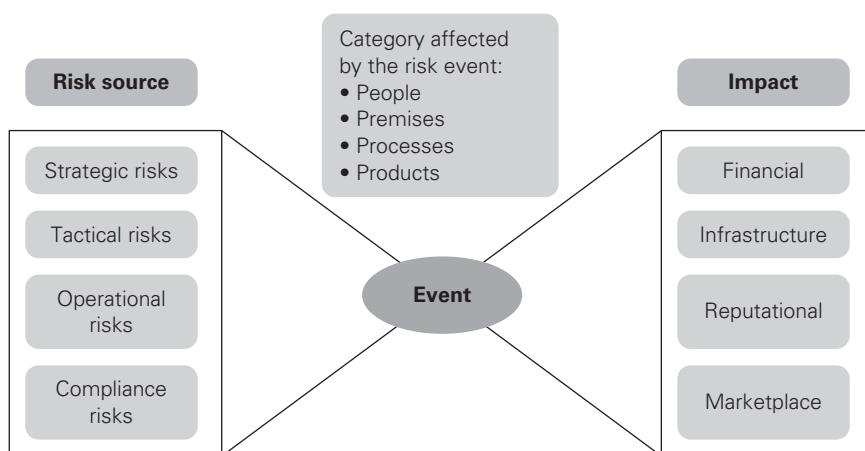
Table 11.1 provides a summary of these risk classification systems. There are similarities in most of these systems. Identifying risks as: 1) hazard, control or opportunity; 2) high, medium or low; and 3) short term, medium term and long term is not considered to be a formal risk classification system.

Many organizations struggle to find a suitable risk classification system. Often, this is because there is insufficient attention paid to the nature of the risks that are being classified. The bow-tie representation of the risk management process illustrates that it is possible to classify risks according to their source, the component of the organization that the event impacts and the impact and/or consequences of the risk materializing.

The use of a bow-tie to represent risk management has become increasingly common. Figure 11.1 provides an example of the bow-tie being used to represent the three components of risk source, event and impact. In this high-level representation, risk sources are identified as strategic, tactical, operational or compliance. Impacts are represented using the FIRM risk scorecard, as described in Table 11.2. At the centre of the bow-tie is the event, as described by the component of the

Table 11.1 Risk classification systems

Standard or framework	FIRM risk scorecard	COSO ERM cube	IRM standard	<i>The Orange Book</i>
Classification headings	Financial Infrastructure Reputational Marketplace	Strategic Operations Reporting Compliance	Financial Strategic Operational Hazard	Strategy Governance Operations Legal Safety Financial Commercial People Technology Information, security Project Programme Reputational

Figure 11.1 Bow-tie representation of risk management

organization that will be impacted by the event. These components are represented in the same way as in Table 2.2. The categories of disruption to organizations described in Table 2.2 use a classification system according to the component of the organization that is impacted, people, premises, processes and products (4Ps) which is a risk classification system.

Figure 11.2 Bow-tie and risks to premises

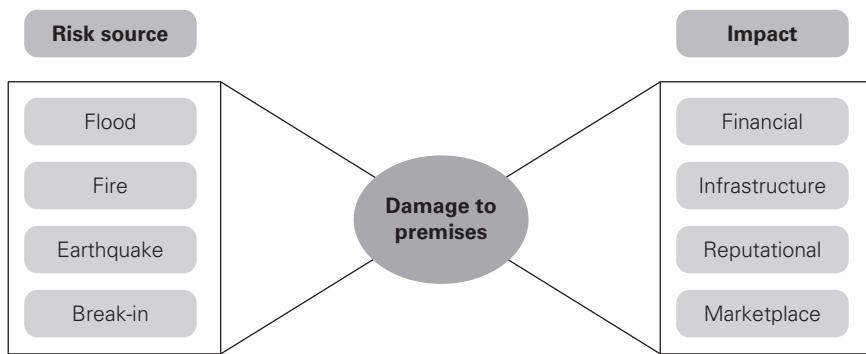


Figure 11.2 presents an operational version of the bow-tie representation of risk management, rather than the high-level overview presented in Figure 11.1. This uses the bow-tie to represent the sources of potential damage to premises and retains the impacts as financial, infrastructure, reputational and marketplace. The sources of potential damage to premises are identified as flood, fire, earthquake and break-in. When a hazard event occurs, it will have an impact on the features of the organization that can cause disruption. For this reason, the event shown in the centre of the bow-tie would be listed in terms of the component of the organization that is impacted by the event.

FIRM risk scorecard

The FIRM risk scorecard builds on the different aspects of risk, including timescale of impact, nature of impact, whether the risk is hazard, control or opportunity, and the overall risk exposure and risk capacity of the organization. The headings of the FIRM risk scorecard provide for the classification of risks as being primarily financial, infrastructure, reputational or marketplace in nature.

The FIRM risk scorecard can also be used as a template for the identification of corporate objectives, stakeholder expectations and, most importantly, key dependencies. The scorecard is an important addition to the currently available risk management tools and techniques. It is compiled by analysing the way in which each risk could impact the key dependencies that support each core process. Use of the FIRM risk scorecard facilitates robust risk assessment by ensuring that the chances of failing to identify a significant risk are much reduced.

The four headings of the FIRM risk scorecard offer a classification system for the risks to the key dependencies in the organization. The classification system

also reflects the idea that every organization should be concerned about its finances, infrastructure, reputation and marketplace success. In order to give a broader scope to commercial success, the headings of the FIRM risk scorecard are as follows:

- Financial
- Infrastructure
- Reputational
- Marketplace

The features of the FIRM risk scorecard are set out in Table 11.2. Financial and infrastructure risks are considered to be internal to the organization, while reputational and marketplace risks are external. Also, financial and marketplace risks can be easily quantified in financial terms, whereas infrastructure and reputational risks are more difficult to quantify.

The inclusion of reputational risks as a separate category of risk in the FIRM risk scorecard is not universally accepted. It is often argued that damage to reputation is a consequence of other risks materializing rather than a separate risk category. It could be said, however, that the nature of reputation has changed in an era of social media. If a broad view of risk is taken, it becomes obvious that reputations can be burnished or damaged at a rapid pace. In any case, there is a wider argument that all risks are a consequence of broader business decisions. Adopting a particular strategy, undertaking a project and/or continuing with established operations all involve risks. If the organization did not undertake these strategic, tactical or operational activities, risks would not be present.

Table 11.2 Attributes of the FIRM risk scorecard

	Finance	Infrastructure	Reputation	Marketplace
Description	Risks that can impact the way in which money is managed and profitability is achieved	Risks that will impact the level of efficiency and cause dysfunction within the core processes	Risks that will impact the desire of customers to deal or trade, and level of customer retention	Risks that will impact the level of customer trade or expenditure
Internal or external risk	Internal	Internal	External	External
Quantifiable	Usually	Sometimes	Not always	Yes

(continued)

Table 11.2 (Continued)

	Finance	Infrastructure	Reputation	Marketplace
Measurement (performance indicator)	Gains and losses from internal financial control	Level of efficiency in processes and operations	Nature of publicity and effectiveness of marketing profile	Income from commercial and market activities
Performance gap	Procedures Failure of procedures to control internal financial risks	Process Failure of processes to operate without disruption	Perception Failure to achieve the desired perception	Presence Failure to achieve required presence in the marketplace
Control mechanisms	Capex standards Internal control Delegation of authority	Process control Loss control Insurance and risk financing	Marketing Advertising Reputation and brand protection	Strategic and business plans Opportunity assessment

PESTLE risk classification system

Table 11.3 provides an outline of the PESTLE risk classification system. PESTLE is an acronym that stands for political, economic, social, technological, legal and ethical risks. In some versions of the approach, the final E is used to indicate narrower environmental considerations. This risk classification system is most applicable to the analysis of hazard risks and is less easy to apply to financial, infrastructure and reputational risks.

The PESTLE risk classification system is often seen as most relevant to the analysis of external risks. External risk in this context is intended to refer to the external context that is not wholly within the control of the organization but where action can be taken to mitigate the risks. It is often suggested that the PESTLE risk classification system should be used in conjunction with an analysis of the strengths, weaknesses, opportunities and threats (SWOT) facing the organization.

There are several advantages and disadvantages to the PESTLE approach. The advantages are as follows:

- simple framework;
- facilitates an understanding of the wider business environment;
- encourages the development of external and strategic thinking;

- anticipates future business threats;
- helps identify actions to avoid or minimize impact of threats;
- facilitates identification of business opportunities.

However, there are certain disadvantages associated with the use of the PESTLE analysis as a means of identifying risks. These disadvantages are as follows:

- can over-simplify the amount of data used for decisions;
- needs to be undertaken on a regular basis to be effective;
- requires different people being involved with different perspectives;
- access to quality external data sources can be time-consuming and costly;
- difficult to anticipate developments that may affect an organization in the future;
- risk of capturing too much data that makes it difficult to identify priorities;
- can be based on assumptions that subsequently prove to be unfounded.

The PESTLE approach in the public sector has been updated by *The Orange Book*. This provides 13 examples of risk categories, shown in Table 11.4.

Table 11.3 PESTLE classification system

Category of risk	Description
Political	Tax policy, employment laws, environmental regulations, trade restrictions and reform, tariffs and political stability.
Economic	Economic growth/decline, interest rates, exchange rates and inflation rate, wage rates, minimum wage, working hours, unemployment (local and national), credit availability, cost of living, etc.
Sociological	Cultural norms and expectations, health consciousness, population growth rate, age distribution, career attitudes, emphasis on safety, global warming.
Technological	Technology changes that impact your products or services, new technologies, barriers to entry in given markets, financial decisions like outsourcing and supply chain.
Legal	Changes to legislation that may impact employment, access to materials, quotas, resources, imports/exports, taxation, etc.
Ethical or environmental	Ethical and environmental aspects, although many of these factors will be economic or social in nature.

Table 11.4 Orange Book risk categories

Category of risk	Description
Strategy	Risks arising from identifying and pursuing a strategy that is poorly defined, based on flawed or inaccurate data or fails to support the delivery of commitments, plans or objectives due to a changing macro-environment (eg political, economic, social, technological, environment and legislative change).
Governance	Risks arising from unclear plans, priorities, authorities and accountabilities, and/or ineffective or disproportionate oversight of decision-making and/or performance.
Operations	Risks arising from inadequate, poorly designed or ineffective/inefficient internal processes resulting in fraud, error, impaired customer service (quality and/or quantity of service), non-compliance and/or poor value for money.
Legal	Risks arising from a defective transaction, a claim being made (including a defence to a claim or a counterclaim) or some other legal event occurring that results in a liability or other loss, or a failure to take appropriate measures to meet legal or regulatory requirements or to protect assets (for example, intellectual property).
Property	Risks arising from property deficiencies or poorly designed or ineffective/inefficient safety management resulting in non-compliance and/or harm and suffering to employees, contractors, service users or the public.
Financial	Risks arising from not managing finances in accordance with requirements and financial constraints, resulting in poor returns from investments, failure to manage assets/liabilities or to obtain value for money from the resources deployed and/or non-compliant financial reporting.
Commercial	Risks arising from weaknesses in the management of commercial partnerships, supply chains and contractual requirements, resulting in poor performance, inefficiency, poor value for money, fraud, and/or failure to meet business requirements/objectives.
People	Risks arising from ineffective leadership and engagement, suboptimal culture, inappropriate behaviours, the unavailability of sufficient capacity and capability, industrial action and/or non-compliance with relevant employment legislation/HR policies resulting in negative impact on performance.
Technology	Risks arising from technology not delivering the expected services due to inadequate or deficient system/process development and performance or inadequate resilience.

(continued)

Table 11.4 (Continued)

Category of risk	Description
Information	Risks arising from a failure to produce robust, suitable and appropriate data/information and to exploit data/information to its full potential.
Security	Risks arising from a failure to prevent unauthorized and/or inappropriate access to the estate and information, including cyber security and non-compliance with General Data Protection Regulation requirements.
Project/ programme	Risks that change programmes and projects are not aligned with strategic priorities and do not successfully and safely deliver requirements and intended benefits to time, cost and quality.
Reputational	Risks arising from adverse events, including ethical violations, a lack of sustainability, systemic or repeated failures or poor quality or a lack of innovation, leading to damage to reputation and/or destruction of trust and relations.

SOURCE HM Government (2020) *The Orange Book: Management of risk – principles and concepts*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866117/6.6266_HMT_Orange_Book_Update_v6_WEB.PDF

Compliance, hazard, control and opportunity

Many risk classification systems include compliance risks within larger categories. For example, in PESTLE they will be in the ‘P’ and the new *Orange Book* classification above refers to these risks within operations. There is a possibility that compliance risks will not be readily identified as a result. A further difficulty associated with compliance risks is that there is often the requirement for a trigger event. In other words, an organization can be exposed to a number of compliance risks but it may be difficult to identify the particular compliance issue that will become a problem.

The risk classification systems discussed in this chapter are most easily applied to the analysis of hazard risks, except that the IRM standard and the COSO ERM cube offer strategic risk as a separate risk category. As with other core processes in an organization, classification of risks facing projects is essential, so that the appropriate response to each risk can be identified. Given that the requirements of any project are that it should be delivered on time, within budget and to specification, these components offer a means of classifying project risks. Separate lists could be devised of risks that threaten the timescale, risks that threaten the budget and risks that will affect the final specification, performance or quality of the project outcome.

Risk classification in the finance sector

There is no standard risk classification system that can be used by all types of organizations. Banks face a large number of risks and these are usually divided into three main categories of market risk, credit risk and operational risk. With enhanced regulation in all countries, compliance is becoming more common and may move from the legal function to the risk function. Often, the risk management framework and architecture will be different for the different types of risks.

Market risks are risks that occur due to fluctuations in the financial markets. The assets and liabilities of the bank are exposed to various kinds of market volatilities, such as changes in interest rates and foreign exchange rates. Market risk is primarily an opportunity risk that is embraced by the bank.

When the bank lends to a client there is an inherent risk of money not coming back, and this is the credit risk. Credit risk is simply the possibility of the adverse condition in which the client does not pay back the loan amount. It is primarily a control risk that has to be managed.

Operational risk relates to failure of internal systems, processes, technology and humans, and to external factors such as natural disasters, fires, etc. Compliance risks will fall within this category since breaching the regulatory framework will be a failure to manage operations. Basel II defines operational risk as 'the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. Operational risk has gained profile because of the need to quantify operational risk exposure, the increased use of technology and recognition of the critical role played by people in finance sector processes.

Operational risk is primarily a hazard risk that has to be mitigated.

Analysing risks

12

The dimensions of risk

Levels of risk

When analysing risk, we can consider three ingredients which have slightly different meanings when considered in terms of the vertical axis on a risk matrix. Table 12.1 illustrates these differences.

Different professions view these aspects of risk at different levels. For example, internal auditors will start with the gross or inherent risk and audit the controls in place. Risk managers prefer to start with the current level of risk and review what can change this level. Health and safety practitioners prefer to undertake risk assessment with the current controls in place, ie at the current level. This relies on the assumption that the current controls will always work to the assumed effectiveness. For example, if an assessment of an x-ray machine is being undertaken, the safety person will assume that the enclosure or cabinet is in good order and the risk should be assessed on that basis. The internal auditor will more easily recognize that the enclosure or cabinet is a vitally important control factor that has to be subject to a routine inspection.

The concept of consequences is a little different. Impact is used to represent the overall level of risk faced by the organization. This level of risk or impact will arise because of the potential consequences. Therefore, ‘consequences’ is used as a broader term that provides more detail and information on how successfully the risk is being managed. For example, a warehouse fire could represent a substantial loss that has a high magnitude. If the organization is fully insured, the impact on the finances should be minimal. However, the consequences of the fire could be significant if (for example) other stakeholders in the vicinity are affected and the reputation of the organization is damaged.

Risks are illustrated in the form of a risk matrix, as shown in Figure 10.1. Having placed the various risks on a risk matrix, the relative importance of the risks can easily be identified. Large organizations frequently make use of a risk matrix as a means of summarizing their risk profile. The risk matrix is very useful and can be used for a range of applications. It can also be used to identify the type of risk response that is most likely to be employed.

Table 12.1 Levels of risk

Level of risk	Definition	Label for vertical axis
Gross or inherent	The level of risk before controls are applied	Impact
Net, residual or current	The level of risk after the application of existing controls	Magnitude
Target	The desired level of risk after the application of planned controls	Magnitude

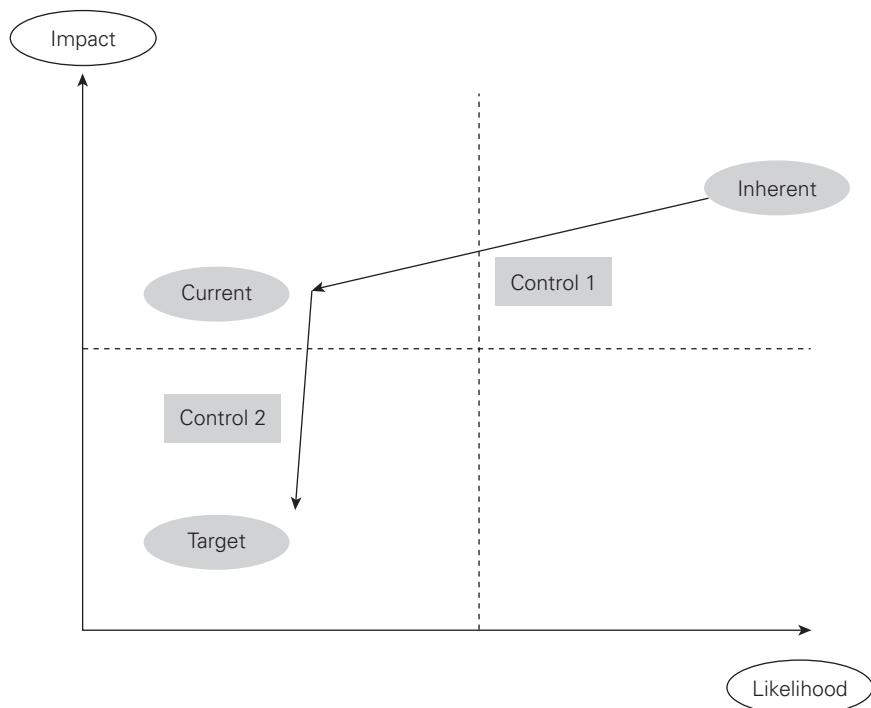
Impact is not the same as magnitude, because a risk may have a high magnitude in terms of the size of the event, but the impact and consequences may be smaller. To take another example, a road transport company may suffer the complete loss of one of its vehicles but, depending on the exact circumstances, this may have a very small overall impact on the business. This will be true if the company did not have sufficient work to fully utilize the type of vehicle involved in the loss or if the company had a sufficiently large number of vehicles to redistribute work amongst its fleet.

Inherent and current level of risk

Risk management practitioners' and internal auditors' preferred measures of risk indicate their different responsibilities: risk managers refer to current levels while internal auditors' primary measure is the inherent level of risk. The advantages of considering the inherent level of a risk are that it enables the effect of individual control measures to be identified. Figure 12.1 illustrates the effect of controls on the level of risk. Control 1 is an existing control which reduces the risk from the inherent level to the current (or residual) level and it can be seen that this control has its main effect on the likelihood of the risk materializing.

Control 2 in Figure 12.1 is an additional control that will be introduced to reduce the risk from the current level to the target level. It is intended to have a significant effect on the impact of the risk, but little effect on the likelihood of it materializing.

The phrase 'current level' is used throughout this book rather than 'residual level' because it indicates a more dynamic measure that can change. The residual level of risk implies a static position where the organization cannot take any further risk mitigation action. Figure 12.1 illustrates the effect of the planned introduction of Control 2, which is intended to reduce the impact of the risk. This is known as the target level of risk and brings the risk into the bottom left-hand quadrant of the risk matrix, or the tolerate/comfort zone.

Figure 12.1 Inherent, current and target levels of risk

When seeking to establish the target level of risk, a concept that is often used by health and safety practitioners is to reduce the risk to a level that is ‘as low as reasonably practicable’ (ALARP). ALARP is one of the fundamental principles of risk management for health and safety risks. It refers to managing risk to the point where the cost of additional controls would exceed the benefits.

As low as reasonably practicable

The requirement for risks to be ALARP is fundamental and in simple terms is a requirement to take all measures to reduce a risk, where doing so is reasonable. In most cases this is not done through an explicit comparison of costs and benefits, but rather by applying established relevant good practice and standards. The development of relevant good practice and standards incorporates ALARP considerations, so in many cases meeting those standards is sufficient. In other cases, either where standards and relevant good practice are less evident, or not fully applicable, measures must be implemented to the point where the costs of any additional measures (in terms of money, time or trouble) would be grossly disproportionate to the further risk reduction (or safety benefit) that would be achieved.

An organization will need to agree definitions for likelihood and impact. Both likelihood and impact can be described in terms of low, medium, high and very high. Many organizations will need to be more specific than these generic descriptions, depending on the type of risk and the size, nature and complexity of the organization. Because impact is used to describe the range of consequences, it is more important for an organization to describe low, medium, high and very high in terms of impact.

Control confidence

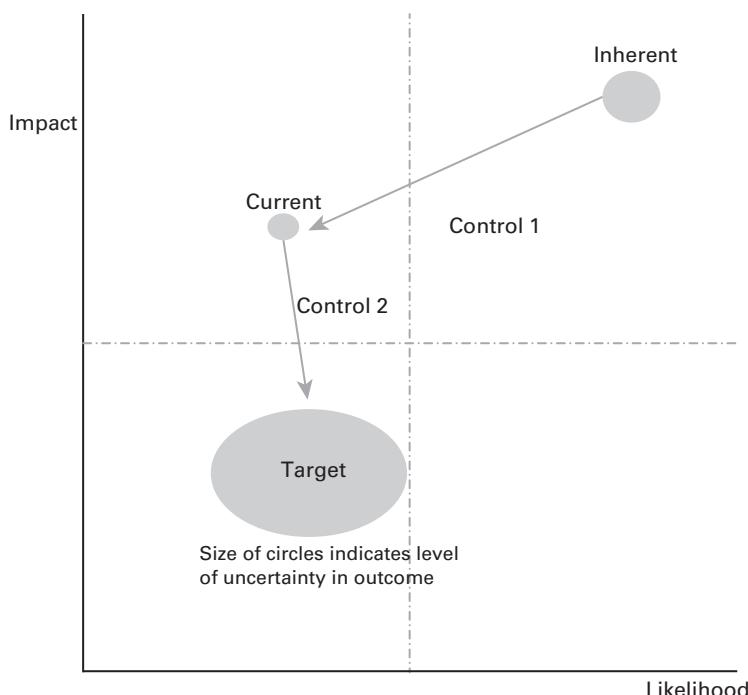
Whilst the target level of risk is indicated in Figure 12.1, it is not possible for an organization to be absolutely confident that controls will always be fully implemented or will be as effective as expected or required. Controls will need to be audited in order to allow confidence that the control selected has been properly implemented and is producing the desired effect.

The level of control confidence can also be illustrated on a risk matrix. If the effectiveness of a control is uncertain, a greater variability of the outcome may be expected. This can be demonstrated on a risk matrix by using a circle or ellipse to represent a risk, instead of representing the risk as a single point on the risk matrix. By doing this, the level of uncertainty or variability in the outcome can be illustrated in relation to both the likelihood and impact of the event materializing.

Two questions need to be asked: 'How confident are we that this is the correct control?' and 'How confident are we that it is fully implemented and effective in practice?' When there is limited confidence in the effectiveness of a control, it will be the role of internal audit to test the control and provide information on the likely level of variability of outcome, should the risk materialize.

It is the responsibility of internal auditors to check that the correct controls have been selected and that they are working correctly in practice. Internal auditors refer to effective and efficient controls respectively when reviewing these points. The use of effective and efficient is also included in this book in relation to core processes of the organization. Undertaking the testing of controls is a key function fulfilled by internal audit, and the importance of the testing of controls should also be recognized by risk management practitioners.

Management needs to receive assurance of adequate control and this can come from internal audit activities, or measurement of the outputs of activities and projects, as well as from management reports. The responsibility for designing and implementing controls and auditing the effectiveness and efficiency of controls should be allocated within the risk management documentation.

Figure 12.2 Confidence in controls

4Ts of hazard risk response

The options presented for risk response can be described as the 4Ts of hazard management, which are: tolerate, treat, transfer and terminate. It is possible to illustrate the 4Ts of risk response on a simple risk matrix, and this is done in Figure 15.1. This figure suggests that in each of the four quadrants of the risk matrix, one of the 4Ts will be dominant, as follows:

- Tolerate will be the dominant response for the low-liability/low-impact risks.
- Treat will be the dominant response for high-liability/low-impact risks.
- Transfer will be the dominant response for high-impact/low-liability risks.
- Terminate will be the dominant response for high-impact/high-liability risks.

The corresponding responses for control and opportunity risks are considered in Chapter 15. Options for responding to opportunity risks are identified as the 4Es (explore, exit, exploit and exist) and decision making in respect of opportunities is

described in terms of the 5Es (which includes ‘expand’ in the acronym). It is important to note that these responses are represented as the dominant or most likely response in each quadrant, but circumstances may dictate that another response may be required as well, or instead.

Different and/or additional responses may be appropriate, depending on the circumstances. For example, if high-impact/high-likelihood risks are embedded within mission-critical activities, they may be unavoidable. In this case, it will not be possible for the organization to terminate those risks.

A difficulty in presenting such a simple risk matrix showing the 4Ts of risk response is that they meet in the centre. Clearly, it cannot be as simple as suggested, because a small change in the likelihood and impact of a risk could take it from the terminate quadrant into the tolerate quadrant. A slightly modified approach that makes this analysis somewhat more realistic is considered in Chapter 16.

A practical difficulty for many organizations is that they may be forced to retain a risk that is recognized as being beyond the risk appetite, or even the risk capacity, of the organization. For example, a firefighting authority may have to accept circumstances where firefighters will be facing a critical level of risk that the organization has no choice but to tolerate, even though all possible controls have been implemented. Where organizations have to tolerate risks that are at the critical level, it is usual for enhanced monitoring of the risks to be put in place. This will enable the organization to ensure that it takes the earliest opportunity of introducing any enhanced controls as soon as they become available.

Risk significance

When undertaking a risk assessment, it is quite common to identify a hundred or more risks that could impact the objective, core process or key dependency that is being considered. This is an unmanageable number of risks and so a method is required to reduce the number that will be considered to be priority issues for management.

In order for an organization to concentrate on significant risks, a test for risk significance is required. Table 12.2 provides suggestions on the nature of the benchmark tests that could be used to decide whether a risk is significant. For risks that will have a financial or commercial impact, the benchmark test is likely to be based on monetary value. For risks that could disrupt the infrastructure or routine operations of the organization, a benchmark test based on the impact, cost and duration of disruption is appropriate. For reputational risks, the most likely benchmark will be based on the adverse publicity that would result if the risk materializes.

This may vary according to the nature of the risk and whether it is a financial or non-financial one. For large organizations, identifying a financial test for significance can be undertaken in a number of ways. Depending on the risk this could be:

- levels of authorization to spend money, often set out in a formal document referred to as a ‘delegation of authority’;
- level at which full board approval is required for expenditure in excess of a particular financial threshold;
- levels that external auditors consider to be material when compiling the accounts of the organization;
- use of financial metrics, for example a proportion of:
 - the budgeted profit for the year (typically 5 per cent), or
 - the budgeted turnover for the year (typically 0.5 per cent), or
 - the value of the balance sheet or reserves of the organization (typically 0.25 per cent).

For an organization with a £2 billion balance sheet, £1 billion annual turnover and £100 million planned annual profit, the significant financial threshold would be £5 million (5 per cent of profits).

Financial limits can be used to test whether a risk is significant in relation to financial and marketplace risk segments of the FIRM risk scorecard. For infrastructure and reputational segments, identifying a benchmark test for significance may be more difficult. One test of significance for infrastructure risks is to ask whether the risk would disrupt normal operations for more than (say) half a day. For reputational

Table 12.2 Benchmark tests for risk significance

FIRM risk scorecard	Typical benchmark test for significance
Financial	Impact on balance sheet of 0.25% Profit and loss impact of 2.5% annual profit
Infrastructure	Disruption to normal operations of ½ day Increased cost of operation exceeds 10% budget
Reputational	Share price falls by 10% Event is on national TV, radio or newspapers
Marketplace	Impact on balance sheet of 0.5% turnover Profit and loss impact of 1% annual profit

risks, the test for significance may be to determine the fluctuation in market capitalization if the stock loses value, or how the event appears within all media, including social media. This can be measured using analytics developed to review the number of times an organization is mentioned, the influence of the publisher and whether it is in a positive or negative context.

Applying these tests during a risk assessment workshop could reduce the number of risks for further consideration to a more manageable number, say about 20. The next stage would be to identify how likely each of the 20 potentially significant risks would be to materialize at or above the financial threshold level. A risk matrix could be used to record and display the results.

Risk capacity

There are several aspects that are important when an organization is deciding how much risk to take. Different approaches will be taken for different types of risks. Hazard risks will give rise to a hazard tolerance, control risks will give rise to a control acceptance and opportunity risks will give rise to an investment appetite. Overall, the organization will have a total risk exposure. This is the sum of the total risk that the organization has taken in these three categories. There will also be compliance risks, but most organizations have no appetite for compliance risks and have the necessary compliance controls embedded into core processes.

An important measure of risk is the risk capacity of the organization. This is a measure of how much risk the organization should take or can afford to take. All of these ways of analysing risk should be compatible with the attitude of the organization to risk.

In simple terms, the risk appetite of the board should be within the risk capacity of the organization and greater than or equal to the actual risk exposure that the organization faces. It would be inappropriate for an organization to embark on a project that could exhaust all of its resources. The capacity of the organization to accept risk will depend on its financial strength, the robustness of its infrastructure, the strength of its reputation and brands and the competitive nature of the marketplace in which it operates.

The more rapidly the marketplace is changing, the greater capacity for risk the organization is required to have available. For example, if an organization is facing a significant change in technology, the strategic options may be limited. Consider an organization that was involved in the manufacture of DVD players when it became obvious that streaming technology was taking over. The organization was faced with a significant risk related to the change in technology and needed to develop a new business model. It needed to acquire new production equipment, new skills and new distribution patterns. It may be that the transfer to the new technology and the risks

that it involves are outside the resources and risk capacity of the organization. If that is the case, the organization may need to explore strategic options, including seeking a joint-venture partner, locating a buyer for the business or simply withdrawing from the marketplace.

Many circumstances will arise where organizations are faced with risks that could destroy them if those risks materialized. For some organizations, there may be several individual and even independent risks, each of which could destroy the organization. In these circumstances, the challenge for the risk management function will be to focus on the circumstances that could trigger one or more of these risks.

Evaluating risks: Risk appetite

Once risks have been analysed it will be necessary to decide how to respond to the risk. This can take the form of the 4Ts for threats (see above) or the 5Es for opportunities (discussed in Chapter 15). Risk evaluation is, in effect, a decision point at which to decide whether to respond or not to respond to the risk.

In order to do so, this implies there is a threshold that the risk will need to cross before action is taken. This threshold is termed the ‘risk appetite’ of the organization and was defined in Chapter 3 as being concerned with the amount of risk required to achieve objectives.

Risk appetite has four overriding principles as expressed in the IRM’s discussion paper on the subject:¹

- 1 Acknowledging interconnectedness:** What is acceptable in one division or business unit may be out of appetite in another and there needs to be a way of reconciling or dealing with this complexity.
- 2 Measurability:** The use of key risk indicators and key control indicators based on data available inside or from outside the organization is needed to apply risk appetite consistently. The organization’s appetite needs to be practically applied, however, in terms that are realistic for the organization for the term to have any currency.
- 3 Variability:** Whilst risks may be assessed consistently and scored against similar matrixes there will be a range of appetites for different risks.
- 4 Maturity:** How adept the organization is at managing risk will have a bearing on the appetite of the organization for taking that risk. Confidence in its management of risk should not be misplaced, however, and may require some form of external validation to corroborate the internal view of risk management maturity.

In the corporate governance section of this book (Part Seven) it will be seen that it is incumbent upon the board to evaluate their risk management capability. Good

corporate governance requires the board to understand their risks and provide clarity in terms of their appetite and tolerance of risk. This is especially so and mandated for all listed companies.

There are some clear benefits to establishing risk appetite in a transparent fashion within the organization:

- It provides clear safeguards within which the organization can operate.
- It creates a framework for better decision making, by bringing clarity and structure to the process.
- It will allow the identification of issues at an early stage.
- It will facilitate the achievement of long-term objectives while respecting stakeholder views.

This transparency should ensure that the first line of defence, the operations, have a clear understanding of the appetite of the organization for risk and can ensure its application or raise a concern if it is felt to be breached.

Note

- 1 Institute of Risk Management (2011) Risk appetite and tolerance, www.theirm.org/what-we-say/thought-leadership/risk-appetite-and-tolerance/ (archived at <https://perma.cc/36DD-BQU4>)

Controlling the downside of risk

Risk likelihood

Risk likelihood indicates how often a risk is expected to materialize. It can also be described as risk frequency. The phrase ‘risk frequency’ implies that the risk occurs on a regular basis. Risk likelihood is used throughout this book and can be determined on an inherent basis, or at the current level of risk, paying regard to the control measures that are in place.

For hazard risks, previous history may be a good indication of how likely the risk is to occur. For a fleet of motor vehicles, there is certain to be a history of vehicle accidents and breakdowns. Controls will be in place to reduce the likelihood of these events. A road haulage company should assess the likelihood of vehicle breakdowns on an inherent basis and also on the basis of current controls. There are, however, difficulties in assessing the inherent likelihood of vehicle accidents, because certain assumptions would have to be taken about what effect the removal of controls would have on the likelihood of accidents.

Even if an assessment of the breakdown likelihood at the inherent level cannot be undertaken, the company will still need to determine the importance of the vehicle maintenance programme in preventing vehicle breakdowns and whether the maintenance activities provide value for money. In relation to vehicle accidents, the company may have driver-training procedures in place and, again, the effectiveness of these procedures can be determined by evaluating inherent and current levels of risk. Whether levels of risk are evaluated at inherent or at current level, there is no doubt that benchmarking the performance of the fleet against the average performance of the industry will be a useful exercise.

An example of a control measure that has an effect on the magnitude of the risk but may have no effect on its likelihood is the use of seat belts in cars. In simple terms, the driver wears a seat belt to reduce the impact of an accident, because the seat belt has no effect on the likelihood of an accident occurring. The driver wears the seat belt as a control measure for when an accident happens.

A sports club will wish to reduce the chances of a key player being absent. The absence may be caused by inappropriate behaviour by a player, resulting in the need for sanctions against that person. Accordingly, the club may decide to introduce a

'code of conduct' for senior players, and this would include a commitment by each player to follow an appropriate, healthy lifestyle. Failure to comply with the code of conduct would result in financial and other punishments.

The club may also decide that additional controls are required to reduce player absence, including fitness monitoring and social support for overseas players who have recently moved to the country to join the team. It may also be agreed that an attempt should be made to place contractual limits on the ability of national teams to call on its overseas players. These actions will be taken in addition to other loss control activities, such as excellent medical facilities to provide immediate medical care and reduce the damage when an injury occurs. Also, the company may purchase insurance to protect itself against the financial losses associated with the absence of a player.

Risk magnitude

Reducing the magnitude of a hazard risk is very important. For hazard risks, magnitude is often referred to as the inherent severity of the risk, should it materialize. Reduction in overall hazard risk severity will be achieved by reducing both the impact and consequences when the adverse event occurs. The seat belt in a car can reduce the impact of an accident, but has no effect on the likelihood of having an accident.

It is possible for a serious fire to occur that results in a considerable amount of property damage and is considered to be very severe and expensive. However, in reducing the severity of a serious fire, the requirement is to reduce the impact of the fire on the finances, infrastructure, reputation and marketplace (FIRM) of the organization. Actions to reduce impact will concentrate on damage limitation at the time of the fire, and cost containment after the event. The consequences relate to the effect on the strategy, tactics, operations and compliance (STOC) of the organization. Loss control is concerned with mitigation of the magnitude, impact and consequences of an adverse event.

Damage limitation is also an important feature of reputational risk management. When a serious incident occurs that attracts public attention, an organization will need to be able to protect its reputation by reassuring stakeholders that the organization responded appropriately to the event. It is almost invariably the case that the CEO or chairman of the company will visit the scene when there has been a serious train or plane crash. There have been examples where a serious incident has occurred and the management of the media by the organization involved has been very poor. In these cases, it is likely that inadequate attention was paid to pre-incident planning, so that the damage to the reputation of the organization was not effectively minimized at the time the incident occurred.

Organizations will also need to be concerned with cost containment. Cost containment following an event is usually based on the business continuity plan (BCP) or disaster recovery plan (DRP) that the organization put in place before the incident occurred. The development of effective BCP and DRP will put the organization in the best position to ensure that the overall cost of the incident is kept as low as possible.

Control of fires in hotels

Given the persistent emphasis on fire peril, perhaps it's not surprising that improvements in sprinkler systems have been a hallmark of the past 40 years. Sprinkler technology has evolved from controlling the spread of fire to suppressing the fire. It has moved from a single spray sprinkler head to extra-large orifice and fast-response sprinkler heads. The use of sprinkler systems has also spread from manufacturing facilities into light-hazard exposures such as offices and nursing homes.

As hotel fittings are susceptible to smoke and water damage, the hotel sector wished to mitigate the damage caused by fire and became more deeply involved in loss control efforts. For example, hotels carried out two initiatives in the early 1980s using controlled fires to prove the efficacy of plastic piping in hotel room sprinkler systems. Before the successful tests, sprinklers relied on iron piping, which was more difficult to install than plastic and which took rooms out of service for days during a re-fit.

Hazard risks

The range of hazard risks where reducing the magnitude of the adverse event is important will include fraud, health and safety, property protection and efficient operation of IT systems, as well as incidents with the potential to cause damage to reputation. Table 13.1 provides a list of the key dependencies that could give rise to hazard risks, using the structure of the FIRM risk scorecard. When hazard risks materialize, actions need to be taken to reduce the magnitude of the event, as well as mitigate the impact and consequences.

Although the main focus of managing hazard risks will be on loss prevention, successful management of hazard risks must also include consideration of damage limitation and cost containment. Insurers, to whom the hazard risk of fire is transferred, will endeavour to settle claims in an efficient and cost-effective manner, which includes helping the organization to get back to normal operation as soon as possible.

Table 13.1 Generic key dependencies

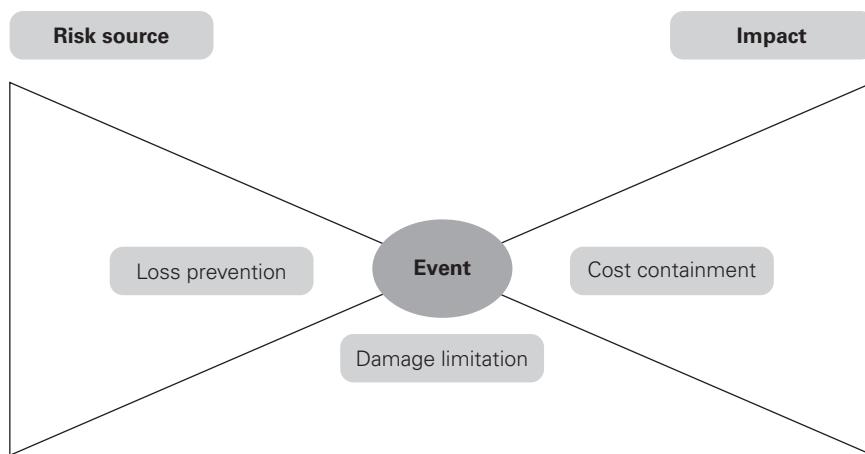
FIRM risk scorecard	Example dependencies
Financial	Availability of funds/finance Correct allocation of funds/finance Internal control (fraud) Liabilities under control (bad debts and pensions)
Infrastructure	People skills and experience Premises/plant and equipment IT hardware and software Communication and transport
Reputational	Brand and brand expansion Public opinion of sector Regulators' enforcement action Corporate social responsibility
Marketplace	Regulatory requirements Health of world or national economy Product development (technology) Competitor behaviour

Reducing the severity of an incident should be seen as part of an overall attempt to implement loss control in an organization. An integrated approach to loss control is important because it will enable the organization to control both the likelihood and impact when a hazard risk materializes. In fact, loss control should be considered to be loss prevention plus damage limitation plus cost containment.

Although the most important component of loss control is loss prevention, hazard risks can materialize despite the best efforts of organizations. Adequate assessment of hazard risks is vital, so that appropriate pre-planning of during-the-loss and post-loss actions can be undertaken. Plans should be in place to ensure that the damage caused by the incident is kept to a minimum and the cost consequences of the event are also tightly controlled and contained.

Figure 13.1 shows how a bow-tie can be used to illustrate the three components of loss control. Before the event occurs, the organization will have controls in place to seek to achieve loss prevention. As the event is developing, steps should be in place to limit the damage that the event is causing. After the event, cost containment controls by way of business continuity and arrangements to reduce the cost of repair should be activated. Disaster recovery plans will be relevant during both the damage limitation and the cost containment stages. The relationship between the three components of loss control and the type of control that will be selected is considered in more detail in Chapter 16. The types of hazard controls are described in Chapter 16 as preventive, corrective, directive and detective.

Figure 13.1 Loss control and the bow-tie



Loss prevention

Another way of looking at loss control activities is that loss prevention is about reducing the likelihood of an adverse event occurring, although it will also be concerned with reducing the magnitude of an event that does occur. Damage limitation is concerned with reducing the magnitude of the event when it does materialize. The contribution of damage limitation will be greatest if actions are planned that can be implemented rapidly as the event is taking place. Cost containment is concerned with reducing the impact and consequences of the event. Effective cost containment will ensure the lowest cost of repairs, as well as business continuity plans to ensure that the organization can continue operations following damage to the asset that has been affected.

Techniques for loss prevention will vary according to the type of hazard risk that is being considered. For health and safety risks, loss prevention is related to eliminating the activity completely or ensuring that, for example, hazardous chemicals are no longer used.

For risks to buildings, loss prevention techniques involve such controls as the elimination of sources of ignition and the control, containment and segregation of flammable or combustible materials. Loss prevention techniques will also include restrictions on smoking and other actions taken to reduce hazardous behaviours by persons using the buildings.

For fraud and theft risks, loss prevention techniques will include segregation of duties and security tagging of expensive items in stores. Fraud prevention techniques may also involve pre-employment screening.

Damage limitation

Damage limitation in relation to fire hazards is well established. Sprinkler systems are a major control measure for ensuring that only limited damage occurs when a fire breaks out. Other damage limitation factors related to fire include the use of fire segregation within buildings, the use of fire shutters, and having well-rehearsed arrangements in place to remove, segregate or otherwise protect valuable items. After the fire at Windsor Castle in 1992, arrangements were quickly put in place for valuable artwork to be removed from areas of the castle that had not (up to that time) been affected by the fire.

Accidents at work still occur, despite the considerable attention paid to health and safety standards and other loss prevention activities. Provision of adequate first aid arrangements is an obvious damage limitation activity and suitable first aid facilities are provided by most organizations. For some high-risk factory occupancies, emergency treatment arrangements and even medical facilities are provided on site.

In some cases, these medical facilities will include specialist treatment facilities related to the particular hazards on site. An example is the provision of cyanide antidotes in factories where chromium-plating activities take place using cyanide-plating solutions. A simpler example is the provision of emergency eye-wash bottles in locations where hazardous chemicals are handled.

The Deepwater Horizon oil spill in the Gulf of Mexico in 2010 provides many risk management lessons. One of the key issues was that the oil spill took some weeks to stop because the equipment for capping the damaged well was not immediately available. The oil industry has learned from this example and a sector-wide approach has now instituted the provision of specialist deep water oil well capping equipment at various places across the world, which is available to all operators.

Cost containment

When a hazard risk materializes despite the efforts put into loss prevention and damage limitation, there may well still be a need to contain the cost of the event. For example, among the activities for minimizing costs associated with serious fires are detailed arrangements for salvage and arrangements for decontamination of specialist items that have suffered water or smoke damage.

Cost containment in relation to a fire will also include arrangements for specialist recovery services. The actions that will be taken to ensure that post-incident costs are minimized should all be set out in business continuity, disaster recovery and crisis management plans, as appropriate. The topics of business continuity planning and disaster recovery planning are considered in more detail in Chapter 19.

A further consideration relevant to cost containment after an incident is additional expenditure that may be required in order to bring the operations back to their pre-incident levels. This is termed ‘increased costs of working’ by insurers and most material damage/business interruption insurance policies will allow for these payments. This may arise when an organization has to sub-contract certain production activities, or has to undertake manufacturing work at another one of its factories, which may be located some distance away.

If a manufacturer discovers that faulty goods have been released into the marketplace, a number of actions become necessary. The organization should have developed plans in advance of the event for notifying customers of the fact that faulty goods are in the marketplace and how to identify them. The box below considers the importance of product recall in these circumstances.

Product recall risk management

Any company or organization that manufactures, assembles, processes, wholesales or retails products could be financially impacted by the direct or indirect costs of a product recall. Direct costs can include wages for staff who have to implement the recall plan. Other direct costs include communications and this could entail purchasing air time on radio and television and notices in newspapers or industry publications.

Indirect costs can include lost production time for staff who must focus on the recall process, as well as the hiring of temporary employees to ensure continued production. However, the greatest indirect cost is the impact that adverse publicity could have on market share. A product recall should be designed to:

- protect the customer from bodily injury or property damage;
- remove the product from the market and from production;
- comply with specific regulatory requirements;
- protect the assets of the company.

Maximizing the upside of risk 14

Defining the upside

A range of interpretations of the phrase ‘upside of risk’ are possible, and some of these are offered in Table 14.1. In simple terms, the upside of risk is achieved when the benefits obtained from taking the risk are greater than any benefit that would have resulted from not taking it. In other words, the organization has received an overall benefit from undertaking the activities that resulted in exposure to the risk or set of risks involved.

The upside of risk may be the reward for taking the risk in the first place. Climbing a challenging mountain may be a significant risk, but the upside of taking that risk is when the climber has safely reached the summit and gains their reward. Another approach is to say that risk management is concerned with achieving the best possible outcomes by reducing uncertainty or volatility. If this is accepted as a definition of risk management, the upside of risk is concerned with maximizing the opportunities that the organization has through reducing uncertainty involving the risk of failure to achieve the desired outcome.

Table 14.1 Defining the upside of risk

Opportunity management, by completing a detailed review of a business opportunity before deciding to embrace it.

Ability to seize an opportunity because competitors did not identify the cost-effective solution to a risky feature of a contract.

Specifically identifying positive events during the risk assessment and deciding how to encourage those events.

Fewer disruptions to normal operations and greater operational efficiency, resulting in less downside of risk.

Achieving a positive outcome in difficult circumstances as an unintended and/or automatic result of good risk management.

When undertaking a risk assessment workshop, the process should also focus on identifying risks that have an upside outcome. The risk assessment workshop would therefore address questions like: 'What events would create a better outcome than expected?' A register of positive outcome risks can then be identified and actions can be taken to make those upside risks more likely to occur and/or have more beneficial impact and consequences when they do materialize.

A more satisfactory explanation of the upside of risk is that the organization will be able to undertake activities that it would not otherwise have the appetite to undertake. In a commercial sense, an organization will be able to seize a business opportunity that a competitor does not have the appetite to take, or considers to be too risky. This may be because of a better process, or because a cost-effective development project has been identified that the competitor failed to recognize. The process or project will have been identified using risk management techniques that analyse and assess the uncertainties which were otherwise inhibiting action.

A further way of looking at the upside of risk is to reflect on a business venture that turned out successfully in circumstances where failure could have been foreseen. This is a somewhat retrospective approach and depends on the organization being willing to pursue a risky venture, albeit with adequate controls in place, that leads to a positive outcome in circumstances where a competitor may not have been willing to take the risk. It can provide lessons for the organization to take other risks in other circumstances.

Finally, there is the analysis of the upside of risk that reflects on the benefits of having a robust risk management process. Achieving the mandatory, assurance, decision making, effective and efficient core processes (MADE2) benefits, especially benefits related to mandatory obligations, may be considered to be a sufficient reason for undertaking a risk management initiative. In these circumstances, certain organizations may consider that achieving compliance with mandatory obligations is an upside of risk. At its most simplistic, and specifically in relation to hazard risks, the upside of risk is that there is less downside. However, that is not a very compelling reason for senior managers to support a risk management initiative.

Perhaps the easiest explanation, and the most compelling, is that the upside of risk is the ability to increase the likelihood of successfully pursuing a business opportunity that competitors are unwilling to embrace. It would also be part of the explanation to say that competitors would be too risk-averse to take such a high-risk opportunity.

Risk management standards do not currently take a coherent approach to the upside of risk. An approach employed in some risk management standards is that the 4Ts (tolerate, treat, transfer and terminate) should be extended to include the fifth T of 'take the risk' and become the 5Ts. The discipline of risk management is still developing and this is an area that requires more research to enable a wider consensus to form.

The story in the next box is an example of embracing an opportunity that could be seen as a highly risky strategy. The individual was willing to pursue the opportunity in order to test this view, and by doing so benefit if the risk proved to be analysed incorrectly, and was not in fact high risk.

Honesty box and the upside of risk

A vendor in Wall Street set up a stand to sell donuts and coffee to passers-by as they went in and out of their office buildings. During the breakfast and lunch hours, he always had long lines of customers waiting, which he knew discouraged many customers who went elsewhere. He worked out that the biggest bottleneck preventing him from selling more donuts and coffee was the disproportionate amount of time it took to make change for his customers.

To overcome this, he put a small basket on the side of his stand filled with dollar bills and coins, trusting his customers to make their own change. He was able to move customers through at twice the pace as a result. Most customers responded by being completely honest, often leaving him with larger-than-normal tips. He also found that his customers liked being trusted and kept coming back. By extending trust in this way, he was able to double his revenues without adding any new cost.

Opportunity assessment

Successfully embracing business opportunities is more likely to be achieved if the organization undertakes opportunity assessments. When taking on a new business opportunity a consultancy firm will undertake a detailed evaluation of the prospect and evaluate the scope for a profitable partnership, opportunities to earn extra income and the reputational benefits that might arise from having that potential client as a customer.

Opportunity assessment can be undertaken in relation to new business ventures, as well as new clients. This opportunity evaluation is designed to identify the additional revenue that could arise from winning that business. The evaluation will also look at the potential disadvantages of pursuing the business, which may have reputational or other consequences.

Consider the options for a theatre that discovers that fewer people are coming to performances and decides to look at the opportunities to take more money from those who continue to attend. The options may include general improvement to the catering facilities within the theatre and the provision of organic produce in the

theatre restaurant. Additionally, there is the possibility of selling merchandise themed to the particular performance.

As well as looking at increased revenue during performances, the theatre may also look at sponsorship arrangements and open dialogue with local businesses to discover what type of production would be most likely to gain local support and sponsorship. In future, part of the assessment of any proposed new production could include an evaluation of the level of sponsorship that might be available. As well as generating greater income, this approach could also enable the theatre to stage productions that otherwise would have been considered too risky.

Many organizations already practise opportunity management, although it may not be seen explicitly as a risk management approach. Ideally, opportunity management should be embedded into procedures for developing and implementing strategy and tactics and/or taking advantage of business opportunities.

When seeking to identify opportunities, many organizations facilitate a risk assessment workshop that seeks to identify and analyse threats and opportunities at the same time. Figure 14.1 provides an example of a risk matrix that can be used to record the outcome of such a risk assessment workshop. The exact design of the risk matrix and the descriptors of likelihood and consequence will vary between organizations. Figure 14.1 should be treated as one example or illustration of how to record the output from the risk assessment workshop.

Figure 14.1 Risk matrix for opportunities and hazards

Upside risk			Likelihood	Downside risk		
High	High	Medium	1:2 Probable	Medium	High	High
High	Medium	Low	1:10 Possible	Low	Medium	High
Medium	Low	Low	1:100 Unlikely	Low	Low	Medium
Major	Moderate	Minor		Minor	Moderate	Major
Consequence						
Multiple objectives exceeded beneficially	Objective delivered significantly early, better, or cheaper	Objective delivered slightly early, better or cheaper	Objective-driven (customer, people, society or key performance)	Slippage and minor deviation	Failure to meet an objective	Extinction of organization

One of the challenges when undertaking a risk assessment workshop that covers both opportunities and hazards is that a wide range of people will need to attend. Hazards tend to be operational and compliance related, whereas opportunities tend to be associated with strategy and tactics. As with hazard risks, the identification and analysis of opportunities has to be followed by an evaluation of the opportunities and the identification of actions or controls that will need to be in place to ensure that the anticipated benefits are more likely to be achieved. The opportunity assessment methodology described earlier in this section will need to be applied to the opportunities that have been identified, analysed and recorded on the risk matrix.

Riskiness index

The risk profile of an organization can be represented in many ways. The most common method used is to prepare a risk register that contains details of the significant risks that it faces. However, a disadvantage of the risk register is that it is usually a qualitative evaluation of individual risks. Organizations need to develop a means of measuring, evaluating and quantifying the total risk exposure of the organization.

One of the features of the enterprise risk management approach is to develop a consolidated view of the risk exposure of the organization. The approach based on calculating the total risk exposure of an organization is similar to the approach taken to the measurement and quantification of risk in operational risk management.

This section introduces the idea of a ‘riskiness index’. The idea is to present a semi-quantitative approach that takes a snapshot of the overall level of risk embedded in the organization. The overall level of risk will take account of the strategy currently being followed by the organization, the projects that are in progress, and the nature of the routine operations being undertaken. This approach can offer an opportunity to benchmark risk management performance and track changes over time.

Table 14.2 presents a set of questions that can be used to develop a riskiness index for an organization. The table uses the structure of the FIRM risk scorecard as a means of categorizing risks. By using the riskiness index, an organization should be able to identify the level of risk faced by its finances, infrastructure, reputation and the level of risk that it faces in the marketplace.

Having completed the riskiness index, the organization can then seek additional controls to reduce the level of risk. The main focus of risk management is then simply to reduce the level of riskiness within the organization without affecting its strategy, tactics, operations or compliance (STOC). The upside of risk then becomes that the organization can follow the desired STOC at the lowest level of risk that is reasonably and cost-effectively achievable.

Table 14.2 Riskiness index

Allocate a score of between 0 and 5 to each component (in accordance with the key at the end of the table) of the generic example of the FIRM risk scorecard to determine the level of risk within the organization, project, operation or location being evaluated.

Financial component of the FIRM risk scorecard		
Index	Description	Score
1.1	Lack of availability (or unacceptable cost) of adequate funds to fulfil the strategic plans	
1.2	Insufficiently robust procedures for correct allocation of funds for strategic investment	
1.3	Inadequate internal financial control environment to prevent fraud and control credit risks	
1.4	Inadequate funds to meet historical liabilities (including pensions) and meet future anticipated liabilities	
TOTAL for the financial component		
Infrastructure component of the FIRM risk scorecard		
Index	Description	Score
2.1	Inadequate senior management structure to support organization and embed 'risk-aware culture'	
2.2	Insufficient people resources, skills and availability, including concerns about intellectual property	
2.3	Inadequate physical assets to support the operational and strategic aims of the organization	
2.4	Information technology (IT) infrastructure has insufficient resilience and/or data protection	
2.5	Business continuity plans are not sufficiently robust to ensure continuation of organization after major loss	
2.6	Product delivery, transport arrangements and/or communications infrastructure are unreliable	
TOTAL for the infrastructure component		

(continued)

Table 14.2 (Continued)

Reputational component of the FIRM risk scorecard			
Index	Description	Score	
3.1	Poor public perception of the industry sector and/or potential for damage to the brands of the organization		
3.2	Insufficient attention to ethics/corporate social responsibility/social, environmental and ethical standards		
3.3	Poor governance standards and/or sector is highly regulated with high compliance expectations		
3.4	Concerns over quality of products or services and/or after-sales service standards		
TOTAL for the reputational component			
Marketplace component of the FIRM risk scorecard			
Index	Description	Score	
4.1	Insufficient revenue generation in the marketplace or inadequate return on investment achieved		
4.2	Highly competitive marketplace with aggressive competitors and high customer expectations		
4.3	Lack of economic stability, including exposure to interest rate fluctuations and foreign exchange rates		
4.4	Marketplace requires constant innovation and/or product technology is rapidly developing		
4.5	Supply chain is complex and lacks competition and/or raw materials costs are volatile		
4.6	Organization is exposed to potential for international disruption because of political risks, war, terrorism, crime or pandemic		
TOTAL for the marketplace component			
Score	Description of the level of risk	Score	Description of the level of risk
0	No risk	3	Medium risk
1	Little risk	4	High risk
2	Some risk	5	Extreme risk

The level of risk identified by the riskiness index represents the risk exposure of the organization. The board can then compare this level of risk exposure with the risk capacity of the organization and the attitude of the board towards risk.

Calculating the riskiness index of an organization requires identification of the hazard risks actually being taken by that organization. In other words, evaluating the riskiness index of an organization helps to identify the actual risk exposure of that organization. Having identified the actual level of risk embedded within an organization, the board of that organization can then ask whether the portfolio of risks is within the risk appetite and/or the risk capacity of the organization and compatible with the risk attitude of the board.

The 2016 version of the UK Corporate Governance Code contains the following requirement for companies listed on the London Stock Exchange: 'The board is responsible for determining the nature and extent of the principal risks it is willing to take in achieving its strategic objectives.'¹ Organizations should be careful to ensure that, having identified the risks that they are taking by a mechanism similar to calculating the riskiness index, the board does not then simply decide that the risks they are currently taking must be the same as the risks they are willing to take.

Upside in strategy

Organizations will have a mission statement, together with a set of corporate objectives and an understanding of the expectations of the different stakeholders in the organization. The board of the organization then needs to develop an effective and efficient strategy that will deliver exactly what is expected in terms of the mission, objectives and expectations. In order to make correct strategic decisions, the board of the organization will need access to risk information. A risk assessment of the proposed strategy, together with a risk assessment of any viable alternative strategies, should be undertaken. The availability of this risk assessment information will ensure that the strategic decisions are more likely to be correct.

For opportunity risks, there is probably even less data available on which to predict risk likelihood. An organization may see an opportunity to acquire a new client or develop and market a new product. Accurate risk assessment of the likelihood of positive and negative events will be necessary in order to determine whether the new venture should go ahead. When a new product is launched, the requirement may well be to increase the likelihood of a positive event occurring. If a new product is being launched, advertising and press coverage will need to be maximized up to the point that this remains cost-effective. Actions should therefore be taken to increase the level of media interest in the launch.

Strategic core processes bring the disciplines of strategic planning and risk management together. Strategic planning is a systematic process for obtaining a consensus

at board level on the small number of issues that could have a massive effect on the long-term performance of the organization. Strategic issues are vitally important, and failure to implement strategy or the selection of an inappropriate strategy can be amongst the most devastating risks to hit an organization. Implementation of strategy is usually achieved by developing tactics that are implemented by way of projects and then ultimately delivered by operational core processes. The operational core processes in place at a specific time represent the business model of the organization, as is discussed in more detail in Chapter 20.

Risk management activities are designed to ensure the best possible outcome and reduce uncertainty. Therefore, the upside of risk in strategy is that risk management efforts help with the design of an effective and efficient strategy. The implementation of that strategy will be achieved through the tactics employed. Those tactics will be designed to improve core processes in the organization, so that the organization is using the most effective and efficient core processes.

Upside in projects/programmes

It is essential that every organization adopts the correct core processes. A core process may be considered as the collection of activities that deliver a specific stakeholder expectation. This is the meaning of core process that is allocated by business process re-engineering (BPR) practitioners.

There is a difference between a process being efficient and effective. An efficient process means that there is no disruption and no excess cost. However, the process may be the incorrect one for cost-effectively delivering the requirements. Where processes need to be improved, a project will normally be undertaken and change achieved. In circumstances where a series of projects are required, this is sometimes referred to as a programme of work. However, programmes tend to be transformational and not transactional. When a project, or programme of work, is implemented by an organization, the desire will normally be to improve the effectiveness and/or efficiency of core processes. In the case of programmes they will transform the way in which the organization operates.

By undertaking adequate risk assessment of the intended change, the organization should be able to ensure that the project is more likely to be delivered on time, within budget and to specification. Achieving the upside of risk in the project or programme management requires that projects are adequately managed and that the correct project or priorities have been selected by the organization.

Often, organizations will undertake a post-implementation review to ensure that the benefits expected from the project have been delivered in practice. This review is often undertaken by internal audit and is designed to ensure that the project was delivered successfully, delivered the benefits that were required and was overall

worthwhile. During difficult financial times, it is important that the organization selects projects that are not only successful, but represent the best possible allocation of limited resources when compared with alternative projects that have not been selected.

Risk management in projects is associated with the implementation of tactics designed to achieve the strategy. In some organizations, projects that will implement tactics are only approved if the project reduces risk. For example, if a particular activity could fail because of poor IT systems, the project should be designed to make the activity more robust. In doing so, risks will be reduced and it should be possible to quantify the benefits that will result from activities that are more efficient because of better use of human resources and because of fewer failures of IT systems.

In summary, the benefits of good risk management within projects are that the project is more likely to be delivered on time, to budget and at the required quality. Risk management activities will assist the delivery of the project and, at the same time, help manage a situation when an outcome is different from what was expected as the project progresses. This different outcome will demonstrate whether the tactics have been successful and the correct project was selected. A negative difference will need to be mitigated and a positive difference will be embraced, as this is one example of the upside of risk.

Upside in operations

It is a fundamental requirement for organizations that they have effective and efficient operations. Efficient operations should make best use of the resources of the organization and should operate without unplanned disruption. Undertaking efficient operations that use minimum resources and produce maximum output will deliver the greatest benefit to the organization. Operations also need to be effective in that they represent the best way of conducting the operations. For example, it is possible to have an efficient journey by car or bus across a busy city. However, the effective way to travel in many large cities is by means of the metro or underground system.

Risk management evaluation of operations can enable the organization to deliver the most effective and efficient activities, operations and processes. By delivering the most effective and efficient operations, a commercial organization can achieve advantages over a competitor and undertake work for a lower cost and still make a profit.

For public services, the delivery of effective and efficient operations is equally important. Most public services have targets for delivery of those services that can be complex and challenging. Failure to anticipate and manage risks appropriately can undermine the delivery of public services. The contribution of risk management will

also help achieve sustained improvements in services by bringing flexibility and resilience to the way in which the services are delivered. This contribution by risk management may be considered to be part of delivering the upside of risk.

In a competitive marketplace, achieving the upside of risk will often be to the detriment of competitors, suppliers or other third parties. However, seeking the upside of risk taking requires awareness of a possible unexpected downside. Deciding not to do something because it appears to have become more hazardous may actually result in the risks increasing. Further aspects of risk appetite and personal perception of risk are discussed in Chapter 26. In terms of business decisions about operational risk, it is important that those risks are taken on an objective basis. Personal views and perceptions of risk can lead to incorrect business decisions. Ensuring the availability of accurate risk information in order to make business decisions is one of the key responsibilities of the risk manager.

Chapter 5 explains that establishing the context is the first stage in the risk management process. The riskiness index set out in Table 14.2 provides a useful structure for establishing both the external context and the internal context of the organization. When establishing the context, it is important to consider the upside of risk, how opportunities will emerge for the organization and how these opportunities can be exploited in relation to strategy, tactics and operations.

Upside of compliance risks

Finally, it is important to note that there is an upside that can be achieved in relation to compliance risks. For some organizations, there will be a regulator that grants licences, and the organization cannot operate without a licence. In these circumstances, a good working relationship with the regulator can often provide an upside of risk. This will be especially true if the organization seeks to influence the regulator to require tighter control of regulated activities. In this way, the organization will set high standards that it is able to achieve, in the hope that competitors may suffer disadvantage, if they also have to achieve these high standards but are not able to do so without additional expense. An organization that demonstrates good risk management to regulators is less likely to be targeted for review.

Note

1 Financial Reporting Council (2016) *The UK Corporate Governance Code*, www.frc.org.uk/getattachment/ca7e94c4-b9a9-49e2-a824-ad76a322873c/UK-Corporate-Governance-Code-April-2016.pdf (archived at <https://perma.cc/XQ66-4EB7>)

THIS PAGE IS INTENTIONALLY LEFT BLANK

PART FOUR

Risk response

LEARNING OUTCOMES

Having studied this section readers will be able to:

- Describe the risk response options in terms of tolerate, treat, transfer and terminate (4Ts), and explain how these can be shown on a risk matrix.
- Explain the benefits of using a risk matrix to illustrate inherent, current and target levels of risk and the effect of controls.
- Describe the types of controls that are available, in terms of preventive, corrective, directive and detective (PCDD) controls.
- Explain the use of a risk matrix to identify the main type of control for different types of hazard risk and the concept of 'hazard risk zones'.
- Describe the importance and structure of insurance, the circumstances in which insurance is purchased and the purpose of a captive insurance company.
- Explain the importance to the insurance purchasing activity of cost, coverage, capacity, capabilities, claims and compliance (6Cs).
- Summarize the importance of business continuity planning (BCP) and disaster recovery planning (DRP) and provide practical examples.
- Describe the approach taken during a business impact analysis (BIA) and the importance of established business continuity standards, such as ISO 22301.

Further reading

- HM Government (2020) *The Orange Book: Management of risk – principles and concepts*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866117/6.6266_HMT_Orange_Book_Update_v6_WEB.PDF
- Institute of Risk Management (2011) Risk appetite and tolerance, www.theirm.org/what-we-say/thought-leadership/risk-appetite-and-tolerance/
- ISO (2012) *ISO 22301:2012 Societal Security – Business Continuity Management Systems: Requirements*, www.iso.org/standard/50038.html
- Taleb, N (2008) *The Black Swan: The impact of the highly improbable*, Penguin, Harmondsworth
- Taylor, E (2014) *Practical Enterprise Risk Management*, Kogan Page, London
- United States Government (2021) Ready business, www.ready.gov/business

CASE STUDIES

The student can review the following examples to illustrate further the areas discussed in Part Four and throughout this book.

Dangote Cement plc: Sustainability

Dangote Cement is a Nigerian multinational publicly traded cement manufacturer headquartered in Lagos, part of the Dangote Group of Companies. The company is engaged in the manufacture, preparation, import, packaging, and distribution of cement and related products in Nigeria and has plants or import terminals in nine other African countries. Their operations are sensitive to climate change as the cement industry is one of the main producers of carbon dioxide. Their operations are, however, strategically important to the advancement of the region, which requires infrastructure for development.

Their annual report includes a ‘sustainability report’, which establishes their commitment to long-term sustainable operations. They also demonstrate a clear framework and purpose for risk management. They say that they ‘believe the identification and management of risk are central to achieving the corporate purpose of creating long-term shareholder value’.

The purpose of their risk management structure and internal control systems is to ‘identify, evaluate and manage risks with a view to enhancing the value of shareholders’ investments and safeguarding assets’. They further state: ‘[the] process ensures the appropriate ownership of risk and accountability of all stakeholders in the risk management value chain whilst ensuring collaboration between risk management and process owners’.

across the business. Measurement of risk takes into consideration our risk appetite tolerance limits to avoid misrepresentation of our risk profile.

Edited extracts from: Dangote Cement (2019) Driving Opportunities in New Markets: Annual report 2019,

https://dangotecement.com/wp-content/uploads/2021/04/DangoteCementPlc_2019_AnnualReport-2.pdf

NHS Resolution: Monitoring and review

This organization is a UK government entity that administers and provides funding for clinical negligence in the NHS. They hold significant reserves and are charged with the prudent but fair delivery of outcomes for those injured as a result of treatment by the NHS. They report in 2020 that their provisions ‘for claims against the secondary care system in England have reduced, to £82.8 billion, largely due to reductions in expected future claims inflation’.

They perform a vital function to ‘provide analysis and expert knowledge to drive improvement’, or, in other words, to learn lessons from losses. The risk management systems for their operations are based around the context that they are essentially an administrative function, with key risks around IT infrastructure and cyber security. In 2020 they highlighted an inquiry into incidents caused by ‘a consultant surgeon who performed inappropriate or unnecessary procedures and operations’ from which ‘378 claims have been reported of which one is an ongoing claim; 237 have settled and 140 discontinued with no damages payment’. The incident also involved a private provider of medical services which made settlements of £37 million to private patients.

As a result of that case they state that they ‘have made a number of improvements to our service which include strengthening the promotion of information-sharing between organizations in the interests of patient safety’.

Edited extracts from: NHS Resolution (2020) Annual Report and Accounts 2019/20, https://resolution.nhs.uk/wp-content/uploads/2020/07/NHS-Resolution-2019_20-Annual-report-and-accounts-WEB.pdf

Thomas Miller Holdings Ltd: Risk committees

Thomas Miller is a company that provides services to insurers and specialist insurance services. The specialist services include the management of mutual insurance facilities for shipping owners along with other marine insurance services. They also manage captive insurance companies, a subject that is discussed in Chapter 18.

Their annual report discusses how they manage risk through their Risk committee and they state:

The Group’s risk management systems continue to be developed and enhanced.... The Group’s compliance and risk management processes and systems are designed to ensure that management and the company’s various businesses regularly review the

risks and controls in their risk registers, and that any outstanding risk mitigation actions are tracked and delivered in a timely manner.

They clearly state that their review process includes regular reviews of the risk register, which 'sets out the principal risks facing the company and the risk mitigation actions, controls and processes by which they are managed' at every meeting as a monitoring process.

Edited extracts from: Thomas Miller Holdings Ltd (2020) Annual Report and Accounts 2019, www.thomasmiller.com/-/media/files/thomas-miller/publications/2019-thomas-miller-report-and-accounts.pdf

Managing and responding to risk 15

The 4Ts of hazard response

Significant risks facing an organization are those that have:

- high or very high impact in relation to the benchmark test for significance;
- high or very high likelihood of materializing at or above the benchmark level;
- high or very high scope for cost-effective improvement in control.

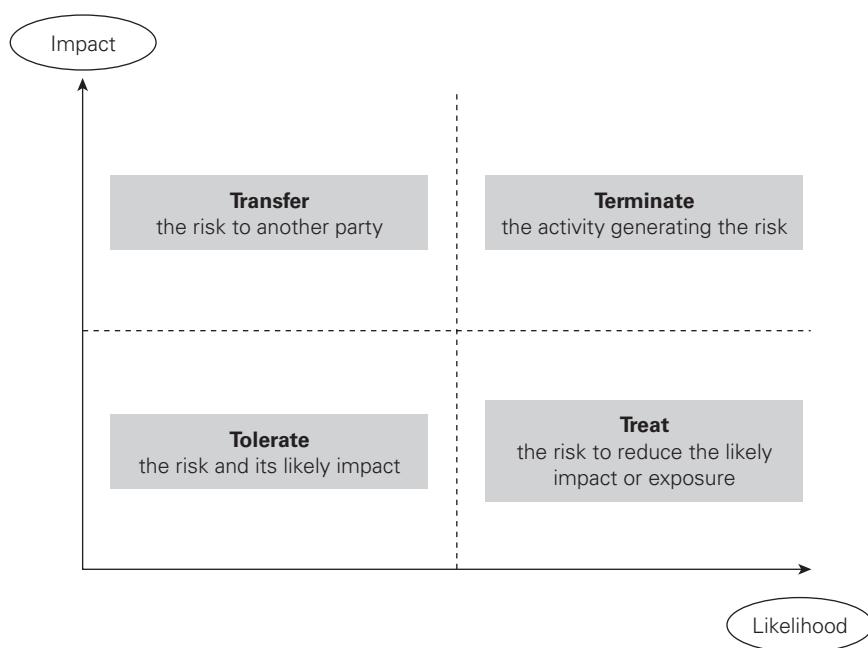
Generally speaking, it is only significant risks that require attention at the most senior level of the organization. However, it is appropriate that compliance risks also receive boardroom attention. In practice, the board will expect these compliance risks to be properly managed and the board will only receive routine/annual reports describing risk performance, or a special report if a specific issue has arisen. The organization will seek to introduce effective and efficient controls to minimize compliance risks.

The benchmark test for significance should be set at a level that represents a significant impact for the organization. The organization then needs to review the controls in place and decide whether further actions are required for those risks. For hazard risks, the range of responses available is often described as the 4Ts (tolerate, treat, transfer and terminate).

There is a broad range of terminology available to describe risk response options. In fact, both British Standard BS 31100 and ISO 31000 use the term ‘risk treatment’ as the more generic description. For example, the British Standard defines risk treatment as the ‘process of developing, selecting and implementing controls. Likewise, Guide 73 defines risk treatment as the ‘process to modify risk’.

The terminology used in *The Orange Book* has been adopted here for the risk response stage of the risk management process. The options for responding to risk can then be identified as the 4Ts. Appendix B contains information on the alternative definitions that are used by different publications.

More information and a brief description of each of the 4Ts is provided in Table 15.1.

Figure 15.1 Risk matrix and the 4Ts of hazard management**Table 15.1** Description of the 4Ts of hazard response

1	Tolerate Accept/retain	The exposure may be tolerable without any further action being taken. Even if it is not tolerable, the ability to do anything about some risks may be limited, or the cost of taking any action may be disproportionate to the potential benefit gained.
2	Treat Control/reduce	By far the greater number of risks will be addressed in this way. The purpose of treatment is that, whilst continuing within the organization with the activity giving rise to the risk, action (control) is taken to constrain the risk to an acceptable level.
3	Transfer Insurance/contract	For some risks the best response may be to transfer them. This might be done by conventional insurance, or it might be done by paying a third party to take the risk in another way. This option is particularly good for mitigating financial risks or risks to assets.
4	Terminate Avoid/eliminate	Some risks will only be treatable, or containable to acceptable levels, by terminating the activity. It should be noted that the option of termination of activities may be severely limited in government when compared to the private sector.

Table 15.2 Key dependencies and significant risks

FIRM risk scorecard	Example dependencies	Example of a significant risk
Financial	Availability of funds	Insufficient funds available from parent company
Correct allocation of funds	Inadequate profit because of incorrect capital expenditure decisions	
Internal control	Fraud occurs because of inadequate internal controls	
Liabilities under control	Higher than expected liabilities arise in the pension fund	
Infrastructure	People	Failure to achieve/maintain health and safety standards
Premises	Damage to key location caused by insured peril	
Processes	IT control systems not available because of virus or hacker activity	
Products	Disruption because of failure of supplier	
Reputational	Brand	Product recall causes damage to product image and brand
Public opinion	Lost sales or revenue because of change in public tastes	
Regulators	Regulator enforcement action causes loss of public confidence	
CSR	Allegations of unethical product sourcing causes loss of sales	
Marketplace	Regulatory environment	Change in tax regime results in unbudgeted tax demands
Economic health	Decline in world or national economy reduces consumer spending	
Product development	Changes in technology reduce product appeal and sales	
Competitor behaviour	Competitor substantially reduces prices to win market share	

Figure 15.1 indicates the dominant response in relation to each of the 4Ts according to the position of the risk on a risk matrix.

In order to give some context to the range of risks that is being considered, Table 15.2 provides examples of the range of potentially significant risks associated with the headings of the FIRM risk scorecard. Assessment of each of the risks will enable the organization to place the risk on a risk matrix. The position of the risk on the risk matrix will then indicate the most likely response to that risk. If the risk assessment is undertaken at the current level of risk, the effect of the existing controls will already have been evaluated as part of the risk assessment exercise.

Consider the case of a supplier to a major grocery store. They need to respond to the call by the store to reduce the cost of the finished goods they supply. Also, a recent failure its own supply chain due to a blockage in the logistics chain caused the supplier to review its supply chain risks. Its responses are decided in relation to all 4Ts. The supplier might decide that it has to tolerate the margin reduction request. It has also decided to treat/reduce the supply chain risk by arranging for an alternative source of its input closer to home. It will terminate existing arrangements with the transport company that had the initial issue and use alternative supplier for the (reduced) supply it needs. The company might also investigate the possibility of extending its cargo insurance, so that it can transfer the cost of future failures in the supply chain.

Tolerate

Risk tolerance is defined in ISO Guide 73 as the organization's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives. The guide then adds that risk tolerance can be influenced by legal or regulatory (compliance) requirements. The comment about legal or regulatory requirements is very relevant, in that organizations will often have to tolerate a risk because of legal or regulatory requirements, even in circumstances where the organization would otherwise not wish to tolerate that risk. It should be noted that tolerance relates to a specific or individual risk, rather than the more general approach represented by risk appetite. Risk appetite refers to the amount and type of risk that an organization is willing to pursue or retain.

There is a difference between when an organization is willing to tolerate a risk and the concept of risk tolerance. An organization may tolerate a risk even if it is higher than the organization would usually choose to accept if it will help to achieve its objectives. Risk tolerance represents the boundaries of risk taking outside of which the organization is not prepared to venture in pursuit of its objectives. In Figure 26.1, the central sections of concerned zone and cautious zone draw the boundary around the risk tolerance. These zones define the boundaries within which the organization desires the level of risk to be confined.

An organization may have to tolerate risks that have a current level beyond its comfort zone and its risk appetite. On occasions, an organization may even have to tolerate risks that are beyond its actual risk capacity. However, this situation would not be sustainable and the organization would be vulnerable during this period.

When the hazard risk is considered to be within the risk appetite of the organization, the organization will tolerate that risk. Risk tolerance is shown as the approach that will be adopted in relation to low-likelihood risks with low impact. However, an organization may decide to tolerate risk levels that are high because they are associated with a potentially profitable activity or relate to a core process that is fundamental to the nature of the organization.

It is unusual for a hazard risk to be accepted or tolerated before any risk control measures have been applied. Generally speaking, a risk only becomes tolerable when all cost-effective control measures have been put in place, so that the organization is accepting or tolerating the risk at its current level. Certain control measures may have been applied because the inherent level of the risk may have been unacceptable. Control effort seeks to move the risk to the low-likelihood/low-impact quadrant of the risk matrix, as illustrated in Figure 16.3.

Sometimes risks are only accepted as part of an arrangement whereby one risk is balanced against another. This is a simple description of neutralizing or hedging risks, but on a business level this may represent a fundamentally important strategic decision. For example, an electricity company operating independently in the northern part of the United States may have to accept the impact of variation in temperature on electricity sales. By merging (or setting up a joint venture) with an electricity company in the southern states, the combined operation will be able to smooth the temperature-related variation in electricity sales. They will sell more electricity in the north during cold weather, when demand in the south is low. Conversely, they also sell more electricity for air-conditioning units in the south in the summer, when demand for electricity in the north may be lower.

Treat

When the level of risk exposure (likelihood) associated with a particular hazard is high but the potential loss (impact) associated with it is low, the organization may wish to treat the risk. Risk treatment will often be undertaken with the risk at the inherent and/or current level, so that when the risk has been treated, the new current level or target level may become tolerable.

Actions to improve the standard of risk control will always be under constant review in an organization. On a personal level, wearing a seat belt when driving a car or fitting an intruder alarm in a house are examples of risk reduction actions. Improvements to standards of risk control in relation to physical (insurable) risks are well known. Fitting sprinklers to buildings, providing enhanced building security

arrangements and employee security vetting are all examples of risk improvement actions designed to better manage hazard risks.

When identifying suitable risk treatment options, the organization will need to look at the effect of the treatment on the likelihood of the risk materializing as well as looking at the impact of the risk should it materialize. Cost-effective risk treatments will need to be selected and the effect of different control measures can be shown on a risk matrix, as in Figure 16.4.

There is an issue of terminology associated with treating the risk. ISO 31000 considers that ‘treat risk’ is the main heading under which various options exist, such as:

- avoiding the risk by deciding not to start or continue with the activity;
- taking or increasing the risk in order to pursue an opportunity;
- removing the risk source;
- changing the likelihood or the consequences;
- sharing the risk with another party or parties;
- retaining the risk by informed decision.

Other risk management standards refer to ‘risk response’ as the main heading and this is the approach taken in this chapter. Using risk response as the main heading then gives rise to the options of tolerate, treat, transfer and terminate. As with all issues of terminology, it is for the organization to establish its own risk vocabulary, one that is consistent with the external, internal and risk management context.

In some cases, terminology will be dictated by the external context. For example, banks and other financial institutions will need to use the terminology of the regulator. On occasions, terminology is dictated by the internal context within the organization. If the terminology that has developed within the organization is inconsistent with the terminology in ISO 31000, it is probably the case that the risk manager would be better advised to use the terminology that already exists within the organization, rather than trying to introduce new terms or new meanings for existing terms.

Transfer

When the likelihood of a risk materializing is low but the potential is high, the organization may wish to transfer that risk. Insurance is a well-established mechanism for transferring the financial impact of losses arising from hazard risks and (to a lesser extent) control risks. The issues associated with the use of insurance as a risk transfer mechanism are considered in more detail in Chapter 18.

In some cases, risk transfer is closely related to the desire to eliminate or terminate the risk. However, many risks cannot be transferred to the insurance market,

either because of prohibitively high insurance premiums or because the risks under consideration have (traditionally) not been insurable, for example reputation.

Risk transfer can be achieved also by contractual agreement. It may also be possible to find a joint venture partner, or some other means of sharing the risk. Risk hedging or neutralization may therefore be considered to be a risk transfer option, as well as a risk treatment option.

The cost of risk transfer is a component of risk financing. Once again, there is variation in the definitions used. In relation to risk financing, BS 31100 states that risk financing involves the cost of contingent arrangements for the provision of funds to meet the financial impact of a risk materializing. Such arrangements are usually provided by insurance, and insurance is, therefore, finance that is contingent upon certain insured events taking place.

ISO 31000 also considers that the cost of risk financing should include the provision of funds to meet the cost of risk treatment. In this text, resourcing of controls is considered to be a separate step in the risk management process. This is another example that illustrates that there is no universally agreed or common language of risk.

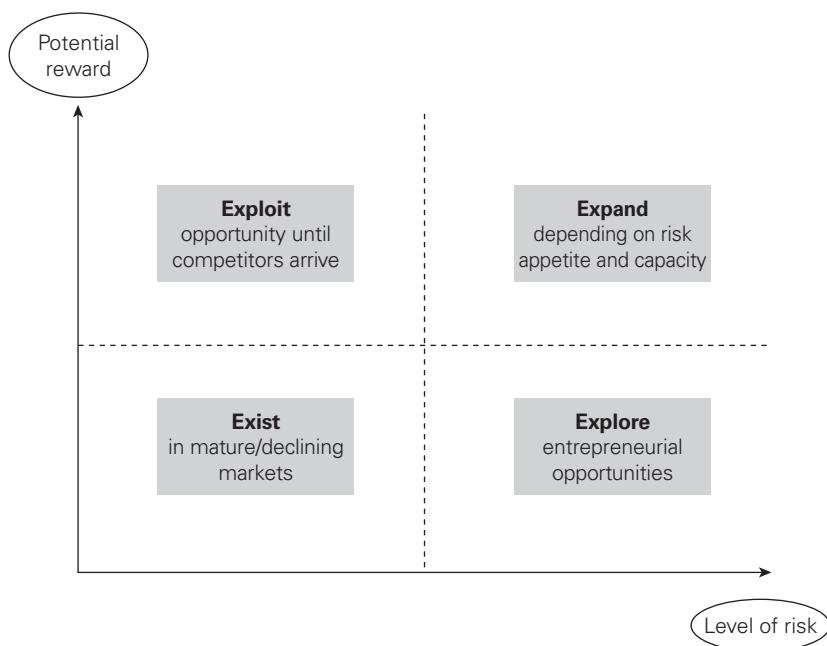
There is another issue of terminology with the use of the phrase ‘risk transfer’. ISO 31000 recommends that risk sharing should be used in preference to risk transfer. The argument is that a risk can never be fully transferred and whatever the intention of the parties, the risk will always be, to some extent, shared. This is an accurate analysis, but the choice of terminology used within an organization will also be influenced by other factors. In relation to risk sharing, the insurance industry uses the terminology risk transfer. It may be difficult for the enterprise risk manager to insist on the use of the phrase risk sharing when the insurance manager in the organization prefers to use the terminology of risk transfer because that is the standard terminology used in part of the external context that is the insurance market.

Terminate

When a risk is both of high likelihood and high potential impact, the organization may wish to terminate or eliminate the risk. It may be that the risks of trading in a certain part of the world or the environmental risks associated with continuing to use certain chemicals are unacceptable to the organization and/or its stakeholders. In these circumstances, appropriate responses would be elimination of the risk by stopping the process or activity, substituting an alternative activity or outsourcing the activity that is associated with the risk.

An organization may wish to terminate a risk, but it could be the case that the activity that gives rise to it is fundamental to the ongoing operation of the organization. In such circumstances, the organization may not be able to terminate or eliminate the risk entirely and thus will need to implement alternative control measures.

Figure 15.2 Risk versus reward in strategy



This is a particular issue for public services. There may be certain risks that have high likelihood and high impact, but the organization is unable to terminate the activities giving rise to them. This may be because the activity is a statutory requirement placed on a government agency or public authority. The public service imperative may restrict the ability to cease the activity, so the organization will need to introduce control measures, to the greatest extent that is cost-effective.

It is likely that such control measures will be a combination of risk treatment and risk transfer. As these control measures are applied, the risk will move to a level where the organization will be able to tolerate it. Because of the variable nature of risks, it may not be possible to get all risks to a level that is within the risk appetite of the organization. The organization may find that it has to tolerate risks beyond its empirical risk appetite in order to continue to undertake a certain activity.

Strategic risk response

The overall approach to the management of control and opportunity risks is similar to the approach adopted for the management of hazard risks. However, there are

sufficient differences in the range of options available for these to be presented separately. It is worth remembering that projects normally reflect and implement the tactics that are being employed to implement strategy.

Figure 15.1 illustrates the 4Ts of hazard risk management and the type of controls that are most likely to be associated with each type of hazard risk response. The types of controls are considered below. This chapter has been concerned almost exclusively with responding to hazard risks. The 4Ts represent the options for mitigating hazard risks. Figure 15.2 suggests that there are a range of responses available for the management of opportunity risks. Developing and implementing effective and efficient strategy will require the evaluation of the level of risk associated with each available strategy and the level of reward that the strategy will deliver.

The 4Es of opportunity management are set out as explore, exit, exploit and exist. There is a close relationship between the 4Es and the status of the organization, as illustrated in Figure 15.2. A start-up operation will face a higher level of risk and low potential rewards.

Entrepreneurial opportunities will be explored at this time. As the organization grows, potential rewards will increase while the level of risk will remain high. The organization will seek to achieve growth, but may feel that growth is too slow or the level of risk remains too high, and if so, it will exit from those operations.

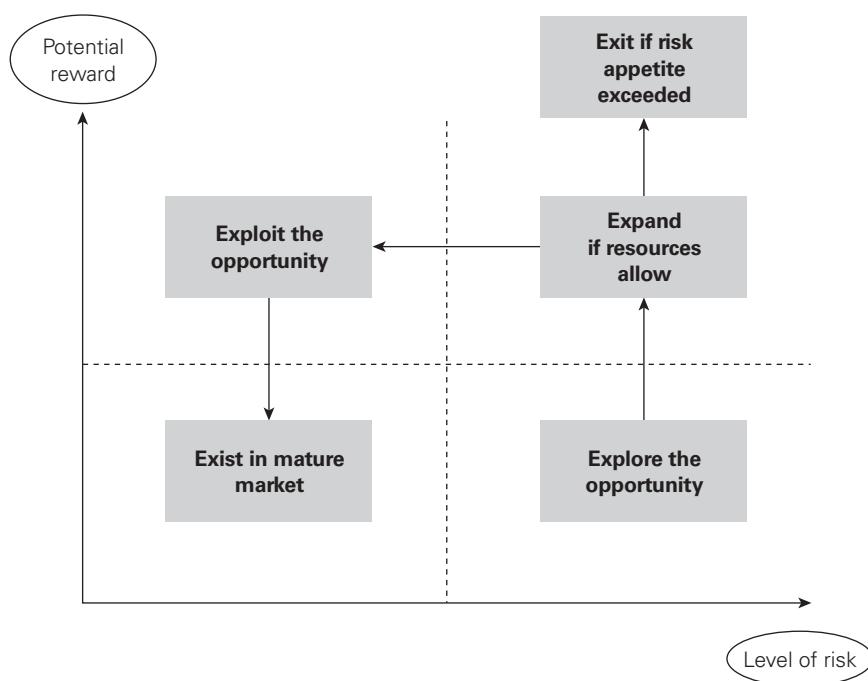
After a period of growth, the organization should be achieving a high reward for a reduced risk. This represents the phase where the organization will exploit opportunities until competitors arrive. This is a mature operation. All mature operations are exposed to the possibility of decline, although many organizations choose to exist in a mature, declining market, where risk exposure is low and so are potential rewards.

The application of the 4Es to the management of strategic, opportunity or speculative risks is consistent with the description of risk and reward offered by Figure 1.3. However, pursuing opportunity risks and the development of strategic objectives are the most important issues for many organizations. Risk management input into strategic decision making may not always be as robust and well-structured as the risk management input into operations and projects.

The allocation of the dominant types of responses and controls to each of the four quadrants shown in Figure 15.2 is similar to the allocation of the 4Ts using hazard risk management. Existing in a mature or declining market is similar to accepting uncertainty in tactics and tolerating hazard risks. Exploring opportunities is similar to looking at the options for treating hazard risks. It is in the area of exploiting opportunities and expanding opportunities where differences in approach between the management of hazards and uncertainties compared with the management of opportunities becomes most evident.

Figure 15.3 shows a refinement to Figure 15.2 in that the area of high risk and potentially high reward is evaluated in a little more detail by taking account

Figure 15.3 Opportunity risks and risk appetite



of risk appetite. An organization may find that it has a viable business opportunity but does not have the resources to exploit it on its own. In these circumstances, the organization has three main choices. It may exit the opportunity because it does not have the risk appetite or risk capacity to pursue that opportunity. It may sell the opportunity on to an organization that does have the appetite, capacity and resources to exploit the opportunity or it may seek to share that opportunity.

Exiting the opportunity may be the appropriate option, because the organization does not have the risk appetite, capacity or resources to pursue the opportunity and has not been able or willing to find a partner to buy or share it. However, most organizations with a viable opportunity will wish to gain from the identification of that opportunity. Selling the opportunity may provide a profitable exit, but sharing it with, for example, a joint venture partner may be a better long-term option.

Entering into a joint venture partnership will reduce the level of risk faced by the organization, but will result in sharing of the benefits. This decision will depend on business strategy, risk appetite, risk capacity and the availability of suitable business partners. As well as a joint venture partnership, exploiting business opportunities may be possible by sharing the risk, using means such as outsourcing to share the risk with others in the supply chain.

It should be noted that Figure 15.3 represents a flow chart from start-up (explore opportunities) to growth (expand), then to a mature organization (exploit) before moving into decline (exist). These stages in a simple business lifecycle are shown in Figure 1.3. It should be noted that as the organization is looking to expand, it will have the option of exiting if the risk appetite and/or risk capacity of the organization would be exceeded. This extends the 4Es approach to become 5Es, depending on risk appetite. The box below provides an example of this approach applied to opportunity management, although the terminology (as is often the case in risk management) is a little different.

Opportunity evaluation and response

The purpose of the evaluation and response is to decide which opportunities require a response and what the recommended response will be. The following are the key terms and concepts when deciding how to respond to an opportunity and they can be used in combination:

- Enhance: The opportunity equivalent of ‘mitigating’ a risk is to *enhance* the opportunity by increasing the probability and/or the impact.
- Exploit: Equivalent to the ‘avoid’ response, but the ‘exploit’ strategy seeks to make the opportunity definitely happen.
- Ignore: The ‘acceptance’ strategy takes no measures to deal with a hazard risk, and opportunities can be *ignored*, with a reactive approach but no explicit actions.
- Sharing (transfer) opportunity: ‘Share’ strategy for opportunities seeks a partner able to manage the opportunity who can maximize the chance of it happening.

Risk treatment controls for hazard risks

16

Types of controls

There are a range of controls that can be applied to hazard risks. The most convenient classification system is to describe these controls as preventive, corrective, directive and detective. This is the risk classification system suggested in *The Orange Book* and is outlined in Table 16.1.

Table 16.1 Description of types of hazard controls

1 Preventive (terminate)	These controls are designed to limit the possibility of an undesirable outcome being realized. The more important it is to stop an undesirable outcome, then the more important it is to implement appropriate preventive controls.
2 Corrective (treat)	These controls are designed to limit the scope for loss and reduce any undesirable outcomes that have been realized. They may also provide a route of recourse to achieve some recovery against loss or damage.
3 Directive (transfer)	These controls are designed to ensure that a particular outcome is achieved. They are based on giving directions to people on how to ensure that losses do not occur. They are important, but depend on people following established safe systems of work.
4 Detective (tolerate)	These controls are designed to identify occasions when undesirable outcomes have been realized. Their effect is, by definition, 'after the event' so they are only appropriate when it is possible to accept that the loss or damage has occurred.

In relation to hazard risks, the control options of preventive, corrective, directive and detective (PCDD) represent a clear hierarchy of controls. The relationship between these four types of controls and the dominant risk of response for different levels of risks is illustrated on the risk matrix shown in Figure 15.1. Table 16.2 gives examples of these four types of controls in relation to health and safety risks.

Preventive controls are designed to limit the possibility of an undesirable hazard event occurring. The majority of controls implemented in organizations in response to hazard risks are preventive controls. For health and safety risks, preventive controls will include substituting a less hazardous material in the activity or enclosing the activity so that employee exposure to dust or fumes is eliminated.

Corrective controls are designed to correct undesirable circumstances and reduce unacceptable risk exposures. Such controls provide a key method whereby the risk is treated so that it becomes less likely to occur and/or the impact is much reduced. In general terms, corrective controls are designed to correct the situation. For example, machinery guards are corrective controls.

Directive controls are designed to ensure that a particular outcome is achieved. In health and safety terms, directive controls would include instructions/directions given to employees to follow, for example, in the use of personal protective equipment. Training in how to respond to a particular risk event and detailed instructions and

Table 16.2 Examples of the hierarchy of hazard controls

Generic control category	Hierarchy of controls for health and safety risks	Hierarchy of controls for fraud risks
Preventive	Elimination or removal of the source of the hazard Substitution of the hazard with something less risky	Limits of authorization and separation of duties Pre-employment screening of potential staff
Corrective	Engineering containment using barriers or guards Exposure reduction by job rotation or limitation on hours worked	Use of insurance to recover any losses Continuous back-up systems
Directive	Training and supervision to enforce procedures Personal protective equipment and improved welfare facilities	Accessible, detailed, written systems and procedures Training to ensure understanding of procedures
Detective	Health monitoring to enquire about potential symptoms Health surveillance to find early symptoms	Reconciliation, audit and review by internal audit Whistleblowing policy to report (alleged) fraud

procedures are directive controls. Directive controls are also associated with actions that must be taken in the event of a loss to limit the damage and contain the costs.

Detective controls are designed to identify occasions when an undesirable outcome has occurred. The control is intended to detect when these undesirable events have happened, to ensure that the circumstances do not deteriorate further. An example of detective controls in a project is undertaking a post-incident review.

The bow-tie representation of the risk management process is a convenient way of illustrating the role of the four types of controls. The relevance of the types of controls to the bow-tie presentation of the risk management process is shown in Figure 16.1. For the sake of illustration, this figure uses the same hazard of damage to premises as represented in Figure 11.2. There is a clear hierarchy of effectiveness of controls that is represented by the order preventive, corrective, directive and finally detective.

Disaster recovery planning (DRP) and business continuity planning (BCP) can be seen as both directive and corrective. Since they are concerned with crisis management they cannot be easily classified as a PCDD type of control and could be considered to be a fifth type of control. In all cases, crisis management will involve directions to the involved parties as to how they should behave if the crisis arises. It could be argued that these are directive controls. Normally, detective controls relate to identification of circumstances where a risk has materialized at a fairly low level with limited impact and consequences. Clearly, DRP and BCP relate to circumstances where risks have materialized at crisis level. Therefore, it is inappropriate to classify DRP and BCP as detective controls.

Figure 16.1 Bow-tie and types of controls

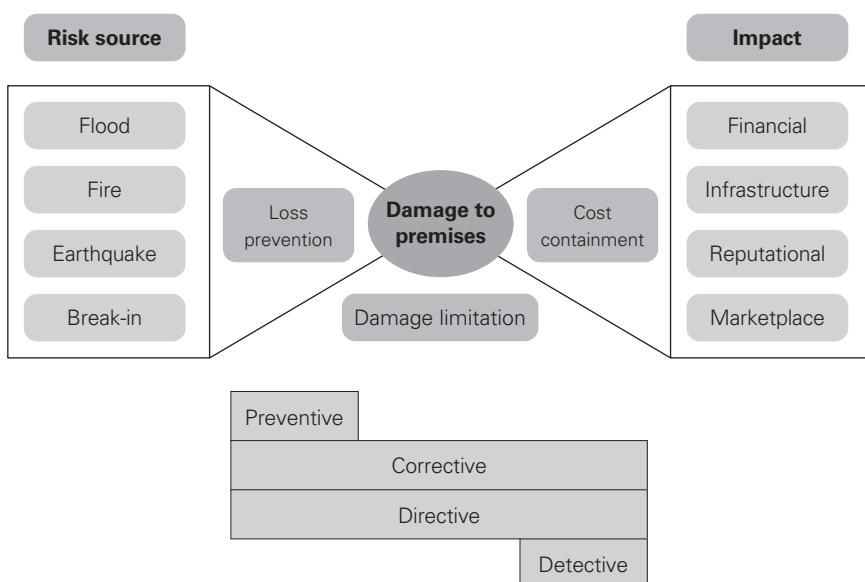


Table 16.3 Application of PCDD

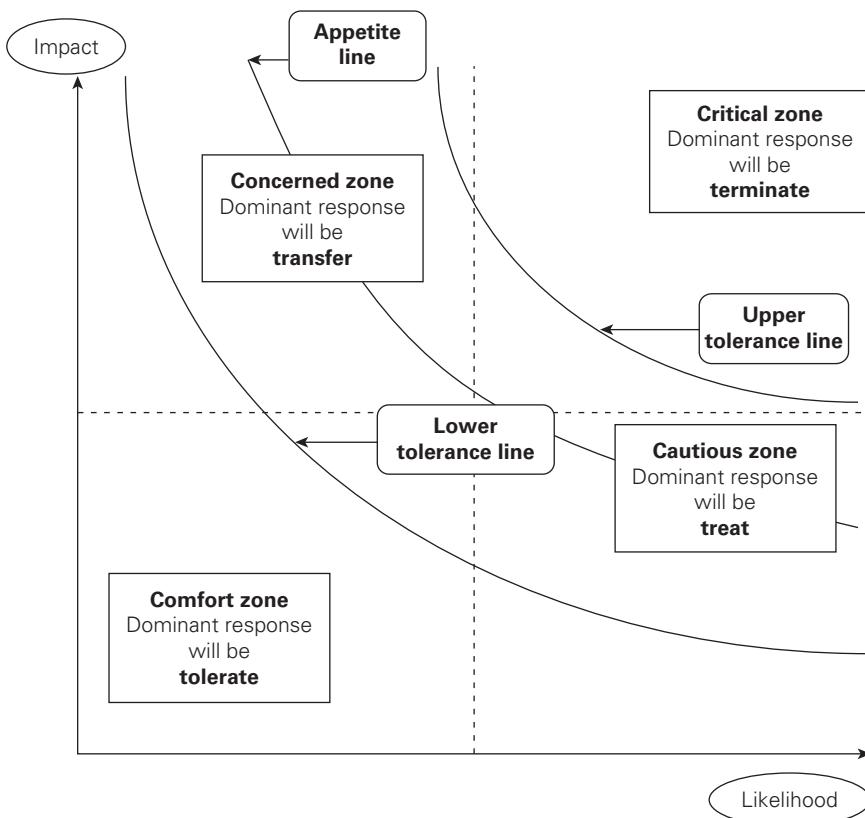
Control type	Example action
Preventive	Review of vehicle routing and realistic estimates on delivery schedules so that drivers do not need to drive dangerously to arrive on time
Corrective	Enhanced maintenance procedures and improved arrangements for drivers to report vehicle defects
Directive	Defensive driver training and the provision of a vehicle driver handbook with practical advice that is easy to understand and follow
Detective	Routine review of drivers' licences to check for penalty points, routine inspections of vehicles to discover and report damage, review of fuel consumption to identify drivers with an aggressive driving style

Hazard risk zones

Although the 4Ts of hazard response can be illustrated on a simple risk matrix, the options are not that clear cut. A small increase in risk likelihood and potential impact would not completely change the approach of the organization to a particular risk. Figure 16.2 demonstrates an analysis that illustrates that the 'cautious' and 'concerned' areas fall within the boundaries of acceptability – or tolerances. The comfort zone is predominantly for low-likelihood/low-impact events. As can be seen, there is a level of potential impact that will always be within the comfort zone. Likewise, there is a level of risk likelihood that is always considered to be so low that it will not happen.

However, as risk likelihood and potential impact increase, a point is reached where judgement is required as to whether the risk is above the lower tolerance line and within the tolerance limits for the organization. Judgement is required within the cautious zone and actions will usually be taken to treat and/or transfer the risks within that zone. The line that divides the cautious zone and the concerned zone represents the risk appetite of the organization. The cautious zone and the concerned zone together illustrate the acceptable variability of the level of risk and can be considered to be the tolerance of the organization to acceptable variability or volatility in the level of that particular risk.

As the risk likelihood and potential impact further increase, the upper tolerance line is reached. When the risk gets above this line, the organization will consider those risks to be critical, as they are outside tolerance limits and will wish to terminate exposure to them. In certain circumstances, the organization will not be able to terminate these risks, either because they may represent a business imperative or because they are associated with a high-risk/high-reward strategy that the board has adopted.

Figure 16.2 Hazard risk zones

Preventive controls

These are the most important type of risk controls, and all organizations will use preventive controls to treat certain types of risks. Prevention or elimination of all risks is not possible on a cost-effective basis, nor may it be desirable for the future of the organization and the continuation of certain activities.

Examples of preventive controls include the separation of duties, whereby no one person has authority to act without the consent of another when paying an invoice, or the use of barriers or guards on machinery. In health and safety terms, preventive controls include the elimination or removal of the hazard and providing a less risky substitute. For example, a hazardous chemical used in a cleaning operation may be substituted with a less harmful alternative.

The advantage of preventive controls is that they eliminate the hazard, so that no further consideration of it is required. In reality, this may not be a cost-effective option and may not be possible for operational reasons. The disadvantages of preventive

controls are that beneficial activities may be eliminated and either outsourced or replaced with something less effective and efficient.

Health and safety practitioners refer to the elimination of hazardous activities ‘so far as is reasonably practicable’. Achieving something so far as is reasonably practicable involves the balance between cost in terms of time, trouble and money against the benefit in terms of the reduction in the level of risk that is achieved.

Corrective controls

Corrective controls are the next option after it has been decided that preventive controls are not technically feasible, operationally desirable or cost-effective. Corrective controls will ‘repair’ or correct things after an event occurs but need to be put in place prior to the event. They are capable of producing an entirely satisfactory result, whereby the current level of risk is reduced to within the risk appetite of the organization.

Examples of corrective controls would be software patches on operating systems, new employee policies or taking disciplinary action.

The advantage of many corrective controls is that they can be simple and cost-effective. Nor do they require the elimination or replacement of existing practices and procedures. The controls can be implemented within the framework of existing activities. The disadvantage of some corrective controls is that the marginal benefits that are achieved may be difficult to quantify or confirm as cost-effective.

Corrective controls can be over-engineered, and their cost can be disproportionate to the benefit that is achieved. Very often, corrective controls are put in place because of regulatory requirements and it is for the organization to ensure that the appropriate level of corrective control is achieved in order to comply with the minimum requirements of legislation.

The design and implementation of corrective controls is often the cause of considerable discussion and potential disagreement. For example, fitting sprinklers as a corrective control that will activate in case of fire will often be viewed as inappropriate in computer rooms where water would damage records. In such circumstances more expensive suppression systems may be considered and factored into a cost/benefit calculation.

Directive controls

Organizations will be familiar with the directive controls, because staff will need to be advised of the correct way of undertaking specific tasks. Where tasks involve a level of risk, documented procedures, together with information, training and instruction, can be seen as directive controls. Therefore, directive controls are likely to be in place for most risks, regardless of whether other types of controls also exist.

An example of directive controls is the requirement to wear personal protective equipment when undertaking potentially dangerous activities. Staff will need to be trained in the correct use of the equipment and a level of supervision will be required in order to ensure that it is used correctly.

The advantage of directive controls is that the risk control requirements can be explained during a normal training and instruction session provided for staff. However, directive controls, especially in relation to health and safety risks, represent a low level of control that may require constant supervision in order to ensure that the correct procedures are being followed.

Directive controls will always be a component in the overall approach to risk control adopted by any organization but, on their own, they represent an insecure and unreliable method of risk control. There is a danger that procedures are not implemented in practice. By developing procedures, the organization acknowledges the risks exist and this imposes on it a duty to ensure the procedures are implemented, otherwise the organization will be unable to defend itself by claiming that it was not aware of the risks.

Contracts, including insurance policies, are also a form of directive control, as they may require certain conditions to be met, such as the use of five-lever mortice deadlocks in theft policy.

Generally, directive controls will be the first response to an unexpected event if it occurs. Instead of a preventive control, it is often easier to implement procedures to reduce the risk by direction, especially if it is a safety risk. This immediate response will then allow corrective controls to be designed and implemented as the new set of circumstances becomes clear and/or stabilizes.

Detective controls

As suggested in the title, detective controls are those procedures that identify when the hazard has materialized. This means they will come into play after the event has materialized, but can be justified in certain circumstances if other controls are unable to completely eliminate the risk.

Examples of detective controls include the extensive use of testing during a health crisis, stocktaking to ensure that goods have not been removed without authorization, or bank reconciliation exercises to detect unauthorized transactions. Post-implementation reviews will detect lessons learned from projects that can be applied in future. Detective controls are closely related to review and monitoring exercises undertaken as part of the risk management process.

The advantage of detective controls is that they are often simple to administer and they will provide an early warning that other risk control measures have broken down. The disadvantage of detective controls is that the risk will already have materialized before it is detected.

For example, detection of fraud is often only possible after the fraud has taken place, but there are considerable advantages in detecting it early, so that the nature and scale of the fraud may be reduced. The next box discusses introducing new financial controls in a charity.

Financial controls for charities

Financial controls will reduce the risk of error and fraud, and their implementation should enhance the element of trust required from donors. They should be discussed and approved by the trustees to ensure their support before implementing any new controls. Controls can then be implemented, noting who is responsible for each control. By making someone accountable for a financial control, it is more likely to be effective.

Controls are only good if they are relevant; therefore, you need to ensure that you routinely review your controls to see if they are still effective. As things change, you need to think about making changes to your controls as your organization evolves. It can be hard to make changes to existing controls, but assessing why the controls are no longer valid and how new controls can help the organization will help you in putting the changes into place.

Cost of risk controls

When considering the cost of implementation of controls, attention needs to be paid to the change in the level of risk by applying that control measure. This involves a review of the change from the inherent level of a risk (with no control measures in place) to the current level of risk (taking account of the control measures currently in place).

Figure 16.3 provides an illustration of the control effect or control vector when controls are put in place. When considering the inherent, intermediate (when more than one control is in place) and target risk levels, the organization should be aware of the cost involved in implementing controls. The cost of the control measures should be considered to be part of the total cost of risk for the organization. The organization can then evaluate whether the controls in place are cost-effective.

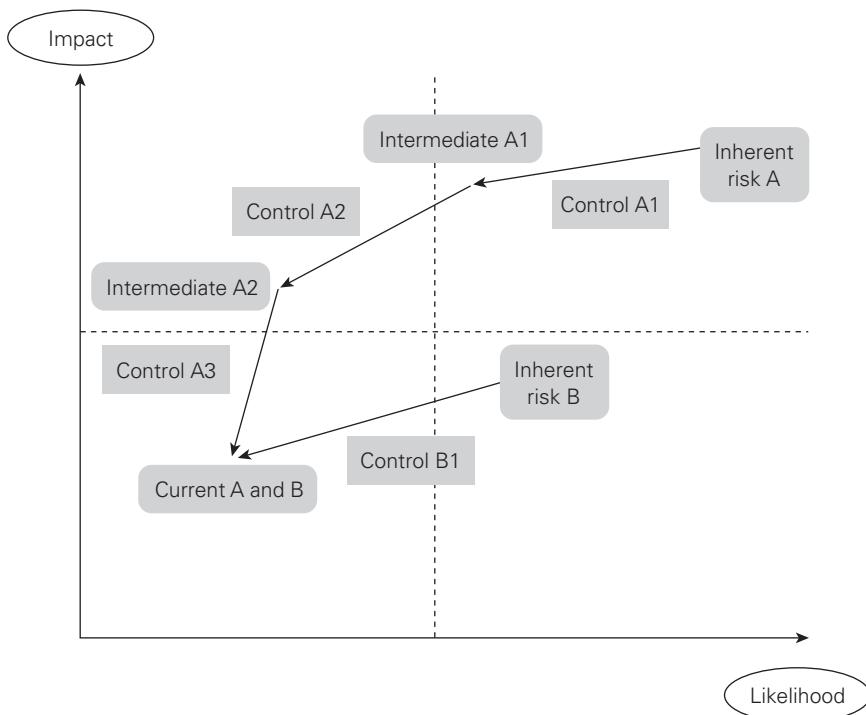
In Figure 16.3, a series of lines are drawn for Risk A to represent the effect of each individual risk control measure. The longer the line, the greater the effect of the control. It is also the case that the longer the line, the greater the control effort, in terms of management time, effort and money. For Risk A, three controls (Controls A1, A2

and A3) are required to get to the target level of risk. For Risk B, only one control is required (Control B1) and this demonstrates that much more effort is needed to maintain Risk A at the target level of risk. Management and internal audit need to be aware of this, so that they can ensure that all of the controls (especially for Risk A) are operating in an effective and efficient manner.

A simple diagram like Figure 16.3 provides an illustration of the distance between the inherent and current level of the risk. If a lower target level of risk is established, additional control effort will be required in moving the level of risk from the current to a new target level (not shown in the figure). This simple illustration of control effort is important, and demonstrates that there is value in undertaking a risk assessment at the inherent level of risk (if this is possible), so that the required control effort can be clearly identified and illustrated.

If a calculation is undertaken of the risk exposure at the original level and a further calculation is undertaken of the risk exposure at the new level, the overall benefit of each control can be measured. Consideration of the cost of each control can then be undertaken, so that a cost–benefit analysis of individual controls may be completed. This will be an important exercise for the organization to undertake, so that cost-effective risk control priorities may be established.

Figure 16.3 Illustration of control effect

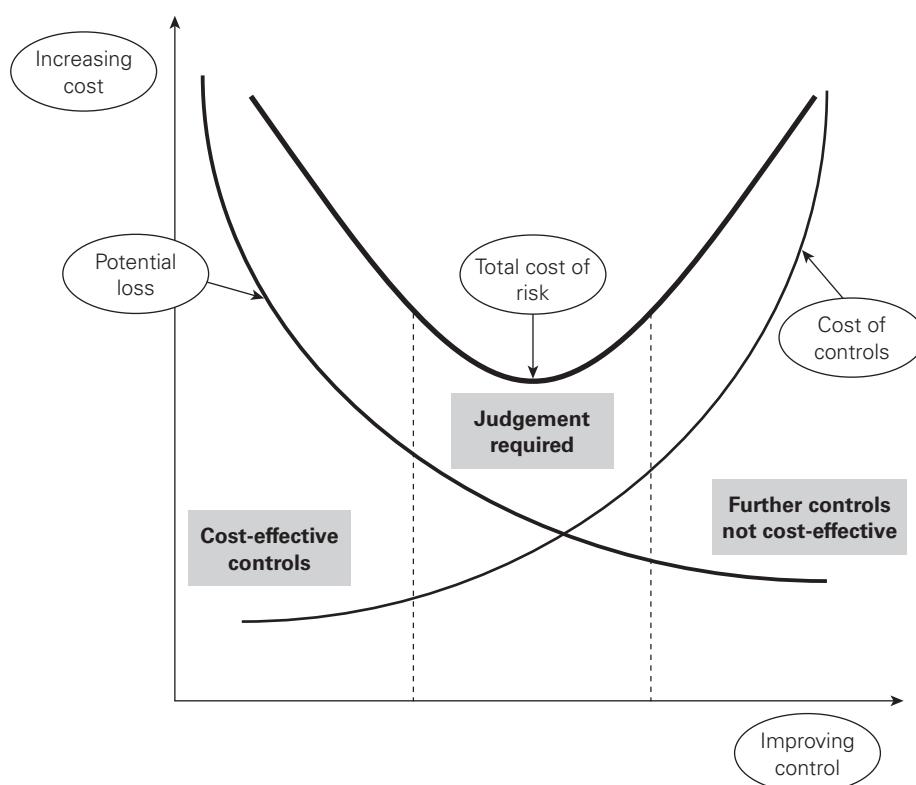


Risk treatment is sometimes referred to as risk response or risk control, and it includes the selection and implementation of actions to reduce risk likelihood and risk impact. The examples in the sections below cover the main hazard risks that are likely to be of concern to an organization. In each case, the section sets out to describe what can go wrong in relation to the hazard, and the considerations and the issues that need to be evaluated. The control options that are available in relation to that particular risk are considered, followed by consideration of the controls that are necessary and appropriate.

Table 16.2 provides examples of the four types of controls described in Chapter 16 as applied to two types of hazard risks. The examples of fraud and health and safety are selected, so that the application of different types of controls to these two hazards can be illustrated. For other hazard risks, a similar generic approach can be taken and the types of controls that are possible can be listed, using the format of preventive, corrective, directive and detective controls.

When selecting and implementing controls, it is important to ensure that cost-effective controls are selected. Figure 16.4 plots increasing the level of control

Figure 16.4 Cost-effective controls



(horizontal axis) against the increasing cost of controls (vertical axis). By adding the total cost of controls and the equivalent potential loss for each level of control, the figure illustrates that there is an optimum level of control that represents the lowest combined cost as a sum of the cost of control and the level of potential losses.

It can be seen in Figure 16.4 that a significant reduction in potential loss is achieved with the introduction of low-cost controls. This section of the diagram is labelled 'Cost-effective controls'. The centre section of the diagram illustrates that spending more on controls achieves a reduction in the net cost of risk up to a certain point. In this segment, judgement is required on whether to spend the additional sum on controls. On the right-hand side of the diagram, spending more on controls achieves only a marginal reduction in potential loss. In this segment, further controls are not cost-effective.

Ongoing monitoring and review

17

When considering how to respond to risk it is important that it is not done as a ‘once only’ approach, but to recognize that the ERM approach is the continuous application of ERM principles.

ISO 31000 recognizes the importance of feedback through ‘monitoring and review’, which ensures that the organization monitors risk performance and learns from experience. Furthermore, ‘establishing communication and consultation’ forms part of the risk management framework and stresses that consultation ‘involves participants providing feedback’.

Similarly, *The Orange Book* specifies that effective risk reporting, including reporting to the board on changes required in risk appetite, is necessary. They advise that clear reporting formats and dashboards are appropriate to form this reporting method but that a ‘Deep dive’ approach will be required for certain key risks.

The Orange Book 2020 – Section D: Risk monitoring

D10 – Monitoring should play a role before, during and after implementation of risk treatment. Ongoing and continuous monitoring should support understanding of whether and how the risk profile is changing and the extent to which internal controls are operating as intended to provide reasonable assurance over the management of risks to an acceptable level in the achievement of organizational objectives.

D11 – The results of monitoring and review should be incorporated throughout the organization’s wider performance management, measurement and reporting activities.

Recording and reporting aims to:

- transparently communicate risk management activities and outcomes across the organization;

- provide information for decision making;
- improve risk management activities; and
- assist interaction with stakeholders, including those with responsibility and accountability for risk management activities.

D12 – The ‘three lines of defence’ model sets out how these aspects should operate in an integrated way to manage risks, design and implement internal control and provide assurance through ongoing, regular, periodic and ad-hoc monitoring and review... When an organization has properly structured the ‘lines of defence’, and they operate effectively, it should understand how each of the lines contributes to the overall assurance required and how those involved can best be integrated and mutually supportive. There should be no gaps in coverage and no unnecessary duplication of effort. Importantly, the accounting officer and the board should receive unbiased information about the organization’s principal risks and how management is responding to those risks.

SOURCE HM Government (2020) *The Orange Book: Management of risk – principles and concepts*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866117/6.6266_HMT_Orange_Book_Update_v6_WEB.PDF

The importance of monitoring

Risks are constantly changing as the external environment alters or internal systems change. It may be that since the initial assessment there have been changes to the regulations under which the organization operates or that new competitors or digital disruption have taken effect. Due consideration will need to be given to economic factors or geopolitical concerns, which may have changed since last reviewed.

Ongoing monitoring of the work that has been performed to analyse, categorize, evaluate and assess the risk should therefore be undertaken at regular intervals. This is especially important for risks that may occur over time if the speed at which they occur may be altered by mitigation taken at the appropriate time.

In addition to monitoring risks, any review should also include a re-evaluation of any mitigation plans to ensure the assumptions that applied when deciding upon the mitigation remain applicable. Without this regular review the mitigation itself may become an unconscious risk which is naively being accepted.

Monitoring risks at intervals will enable a re-assessment of the magnitude and likelihood to assure the ERM practitioner that the risk remains within appetite. This will enable reporting to management if risks have expanded beyond the appetite of the organization and allow risk treatment to occur. Alternatively, a review may show that the appetite of the organization for that risk may have also changed.

By re-evaluating risks, it may be that new risks have emerged that require evaluation and a re-prioritization or ranking of other risks. Following review, some risks may in fact have reduced as threats and do not require the same allocation of resource as previously.

When reviewing opportunity risks, such as new markets, the factors that influence the uncertainty of the opportunity may change quite quickly. For example, a new country may become available to do business in due to a change in sanctions policy. This may cause a review to take place to identify the areas that should be exploited and the factors that need to be in place to optimize the return.

Frequency

The schedule for monitoring risks will vary depending upon the nature of the risk and of the organization. For some organizations an annual review process may suffice but in others operating in a fast-paced environment and subject to more rapid alterations of environment this may be much more frequent. In project management, for example, the project may require a weekly re-evaluation of the risk register to take account of the work and findings from the previous week.

Whichever frequency is decided upon, it is important to have the time scheduled for all interested parties to be aware of the timing and to contribute to the review.

Process

When actively monitoring risk, this should be undertaken using a defined process that is appropriate for the organization concerned. This could be a formal review process requiring discussion papers to be prepared before risk committee meetings, or it may involve less formal, but still documented meetings.

Whichever type of review is undertaken, the process will usually involve two stages:

1 Categorizing which risks require review and at what interval.

Not all risks should be reviewed monthly, as their ability to change will be limited and the benefit of undertaking such action would be negligible and waste the time of those providing input. For example, the risk of product substitution or competitor action may occur less frequently and be subject to annual review. Conversely, some risks will already be under constant and continuous review; for example, risks of cyber attack will probably be monitored by means of automated processes taking feeds from external sources, or an outsourced protection supplier may be involved.

Included in the categorization process should be an awareness of how any change to the likelihood or magnitude of the risk may push it outside of acceptable limits.

2 Identifying and accessing all sources of information that may be appropriate for the review.

These will include those sources that contributed to the initial review, but in addition further input will be required to assess any changes that have occurred since that review. These will be both internal and external to the organization:

- Internal sources of information: This will include those individuals and units that contributed initially but will also now include reference to reports that will be available as part of the general organizational management information such as sales, revenue, customer retention, cost of goods sold and similar performance metrics. These will have a bearing on how the risk has changed since it was previously considered. These metrics are, however, of a historical nature and may need to be supplemented with indicators that are more forward-looking. Due consideration should be given to various trend analyses from these indicators to enable some element of future-looking.
- Key risk indicators should be reviewed here (for more detail on KRIs see Chapter 22).
- Internal audit reports should also be sought to assist in the risk monitoring process, since they will be evaluating whether business units are taking the agreed-upon actions.
- External sources of information: It is critical to this process that the monitoring process looks outside the organization to establish the up-to-date position with the risk concerned. This is necessary to ensure that ‘groupthink’, where assumptions are unchallenged, does not arise. Such external sources of information will be readily available and can include:
 - news aggregators such as Google News;
 - data mining, which may be readily available from external sources such as third-party suppliers, consultants, brokers or trade associations;
 - sector publications and professional institutes’ websites.

Reporting

The reporting of regularly monitored risks will vary depending upon the urgency and importance of the findings. Clearly, any review which establishes that risks have changed to become outside of the agreed risk appetite will be escalated to the level of management, or, if appropriate, a non-executive director, who need to consider the actions required to bring such a risk back to within acceptable parameters at the

earliest possible juncture. More regular findings will probably form part of a management information pack that provides regular updates to enable the management of the organization.

Such regular reports may involve a simple dashboard or similar report showing changes to the risks, or alterations to mitigation plans and profile which had been seen previously. It will be important not to overload management with reports that may be immaterial, in that risks have changed insignificantly. Ultimately, this will weaken the position of the risk management function in the eyes of senior management in that the ERM function may appear to be overly bureaucratic.

It may also be possible to automate risk reporting on a more continuous basis using technology, especially if the organization uses digital processes in its ordinary course of working. For example, there is software available that takes input from those operating in the organization and aggregates the information automatically. The data that is produced is then capable of being interrogated to produce more up-to-date output. In similar fashion, there is dedicated software available and used by many construction and industrial companies to monitor and manage risk on site, which enables workers to conduct risk audits using mobile phones and tablets, with that information being fed into the risk register and safety database in real time.

Responsibility

If the organization has an ERM function this will be responsible for facilitating the review. It is likely, however, that under each risk a risk owner will have been appointed and this person should have initial responsibility for undertaking the review. At some point, a collaborative review will be required. This will be required to consider where risks cross over more than one business unit and also due to the need to consider external sources of information in order to challenge established assumptions held within the organization.

Insurance and risk transfer 18

History of insurance

Insurance has a very long history that can be traced back to Chinese and Babylonian traders. It became formalized in the shipping industry, where marine insurance can be traced to the mid-1300s in Europe. In the 1680s, a coffee shop (Lloyd's) opened in London, which became the meeting place for parties wishing to insure cargoes and ships.

Insurance developed rapidly during the 18th and 19th centuries to provide financial protection for property. In the United States the development was often spurred by major disasters, typically large fires that laid waste to cities through spreading in closely confined neighbourhoods. This happened in New York in 1835, and Chicago in 1871. Insurers developed codes to assess risk and worked with cities to introduce building standards.

Some insurance arrangements were also associated with protection for dependants following the death of the money-earning member of the household. These arrangements became more formalized with the establishment of friendly or benefit societies during the 19th century.

In the 1900s insurance expanded into providing financial protection from theft and accidental damage together with providing financial protection for the liabilities an organization might incur whilst driving automobiles. This was extended by government regulation to workmen's compensation acts in many jurisdictions also around that time.

Transferring the financial consequences of risk

Risk transfer is one of the main risk responses available in relation to hazard risks. This transfer normally takes place by way of insurance and it is often described as risk financing. The fundamental principle of insurance is that the insurance company will pay for loss that might be suffered in defined circumstances. The amount the insurance company will pay is intended to 'indemnify' or to put the organization back into the financial position it was in before the loss.

Insurance operates in three broad areas:

- It pays for damage suffered to the organization's assets: first-party insurance.
- It pays compensation to others for something the organization is alleged to have caused: third-party insurance.
- It provides financial protection to employees, including to directors: benefits insurance.

Insurance is a risk transfer or risk sharing response. It represents an after-the-event cost containment response to a risk. Insurance is most important for low-probability/high-impact risks, such as destruction of assets or the payment of liability costs in circumstances where liability insurance is legally required or catastrophic losses are possible. As well as repairing assets, insurance is available for the cost of implementing disaster recovery plans and the business continuity plans. Insurance can also be purchased to cover the increased cost of operation, as illustrated in Figure 18.1.

There are advantages and disadvantages associated with the use of insurance as a risk transfer mechanism. These are illustrated in Table 18.1

Insurance contracts are governed in the UK by the Insurance Act 2015 and require the organization purchasing the insurance to make a 'fair presentation of the risk'. This means that the insured party is required to disclose all information relevant to the insurance contract. If this information has not been disclosed, the insurance company or underwriter has the right to refuse to continue to provide insurance cover and may refuse to pay any claims that have arisen. In some jurisdictions this is still called a duty of 'utmost good faith' or *uberrima fides*.

Table 18.1 Advantages and disadvantages of insurance

Advantages	Disadvantages
Provides indemnity against an expected loss	Delays are often experienced in settling an insurance claim
Reduces financial uncertainty regarding hazard events that may occur	Difficulties can arise in quantifying the financial costs associated with the loss
Economic benefit if the loss is greater than the insurance premium	Disputes regarding the extent of the cover and the exact terms and conditions of the insurance contract
Provides access to specialist services as part of the insurance premium. These services may include advice on loss control	Difficulty in determining the amount of insurance to purchase may result in under-insurance and failure to have claims paid in full

Organizations may decide to retain a certain amount of the financial impact associated with the losses. Risk retention may be achieved by accepting a large excess or deductible on an insurance policy, deciding not to insure a certain risk exposure (self-insurance).

There are alternatives to buying insurance from an insurance company that involve retaining larger amounts of risk in order to achieve greater efficiency in transferring the financial impact of a hazard event. These alternatives are sometimes referred to as alternative risk transfer (ART) or alternative risk financing techniques. These techniques include, for example, using a subsidiary company to insure the organization; this is called a captive insurance company.

Organizations with similar risk exposures may decide to ‘pool’ their risks in a jointly owned insurance company. This is often referred to as a mutual insurer. The oil industry provides some insurance to its members against the risks of pollution, for example in a company called the Offshore Pollution Liability Association (OPOL).

The risk financing options available to an organization include:

- conventional insurance;
- contractual transfer of risk;
- captive insurance companies;
- pooling of risks in mutual insurance companies;
- derivatives and other financial instruments;
- alternative risk finance mechanisms; and
- single premium insurance bonds.

Types of insurance cover

The different types of insurance cover that may be required by an organization are set out in Table 18.2. Generally speaking, the three reasons why an organization will wish to purchase insurance cover are met through the broad areas in which insurance operates (as shown above): These are:

- balance sheet/profit and loss protection (first-party protection);
- mandatory legal and contractual obligations (third-party protection);
- protection of employee assets (benefits insurance).

Table 18.2 provides more information on the different types of insurance that are available and the circumstances in which insurance should be purchased. In most cases, the purchase of insurance is not compulsory. However, most countries make the purchase of insurance compulsory for some liability classes, such as insurance

Table 18.2 Different types of insurance**Mandatory, legal and contractual obligations**

- Employers' liability – compensation to employees injured at work
- Public liability – compensation to public or customers
- Motor third party – compensation following motor accident
- Product liability – compensation for damage or injury
- Professional indemnity – compensation to client for negligent advice

Balance sheet/profit and loss protection

- Business premises – damage to premises by adverse events
- Business interruption – loss of profit and increased cost of working
- Asset protection – losses, such as loss of cash, goods in transit, credit risk and fidelity guarantee (staff dishonesty)
- Motor accidental damage – repair of own vehicles
- Terrorism – compensation for damage caused by terrorism
- Loss of a key person – compensation on loss of key staff member

Employee benefit/protection of employee assets

- Life and health – benefits to employees that can include: life cover, critical illness cover, income protection, private medical costs, permanent health cover, personal accident and travel injury/losses
- Directors' and officers' liability – legal and compensation costs

cover to compensate injured employees and for the parties involved in road accidents. Professions often require their members to purchase professional indemnity insurance in order to carry on trading.

Apart from the compulsory classes, organizations can decide whether to purchase insurance. This decision will be based on the assessment of the risk and whether the nature and level of risk is within the hazard tolerance of the organization. The cost of insurance (premium) and the extent of insurance coverage are also important considerations when deciding whether to buy insurance. Typically, insurance is purchased for low-likelihood/high-magnitude risks, such as flooding, hurricane damage and major fires.

Evaluation of insurance needs

Table 18.3 provides a checklist for organizations to decide which types of insurance are required. There is a wide range of different types of insurance available and the specific activities and features of the organization will assist in deciding the scope of insurance that needs to be purchased. Sometimes, there is a shortage of insurance capacity and although the organization has decided that it wishes to purchase that type of insurance, it may not be available at an affordable cost.

Table 18.3 Identifying the necessary insurance

Feature of the business insurance requirement	Type of insurance
1 Business has employees	Employer's liability
2 Employees travel outside the country	Business travel
3 Members of the public could be affected	Public liability
4 Business supplies products or components	Product liability/recall
5 Business provides professional advice	Professional indemnity
6 Theft or dishonesty by employees could occur	Fidelity guarantee
7 Business occupies business premises	Premises
8 Premises has machinery or other stock	Contents
9 Business depends on machinery or computers	Engineering
10 Business could be disrupted by fire, flood, etc	Business interruption
11 Business is involved in transporting goods	Goods in transit
12 Business has motor vehicles on public roads	Motor
13 Business provides life benefits to employees	Life and health
14 Certain staff are key to operation of business	Key person
15 Business would suffer in event of a bad debt	Trade credit
16 Business has directors and/or officers (D&O)	D&O liability

There has been a tendency in recent times for organizations to look at the whole portfolio of risks they face. This enterprise risk management approach to risk has resulted in a careful review of how much insurance an organization wishes to purchase. For example, if there are significant risks within a project, but insurance is only available for limited risk exposures, purchase of insurance for only those limited risks may not be appropriate.

This enterprise approach to risk management has reduced the use of insurance as a risk control mechanism for some organizations. For example, bp stopped purchasing insurance other than for mandatory classes altogether in the 1990s on the basis that insurers were unable to provide the capacity they required and receiving payment of any meaningful claim would probably require litigation.

One of the features of the insurance market is that the cost of insurance varies significantly. The market will cycle between soft market conditions (low premium) and hard market conditions (high premium) over perhaps a 6–10-year period. When the premium rates are high, organizations will tend to buy less insurance and make greater use of a captive insurance company (as described below). When premium rates are low, organizations will purchase more insurance because the insurance becomes a more cost-effective control measure.

Purchase of insurance

When looking at the purchase of insurance cover, the organization will need to consider the 6Cs of insurance buying, as shown in Table 18.4.

Insurance companies receive premiums at the beginning of the policy, but do not have to pay claims until after the event or loss. This can often be years in advance, and delivers a positive cash-flow position for insurance companies with the associated opportunity to earn investment income.

This means there is a credit or counterparty risk. The insurer may suffer a downgrade of their financial status if they have to pay significant losses before paying the organization's claims. Economic conditions may mean its forecasts of low interest rates or the poor performance of stock markets do not provide the investment income it expected. Accordingly, buyers of insurance need to pay attention to the financial status or credit rating awarded to individual insurance companies when making decisions about which company to use.

The handling of insurance claims can be a detailed and forensic exercise. Sometimes claims handling involves complex legal procedures involving specialist engineers and accountants. Property damage claims may be easier to quantify, but

Table 18.4 The 6Cs of insurance buying

Issue	Consideration
Cost	This consists of the insurance premium and the cost of any self-insurance (including excess or deductible) that is imposed by the policy.
Coverage	Insurance policies have limitations, warranties and exclusions. These state the circumstances under which claims are paid. These coverage issues need to be explored in detail by the organization purchasing the insurance to ensure that adequate coverage is available. The history of the particular insurance company in relation to the payment of claims and the reputation of that insurance company will be important factors when deciding which insurance company to appoint.
Capacity	One insurance company on its own may not be able to offer coverage up to the full value of the assets of very large organizations. When buying insurance, the organization will need to think about the capacity that the insurance company is willing to offer in relation to the value of the assets/exposure that need to be insured.
Capabilities	Many insurance companies offer services in addition to insurance. These may include loss control services and assistance with business continuity planning. The capabilities of the insurance company in these areas may be an important factor in deciding which insurance company to choose.

(continued)

Table 18.4 (Continued)

Issue	Consideration
Claims	An increasingly important issue for buyers of insurance is the financial security, status and capabilities of the insurance company.
Compliance	This has two components. Firstly, the insurance contract should be agreed before the policy period commences. This is often referred to as being 'contract certain'. Secondly, in relation to international organizations, most countries have introduced insurance premium taxes which must be paid where an organization has assets. Additionally, some jurisdictions will only recognize insurance cover or payments from policies issued in that country.

claims associated with the business interruption element of the loss can be very difficult to measure and agree.

If an organization has devised adequate business continuity plans, the disruption to the business and the size of the insurance claim will be much reduced. In risk management terms, depending fully on insurance to make good all losses is not sufficient. Every organization should look to its business continuity plans to ensure that arrangements are in place to guarantee minimum disruption should an adverse event materialize.

Captive insurance companies

A captive insurance company is an insurance company owned by an organization that is not otherwise involved in insurance. The purpose of a captive insurance company is to provide insurance for the organization by using its internal financial resources to fund certain types of anticipated losses or insurance claims. The organization that owns a captive insurance company is often referred to as the parent of the captive, or simply the parent organization.

In general, captive insurance companies are domiciled in locations that have favourable regulatory and accounting regimes. Domiciles for captive insurance companies include Guernsey, the Isle of Man, Gibraltar, Malta, Luxembourg, Bermuda and Ireland. The nature of captive insurance companies can vary quite widely. In theory, such a company may write insurance business directly into other countries, although compliance issues may need to be carefully considered.

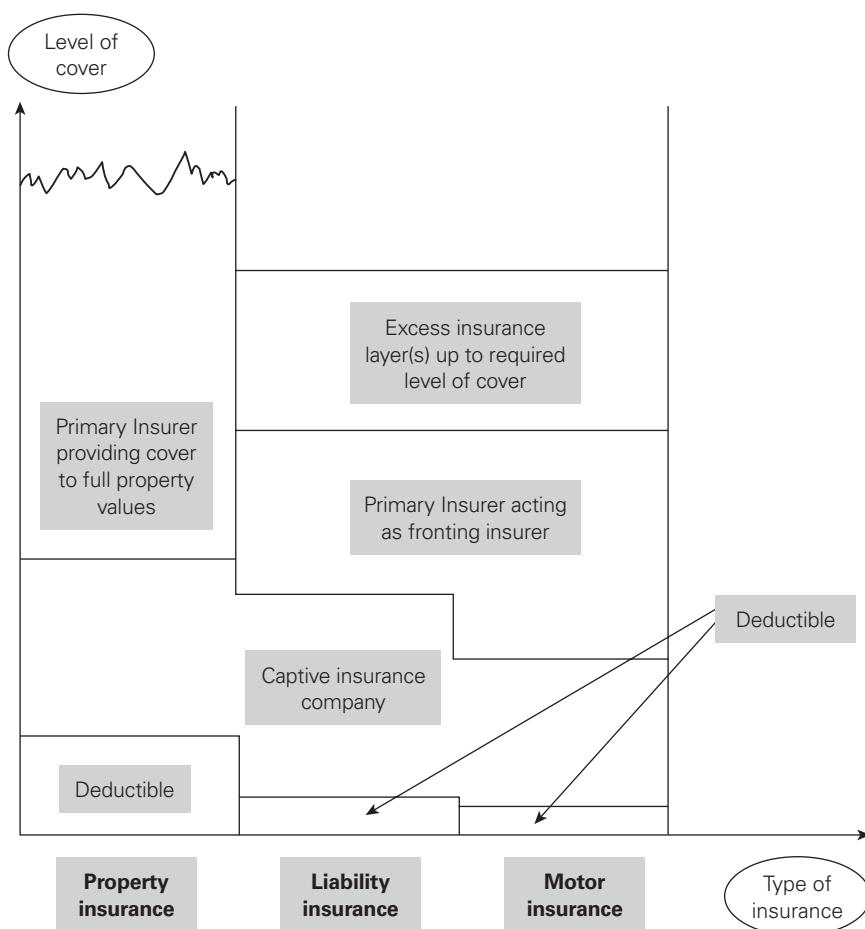
It is more common for a captive insurance company to operate as a re-insurer, providing insurance cover to the main insurance company appointed by the organization. This arrangement provides the insurance company of the organization, often referred to as the fronting insurer, with the means of receiving reimbursement for certain types of claims up to the financial limits or risk retention levels agreed with the captive insurance company.

A typical financial structure for a complex insurance programme is illustrated in Figure 18.1. The organization will accept deductibles or excesses on its different classes of insurance, and these may vary by class of insurance. The captive insurance company then accepts the next level of loss up to an agreed limit for any individual loss and also up to an agreed limit for total or cumulative losses during the policy year.

The primary or fronting insurer will then be responsible for payment of that part of larger losses that exceeds the captive insurance company limit. The fronting insurer will be responsible for payment of all losses once the cumulative totals for the captive have been breached. For statutory classes of insurance, the primary or fronting insurer will be responsible for the payment of the total claim.

The fronting insurer will then reclaim the money from the captive insurance company to the extent that the captive insurance company is liable. This can present a credit risk for the fronting insurance company, which in practice is overcome by the issue of some form of security, such as a letter of credit.

Figure 18.1 Role of captive insurance companies



Some captive insurance companies are set up to provide insurance to their customers. A typical example of this is extended warranty insurance offered by the retailers of electrical goods. The customer will purchase a policy issued by a well-known insurance company, but the funding of the insurance will be provided by the captive by way of re-insurance of the fronting insurer. By setting up this arrangement, the organization should earn extra income and profit from its customers.

The advantages of captive insurance companies are as follows:

- Savings may be achieved in overall insurance costs because they charge lower premiums than traditional insurance companies, which have a higher cost of administration.
- The captive insurance company can gain access to reinsurance markets, where premium rates and risk capacity can be favourable.
- By being exposed to the cost of insurance claims, a greater risk awareness and greater concern about loss control can be achieved.
- Greater insurance cover can be offered by the captive insurance company than is available in the commercial market.
- Certain tax benefits may be available from having a captive insurance company, although these have reduced in recent times.

The disadvantages of captive insurance companies are as follows:

- The captive will be exposed to insurance claims that would otherwise have been paid by the commercial insurance market.
- The parent organization has to allocate capital to ensure adequate solvency of the captive insurance company.
- When large losses are paid by the captive, these are consolidated to the parent balance sheet and the organization ultimately pays these losses.
- Captives writing business in other territories will probably do so on a non-admitted basis and this may create compliance difficulties.
- Significant administrative cost, time and effort can be involved in the management of the captive by parent head office personnel.

Surviving shocks and disruption

19 ERM, BCP and resilience

VUCA

The current environment is said to be volatile, uncertain, complex and ambiguous (VUCA). This is clearly evident in the health crisis of Covid-19. The unprecedented disruption to economies, health care systems, organizations and individuals has tested the ability of organizations to withstand sudden shock and revealed gaps in many plans to ensure continuity of business. Surveys of risk managers in 2020 predicted more disruption in the coming years in areas such as climate change, technology, and political shocks of new regulations.¹

This illustrates the importance of business continuity planning (BCP) as an integral part of risk management. In simple terms, BCP is how an organization prepares for future incidents that could disrupt operations and jeopardize its existence. The range of incidents that should be covered will include everything from local events like fires through to regional disorder and global events such as earthquakes, terrorism and pandemics.

British Standard BS 31100:2011 defines BCP as:

[An] holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability for an effective response to safeguard the interests of its key stakeholders, reputation, brand and value-creating activities.²

In case of a serious incident, such as loss of access to premises or the failure of a major part of an organization, it is important to have in place a well-defined, documented and tested disaster recovery plan. Such plans inevitably focus on recovery of access to IT systems and data, but also commonly cover the provision of alternative premises (if needed) and other facilities, as well as setting out plans for communication with employees and with other stakeholders such as suppliers, customers and the media at a time of crisis.

Business continuity plans build upon this by setting out longer-term plans for restoration of ‘business as usual’ in the immediate aftermath of a disaster. A business continuity plan is an important part of reducing the impact of a hazard incident. The

plan should include arrangements for reducing the damage caused during the incident and containing the cost of recovery from it.

Disaster recovery plans (DRP) are a particular component of BCP. If a computer system fails to operate correctly, or data has become corrupted, the organization will need emergency procedures to ensure that the data can be recovered and/or ensure that the organization continues in existence. There may also be a wider need for a specific plan to manage any crisis that may result from an operational disaster. The main difference between disaster recovery and crisis management plans is that a disaster recovery plan will be mainly concerned with actions to restore the infrastructure of the organization and a crisis plan will also be concerned with external stakeholders and actions to manage the associated stakeholder reaction and expectations.

For a printing firm, for example, the IT system is fundamental to the operation of the company, to process orders, schedule printing and manage invoicing. To protect the integrity of its information it will need to ensure back-up processes and will probably make use of cloud storage systems to ensure the availability of this business-critical detail.

Business continuity planning and resilience

There has been considerable discussion about the nature of business continuity and disaster recovery in terms of the types of control that they represent. HM Treasury in the UK considers these controls to be corrective, whereas the Scottish Government considers them to be directive. In terms of loss control, disaster recovery plans can be seen as primarily damage limitation controls, whereas business continuity controls are more concerned with cost containment. The important issue is that disaster recovery and business continuity plans are concerned with circumstances where the event is taking place or has occurred.

The broader term of ‘resilience’ has been coined to encompass the use of business continuity and disaster recovery but from a deeper and more embedded angle where senior management specifically build into their long-term strategy for the organization the ability to ensure long-term resistance to shocks. Resilience is discussed as a concept at the end of this chapter, but we turn firstly to BCP.

Business continuity planning

Many organizations see BCP as having three components:

- 1 The activation of the crisis management plan to contain the crisis and ensure the appropriate responses are taken whilst fully engaging stakeholders to avoid/reduce damage to reputation.

- 2 Implementation of recovery procedures whilst ensuring the ongoing management of the crisis.
- 3 Execution of the continuity plans to ensure operations continue as before (if possible).

Figure 19.1 Disaster recovery timeline and costs

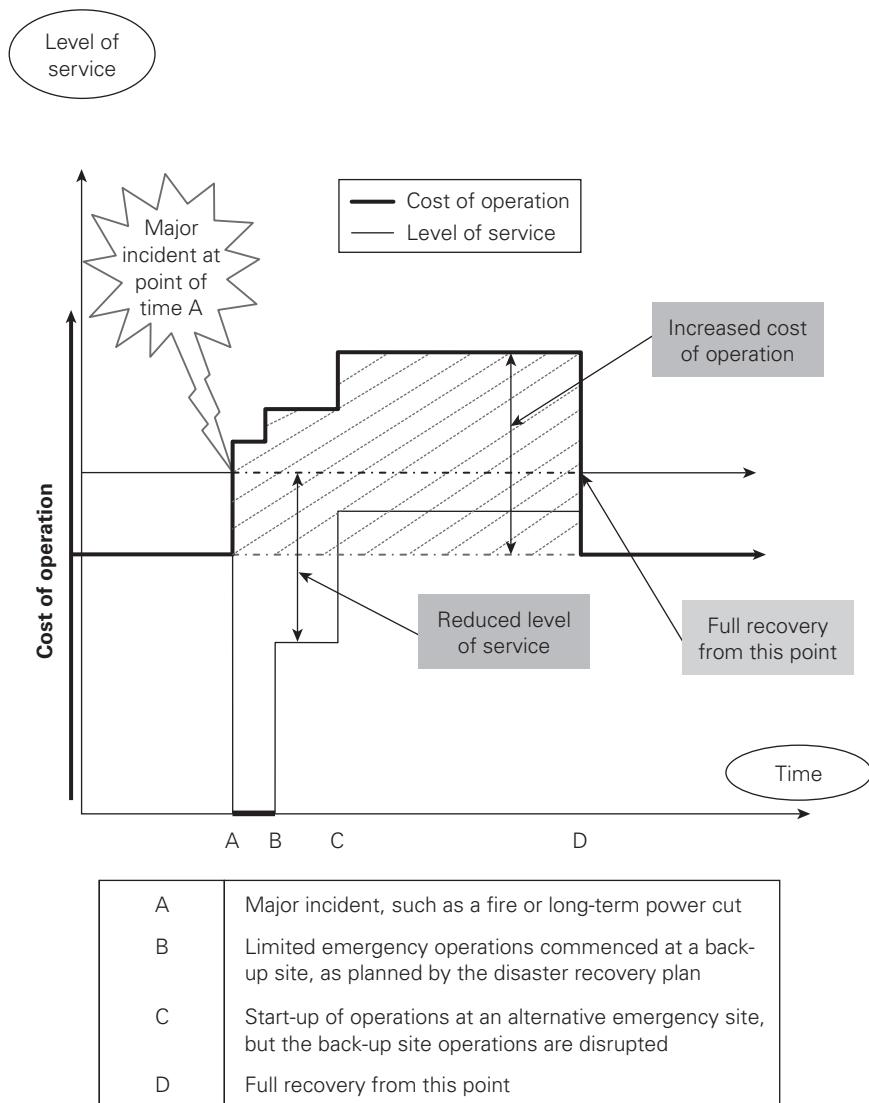


Figure 19.1 provides an illustration of a disaster recovery timeline and costs and this is discussed later in this chapter. The need to ensure adequate crisis management and effective communication with stakeholders covers the whole period of disruption (from point A to point D) and possibly beyond.

Business continuity standards

The international standard for BCP is *ISO 22301:2012 Societal Security – Business Continuity Management Systems: Requirements*. It describes a plan–do–check–act (PDCA) approach that is similar to the plan, implement, measure and learn (PIML) approach used throughout this book and described in detail in Chapter 7.

ISO 22301 identifies a BCP lifecycle that has the following five components related to the business continuity management system:

- Identify crucial risk factors already affecting the organization.
- Understand the needs and obligations of the organization.
- Establish, implement and maintain your business continuity management system.
- Measure the overall capability to manage disruptive incidents.
- Guarantee conformity with stated business continuity policy.

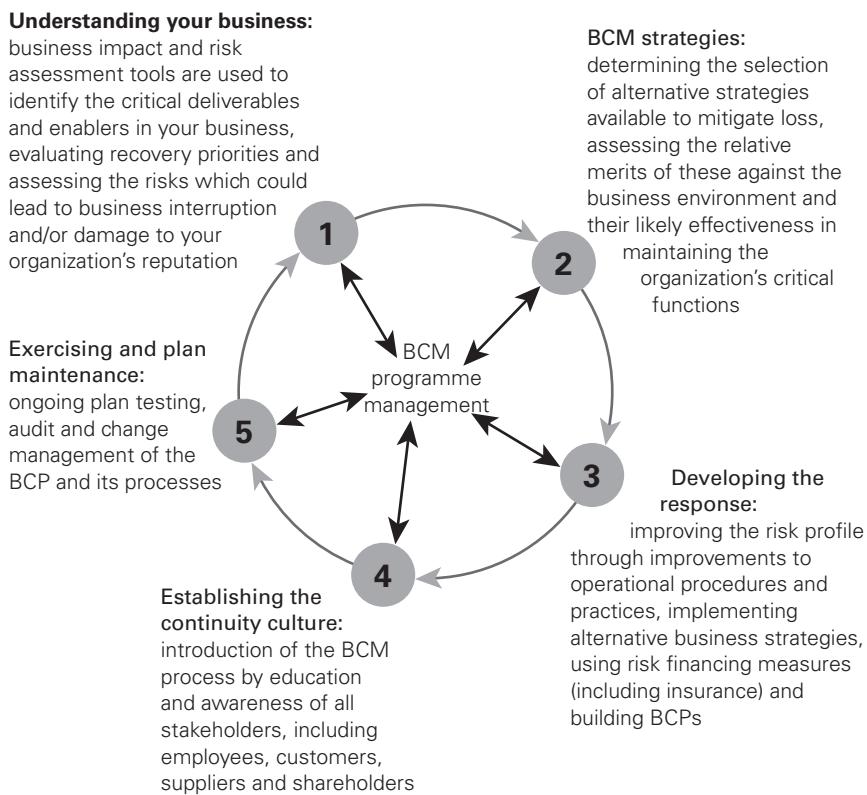
Figure 19.2 provides a model for BCP that is consistent with ISO 22301. Table 19.1 provides a checklist of the key activities involved in BCP. Having business continuity plans is recognized as essential by most large organizations. Indeed, many governments take an active role in encouraging businesses (especially small businesses) to develop and implement adequate business continuity plans.

ISO 22301 was the first standard to be written using the new high-level structure, which is common to all new management systems standards. This makes integration straightforward when implementing more than one management system. The phrase ‘preventive action’ has been replaced with ‘actions to address risks and opportunities’. ISO 22301 puts a much greater emphasis on setting objectives, monitoring performance and metrics – aligning business continuity to executive management strategic thinking.

The overriding principles appropriate to successful BCP are that the plan should be:

- comprehensive;
- cost-effective;
- practical;
- effective;
- maintained;
- practised.

Figure 19.2 Model for business continuity planning



It is important that the BCP should cover all the operations and premises of the organization to ensure that the plan can facilitate a complete resumption of normal business operations. It is also important that the plan is cost-effective and proportionate to the risk exposures.

The BCP must be practical and easily understood by staff and others who are involved in the execution of the plan. Overall, the BCP must be effective in that it will recognize the urgency of certain business components or functions and identify responsibilities for ensuring timely resumption of normal work.

In order to guarantee that the BCP will be effective, it needs to be tested, maintained and practised. All members of staff need to be familiar with the intended operation of the plan and training will need to be provided. The lessons learnt during testing and practice of the business continuity plan should be incorporated into the plan so that it becomes more effective. The need for rehearsals is emphasized in Figure 19.2 and Table 19.1.

Testing of business continuity plans is an essential component of ensuring that they will be appropriate and effective. However, testing of plans can be time-consuming and, in some circumstances, disruptive and costly. Even the simple

Table 19.1 Key activities in business continuity planning

- 1 Assess company activities to identify critical staff, materials, procedures and equipment required to keep the business operating.
- 2 Identify suppliers, shippers, resources and other businesses that are contacted on a daily basis.
- 3 Plan what to do if any important buildings, plant or store were to become inaccessible.
- 4 Identify necessary actions to ensure continuity of critical business functions, especially payroll.
- 5 Decide who should participate in compiling and subsequently testing the emergency plans.
- 6 Define crisis management procedures and individual responsibilities for disaster recovery activities.
- 7 Co-ordinate with others, including neighbours, utility suppliers, suppliers, shippers and key customers.
- 8 Review the emergency plans annually and when the business changes and/or new members of staff are recruited.

example of a fire evacuation drill from a building illustrates that the testing of procedures is inevitably going to disrupt normal routine operations.

Successful business continuity

The first stage in successful BCP, DRP and crisis management is to gain a thorough understanding of the organization and its interactions, both internal and external. Part of gaining this understanding will be to identify the objectives of the organization and its key dependencies. It is important to understand the critical functions within the organization and identify key resources.

Determining BCP strategy will require the identification of risks to the business and decisions about how likely it is that the risks will materialize. It is also necessary to understand the impact of risks on the business. These assessments should then be used to prioritize treatment of the risks and to agree the likelihood and impact of the risks materializing.

Developing and implementing a BCP and appropriate controls for each of the identified risks will require decisions on the appropriate risk responses. The range of risk responses available have already been discussed as the 4Ts of hazard risk

management. In respect of each of the major risks, the decision will have to be taken whether to tolerate, treat, transfer or terminate the risk.

Building and embedding a business continuity management culture will require good communication throughout the organization. All stakeholders will need to be engaged and involved in the business continuity activities and will need to understand the reasons for the development of the BCP and DRP. The important role of all employees in the avoidance of incidents that could result in major disruption should be emphasized.

When developing the BCP, the mission-critical activities should be identified, together with key roles and responsibilities. These may be produced in the form of clear instructions and checklists. It is important to exercise, maintain and review the BCP by creating a programme to test the plans, review and amend them as necessary, and rehearse staff to improve understanding of the plans. BCP and DRP should be reviewed at least annually, as well as after a test of the plans. Also, if an incident occurs, the lessons learnt should be incorporated into the plans.

Figure 19.1 provides a practical example of DRP and BCP. This example is based on a broadcasting organization that suffers a major disruption at its main broadcasting facility at point A on the timeline. The disaster recovery plan will ensure that broadcasting resumes within a short space of time, but this may only be an emergency broadcast. The emergency broadcast starts from point B on the timeline. Note Figure 19.1 does not include the cost of repairing or restoring the facility that has been damaged.

After a short period of emergency broadcasts, the organization will be able to commence full broadcasting of its normal service from an alternative location. For example, the broadcaster may move the London broadcast facilities to studios in Manchester. In order to do this, however, the Manchester capability will be lost. Therefore, Figure 19.1 shows that the level of service is much improved at point C, which is the move to Manchester, but because the Manchester broadcast facility has been lost, the level of service is not up to the previous level.

There will be an increased cost of operation from the time of the incident. There will be a cost associated with implementing the disaster recovery plan and further costs associated with emergency broadcasting and then the move to Manchester. During the period of broadcasting from Manchester, increased costs will be involved by way of temporary accommodation for staff and increased technical facilities. Eventually, from point D on the timeline, the facilities in London have been repaired and full recovery has been achieved.

Figure 19.1 represents a typical set of circumstances for an organization that suffers a major incident. The impaired level of service will continue for some time and increased cost of operation will be involved. Insurance may be available for the increased cost of operation, provided that it does not exceed the indemnity period (duration of the disruption) quoted in the insurance policy. It is unlikely that

insurance cover will be available to cover any losses associated with a reduced level of service from the time the incident occurs until the point of full recovery, unless specific types of costs or losses are identified and insured.

Business impact analysis

A critical part of ensuring that adequate business continuity plans and disaster recovery plans are in place is completion of a business impact analysis (BIA). The BIA will identify the critical nature of each business function by assessment of the impact of interruption to that activity. This information will be required in order to identify appropriate continuity strategies for each function.

The BIA is similar to the risk assessment that is undertaken as part of the overall risk management process. However, the critical difference from BCP is that the emphasis of a BIA is the identification of the relative importance and criticality of each function, rather than identifying the events that could undermine that particular function.

Therefore, the risk assessment and the BIA are related and could well be undertaken together. The risk assessment will help in identifying the risks that might threaten the achievement of the business continuity objectives. For a television company, broadcasting continuity is the target and may even be a requirement imposed by the licensing authority. Both risk assessment and BIA require a structured and systematic approach.

The business impact analysis has three clear purposes, as follows:

- 1 Identify mission-critical activities and the required recovery time in the event of disruption. This identification activity will establish the timeframe within which the critical functions must be resumed after the disruptive event.
- 2 Establish the impact potential and the resource requirements for recovery within the agreed timescale. The business requirements for recovery of the critical function must be established.
- 3 Determine whether the likely impact is within the risk appetite of the organization as the basis for business continuity strategy. The technical requirements for recovery of the critical function also need to be established.

The business impact analysis could be based on the sources of disruption that are described as the 4Ps (people, premises, processes and products) in Table 2.2. Once the sources of disruption that face the operations of an organization are identified, undertaking a BIA will become simpler. The focus of a business impact analysis, however, is likely to be on processes within the organization and how these may be disrupted. This seems especially relevant as continuity of business processes safeguards the interests of key stakeholders, reputation, brand and value-creating activities.

Resilience, business continuity and ERM

Resilience as a concept evolved from information technology around the 1990s, expanding into business continuity in the mid-2000s. In the USA the International Consortium for Organizational Resilience was founded in 2006. The BSI issued its *Guidance on Organizational Resilience* in 2014. ISO created its standard 22316 in 2017 and the Bank of England published a discussion paper on operational resilience as a key feature for financial institutions' health in the UK in 2018.³ There is a clear trend here to ensure organizations are fit to withstand future shocks.

Resilience is a combination of proactive ERM processes and BCP focused on maintaining continuity of operations if faced with disruption. It goes beyond BCP by its focus on the long-term viability of the organization and so could be said to have two legs, operational and strategic, which are discrete but connected.

Business continuity is 'event oriented', ERM focuses on the enterprise as a whole, but they both have roots in being preventive. They have both proactive and reactive components. ERM processes determine when proactive or reactive resilience measures should be implemented through defining the significance of the risks. By applying risk assessment and evaluation techniques the organization should be able to prioritize actions within commonly understood concepts of risk appetite and tolerance.

To achieve resilience there needs to be a focus on the future and an understanding of how an organization might become vulnerable to future trends. This involves scenario planning, which is an important component of business continuity and has broader implications for the successful implementation of enterprise risk management. For financial institutions, scenario planning extends to evaluation of the balance sheet capital that would be required by the financial institution in the event of disturbances in the economy and is usually referred to as 'stress testing'.

Scenario planning needs to take account of the external and internal context of the organization, as well as the business impact analysis. It will require input from all parts of the organization. This can cause tension amongst competing elements or divisions and requires clear and robust governance structures to maintain focus and ensure the process pays off.

There is a strong relationship between scenario planning and crisis management. Disaster recovery planning and business continuity planning can take account of foreseeable incidents, but it is more difficult to foresee every crisis that might arise. Therefore, a useful aspect of scenario planning is that it anticipates highly unlikely circumstances and then challenges senior management to develop successful responses.

The lessons from scenario planning can then be used to take actions that will increase the resilience of the organization. The next box describes an approach to scenario planning supported by the Cabinet Office of the UK government, in relation to disruption of national infrastructure, such as the electricity supply network.

Reasonable worst-case scenarios

Event standards can be established to set a level of resilience against an extreme event so that the network or system should be able to continue to operate without widespread loss or disruption to the essential services. Describing reasonable worst-case scenarios for hazards will enable infrastructure owners and operators to identify and assess their resilience, and consider any gaps in resilience of an asset or network between the event and the actual or current design and service standards.

The ability and capability to manage and respond to events greater than these reasonable worst-case scenarios is dependent upon their generic organizational resilience. Alongside this, infrastructure owners should consider, in their business continuity plans, the speed with which they expect to be able to restore services in the event of supply being disrupted for whatever reason, including events that are not specifically itemized or which are more serious or extreme than those covered in the reasonable worst-case scenarios.

SOURCE Cabinet Office (2020) Guidance: National Resilience Standards for Local Resilience Forums (LRFs), www.gov.uk/government/publications/national-resilience-standards-for-local-resilience-forums-lrf

Civil emergencies

In many countries, there is an obligation placed on local government to ensure the continuity of local businesses in the event of a major civil emergency. The emergency may be triggered by a natural disaster such as flooding or an earthquake. Alternatively, it could be caused by terrorism, civil unrest or, as we have seen, by a pandemic. The ISO 22300 series of standards relate to societal resilience and the increasing importance of this series of standards is also considered in Chapter 9.

Many civil authorities publish guidance for businesses to assist them with their BCP. For example, the US government provides valuable information on its website. Also, several trade associations and small business associations offer practical guidance on BCP, including appropriate actions in the case of civil emergency.

Most local authorities have statutory responsibility for responding to civil emergencies. Factories and warehouses may have equipment and facilities that could be useful in the event of a civil emergency. Likewise, retail shops will have food and other goods that may be required for distribution as emergency supplies. The products that may be useful in a civil emergency will include food, bottled water, clothing and blankets. Also, schools and other civic buildings may be required as accommodation in the event of a civil emergency, such as the wide area floods that have become more frequent in several European countries.

Encouraging organizations to make arrangements to ensure business continuity will benefit local authorities in charge of civil emergencies, because there will be fewer problems and issues for them to take into account at the time of the emergency. The box below provides a summary of typical advice provided by a municipal authority to small businesses in the local area.

Secure your business

Thoroughly assessing the disasters that could threaten your firm will give you a clear idea of the business areas that are most important to secure. Usually, these will be the areas on which your business relies the most, and which are exposed to the greatest degree of risk. This is the most important part of your plan.

Clearly, your premises are fundamental to your business – so much so that you probably take them for granted. But you should consider the long-term impact that damage to or destruction of your premises would have on your business. The same applies to business-critical machinery, plant and equipment.

Embedding organizational resilience into governance mechanisms should ensure that the management of the risks to critical infrastructure posed by natural hazards, major accidents and other malicious damage is considered by the board. The needs of organizational resilience would thereby inform strategic investment and procurement decisions, risk management and discussions with supply chain partners. It would enable infrastructure owners and operators to improve their understanding of the resilience of their infrastructure, measure the success of the strategy at regular intervals, and make necessary amendments to secure delivery or to match changing organizational priorities.

Notes

- 1 IRM (2021) *Organisational Resilience: A risk manager's guide*, https://issuu.com/irmglobal/docs/organisational_resilience_-_a_risk_manager_s_guide (archived at <https://perma.cc/FN6L-KMA9>)
- 2 BSI (2011) *BS 31100:2011 Risk Management: Code of practice and guidance for the implementation of BS ISO 31000*, British Standards Institution, London.
- 3 BSI (2014) *BS 65000:2014 Guidance on Organizational Resilience*, British Standards Institution, London; ISO (2012) *ISO 22301:2012 Societal Security – Business Continuity Management Systems: Requirements*, www.iso.org/standard/50038.html (archived at <https://perma.cc/7YA3-6G6L>); Bank of England, PRA and FCA (2018) *Building the UK Financial Sector's Operational Resilience: Discussion paper*, www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf (archived at <https://perma.cc/QS5F-Y4CC>)

THIS PAGE IS INTENTIONALLY LEFT BLANK

PART FIVE

Organizational environment

LEARNING OUTCOMES

Having studied this section readers will be able to:

- Explain the importance of dynamic business models and the relationship with strategy, tactics, operations and compliance (STOC) activities.
- Outline the components and the importance of the business model and how this is supported by the resilience of the organization.
- Explain the importance of corporate social responsibility, including supply chain, ethical trading risks and the importance of reputation.
- Explain the key components of the risk architecture, strategy and protocols (RASP) for an organization and how these fit together.
- List the main sections of a typical risk management manual, describe the importance of each section and summarize the range of risk documentation and records.
- Explain the importance of the allocation of risk management responsibilities, including the governance responsibilities of non-executive directors.
- Produce practical examples of the control of selected hazard risks, including risks to finances, infrastructure, reputation and marketplace.
- Describe the process of learning from controls in order to ensure that controls are cost-effective and risk/reward decisions are appropriate.

Further reading

- ASIS International (2009) *Organizational Resilience: Security, preparedness and continuity management systems, ASIS SPC.1-2009. American National Standard*, www.ndsu.edu/fileadmin/emgt/ASIS_SPC.1-2009_Item_No._1842.pdf
- FRC (2014) *Guidance on Risk Management and Internal Control and Related Financial and Business Reporting*, www.frc.org.uk/getattachment/d672c107-b1fb-4051-84b0-f5b83a1b93f6/Guidance-on-Risk-Management-Internal-Control-and-Related-Reporting.pdf
- Hopkin, P (2013) *Risk Management (Strategic Success)*, Kogan Page, London
- Institute of Risk Management (2010) *A Structured Approach to Enterprise Risk Management (ERM) and the Requirements of ISO 31000*, IRM, London
- Pullan, P and Murray-Webster, R (2011) *A Short Guide to Facilitating Risk Management*, Gower Publishing, Aldershot
- Task Force on Climate-related Financial Disclosures (2020) *2020 Status Report*, https://assets.bbhub.io/company/sites/60/2020/09/2020-TCFD_Status-Report.pdf
- Woods, M (2011) *Risk Management in Organizations: An integrated case study approach*, Routledge, Abingdon

CASE STUDIES

The student can review the following examples to illustrate further the areas discussed in Part Five and throughout this book.

Whitbread plc: Business model and ethics

This company owns and operates the Premier Inn group of budget hotels in the UK and Europe. They have been adversely affected by Covid-19 as both business travel and leisure tourism effectively ceased. The company has a 'force for good' ethos and they herald their contribution to the various community stakeholders they serve. They have a clear outline of their business model and how that creates value, which is shown on page 16 of their annual report.

They have a section in their annual report on emerging risk and the Covid-19 response, and show a clear linkage between their strategic priorities, key risks, risk appetite for each risk and mitigation activities. Given the significant impact the pandemic has had on their business, the report is an interesting example of how companies deal with challenges to their operations. For example, their first risk is identified as that of:

longer-term decline in returns and cash flow, pressures on Whitbread's balance sheet, including the value of Whitbread's property assets, the revolving credit facility covenants tests, requiring us to extend existing waivers or arrange

alternative funding, and the pension covenant test requiring us to extend existing waivers or make whole the Pension funds secondary funding target deficit.

The report has a 'Section 172 statement' which refers to their stakeholder engagement activity and links to their 'force for good' initiative in its ethical stand.

*Edited extracts from: Whitbread plc (2020) Annual Report and Accounts 2020/21,
https://cdn.whitbread.co.uk/media/2021/05/05141427/23076_Whitbread_AR2020_web.pdf*

East African Breweries Limited: Whistleblowing

This company is part of the Diageo group of companies and reports its activities locally in Kenya. Their risk management processes are in line with their parent, a globally recognized drinks manufacturer, and they annually:

undertake a 'blue sky' risk assessment. Thereafter, the top internal and external risks are ranked based on their likelihood of occurrence and their impact to the business. Action owners are then tasked with ensuring that robust risk-mitigation plans are in place. These risks are reviewed every quarter by business units at the Risk Management Committee (RMC). The general managers of our respective businesses in Kenya, Uganda and Tanzania each chair the RMC in their business.

Interestingly, this company shows its commitment to compliance and ethics by making a separate report about its 'Speak Up' facility and makes a feature of the 5 per cent increase in cases reported year on year, resulting in nine employee dismissals for breaches of their compliance code. Presumably this monitoring and reporting will continue in order to reduce and act as a control against internal fraud.

Edited extracts from: East African Breweries Limited (2020) Shifting Gears for Growth: 2020 integrated report and financial statements, www.eabl.com/sites/default/files/eabl_2020_annual_report.pdf

Booz Allen Hamilton: Ethics and community response to Covid-19

Booz Allen is a global business consultancy which is US based and listed on the New York Stock Exchange. They work closely with the US government and military but also wider private companies. Their annual report itemizes their response to the pandemic and explains the \$100 million 'investment' made by the company in 'job security and benefits for Booz Allen's people and large grants to community service organizations'. They have a large section on their response to the pandemic and developing opportunities through telemedicine in the future.

As a company trading under SEC rules, their issued Form 10-K lists some of their risks as follows:

- relationship with US government;
- compliance with complex regulation;

- after effects of the pandemic;
- harm to their professional reputation;
- security breaches in the systems they develop;
- compliance issues around the use of personal data in the business;
- risks relating to attracting talent, retaining employees and developing leadership.

Edited extracts from: Booz Allen Hamilton (2020) Fiscal Year 2020 Annual Report, <https://boozallen.gcs-web.com/static-files/49da105f-c53b-4caa-8b45-7f7ca7bfdea1>

Business and the risk environment 20

Dynamic business models

In this chapter we will look at the processes that underpin an organization. For simplicity we will review businesses that seek to make a profit or surplus, but the processes can equally be used for a not-for-profit organization such as a public or health service provider. In each case there will be a ‘business’ model (or a delivery model) to which risks will attach.

Organizations have both business and strategic objectives. Often these are documented separately and the risk management process undertaken will need to view both of these sets of objectives and explore the relationship between them. Business objectives will often relate to the annual budget of the organization and comprise details of the anticipated sales as income and the cost of sales as expenditure.

Underpinning the business objectives of the organization will be the business delivery model (or business model for short) that the organization has developed. For example, a membership organization will seek sponsorship from organizations that deliver services to the membership. This source of sponsorship income will be a fundamental part of the business model and the annual business objectives. The membership body will need to estimate income from membership subscriptions and from sponsorship, and determine what services will be delivered to the members in return for their membership fee, and what benefits will be delivered to the sponsors in return for their sponsorship money.

The risks that are attached to business objectives are associated with the robustness of the business model and the efficiency of the business model. When undertaking a risk assessment of the annual budget, the events that could undermine sponsorship and membership income, together with the events that could disrupt the delivery of services and benefits, should be considered. The essence of the business objectives normally relates to the organization as it currently exists.

Figure 20.1 identifies the essential features of a business development model. The business model is underpinned by the business objectives and the annual business plan. The organization will also have plans to develop and enhance the business model in line with long-term strategy. Figure 20.1 describes how the existing business

model is developed by implementing the tactics that achieve that long-term strategy. The existing business model is defined by the existing operations or ‘where the organization is now’.

Business delivery and development models

Whenever a business is established, it either explicitly or implicitly employs a particular business delivery model that describes the architecture of the value creation, delivery and capture mechanisms employed by the business enterprise. The essence of a business delivery model is that it defines the manner by which the business delivers value to customers, entices customers to pay for value, and converts those payments to profit: it thus reflects the belief of the organization about what customers want, how they want it, and how the enterprise can organize to best meet those needs, get paid for doing so, and make a profit.

The business delivery model is used to describe and classify businesses, but is also used by management inside companies to explore possibilities for future development. Future enhancement of the business delivery model is achieved by implementation of a business development plan. In fact, a well-established business delivery model will act as the basis for creative organizations to develop future strategy.

Most organizations recognize that changes in the external environment mean that ‘current’ business models will not always be successful. If business objectives are to be sustainable in the long term, then the business will need to develop. In our example of a membership organization these developments could include exploring wider sponsorship opportunities, delivering new services and products to generate new income, and increasing efficiency in the delivery of the existing business model. Development of the business model to fulfil strategic objectives can be considered to be the business development model and it is the main topic of this chapter.

In order to place risk management within the context of business operations, it is necessary to consider a simplified business development model. Figure 20.1 sets out the elements of a business development model in simple terms. The first stage for an organization is to decide the strategy that it is seeking to deliver. The strategic aims will be determined by considering the mission statement of the organization, the corporate objectives and the stakeholder expectations. The strategy should be capable of delivering the mission statement of the organization.

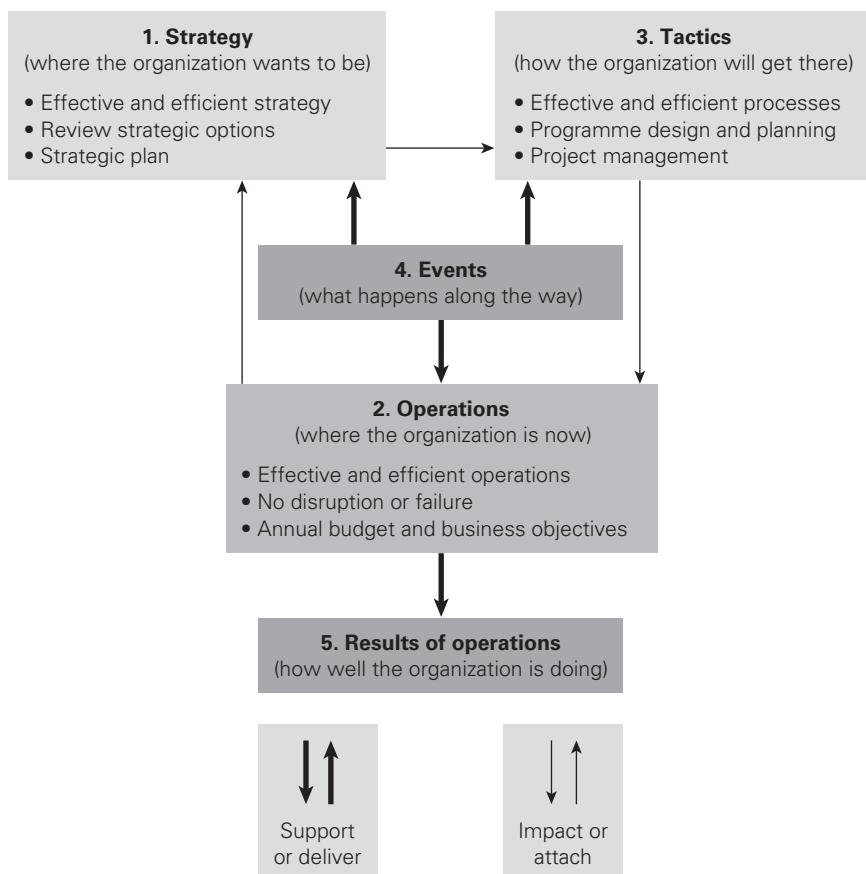
Once the overall strategy is established, the tactics that will deliver it need to be identified. If the strategy requires changes to core processes or the introduction of new core processes, then projects or programmes of work will be required. The

tactics introduced by the organization should ensure that effective and efficient core processes to deliver the desired outcomes in the most cost-effective manner are in place. In relation to operations, the desired state of the organization is the continuity of normal efficient operations with no unplanned disruption.

Figure 20.1 sets out the stages that are described above. The strategy can be seen as 'where the organization wants to be'. Review of the operations of the organization will collect information on 'where the organization is now' and the tactics define 'how the organization will get there'. This is a three-stage approach to development of the business model that has events at its centre. In many circumstances, these events will represent risks that could materialize. The other component of this business development model is the reporting of the results of operations.

Actions and events can be good, bad or routine, and enable the organization to monitor what progress is being made against the business strategy, tactics, operations and compliance. These actions and events impact the organization and its

Figure 20.1 Business development model



ability to sustain effective, efficient and compliant business operations and core processes. Although compliance core processes are not specifically mentioned, they represent the means by which the organization will ensure that it fulfils its legal, regulatory and contractual obligations. Compliant core processes should underpin all the activities of the organization and will be similar in nature to operational core processes.

Identification of strategy will require an approach based on opportunity management. Delivery of tactics, often by way of projects, will require attention to uncertainties and management of controls will be important. Delivery of effective and efficient operations will require particular attention to the successful management of hazard risks.

Types of business processes

An organization will have existing business processes and these may be satisfactory for generating the required income and controlling costs so that the business objectives are delivered. To ensure that risk management has an adequate input into the delivery of business objectives, the objectives must relate to routine operations within the organization. However, it is not unusual for organizations to fail to establish business-as-usual objectives. Most objectives tend to be annualized change objectives that relate to the delivery of the strategic plan for the organization. In summary, for risk management to make a full contribution to the success of an organization, objectives need to be fully established that cover strategy, tactics and operations.

A core process is one that is fundamental to the continued success (or even existence) of the organization. Core processes ensure that the organization is able to achieve the mission and corporate objectives and fulfil stakeholder expectations. Each core process creates value and is designed to deliver one or more of the stakeholder expectations.

There are four basic types of core process. These are processes designed, implemented and managed to ensure the following:

- development and delivery of strategy;
- management of tactics, projects and enhancements;
- continuity and monitoring of routine operations;
- activities that are designed to ensure compliance.

An activity is an individual job or task that builds into the processes that deliver stakeholder expectations. The processes themselves are designed and intended to add value to the organization, but the addition of extra activities will add cost. Therefore, the challenge is to develop effective core processes that are also efficient.

Having identified stakeholder expectations, core processes can then be put in place to ensure that these expectations are delivered to the level that the organization has decided is appropriate. No organization will be in a position to fully deliver all expectations to the level desired by all stakeholders. Often, this is because different stakeholder expectations are contradictory.

Weaknesses or gaps in the core processes of the organization are likely to be present, as follows:

- There may be weaknesses related to the development and delivery of strategy. These weaknesses will result in the organization failing to retain its position as a market leader. They give rise to a leadership gap.
- There may be weaknesses related to the management of tactics, including projects and product or service enhancements. These weaknesses will result in failure to keep up with competitors. They give rise to a competition gap.
- There may be weaknesses related to failure to ensure efficiency, continuity and monitoring of routine operations. These weaknesses will result in failure to maintain efficient operations. They give rise to an efficiency gap.
- There may be weaknesses related to the activities designed to fulfil mandatory requirements placed on the organization. These weaknesses will result in failure to maintain reputation. They give rise to a compliance gap.

Strategy and tactics

Business strategy is the statement of what the organization intends to achieve and how it plans to achieve it, and is based on the decisions about the future of the organization. Establishing a detailed business strategy enables the organization to deliver its mission, objectives, strategy and plans. The overall objective of risk management input into strategy is to ensure effective and efficient strategy and strategic decisions that will deliver the desired outcomes.

The main risk management input into business strategy is likely to be risk assessment. This is a critical component for the formation of strategy. Risk assessment of the existing strategy and any proposed new strategy should be undertaken. If clear strategic options are present, then a risk assessment of each of the viable options should be undertaken individually.

Some organizations exist in a very competitive marketplace that is undergoing disruption due to technological change. These circumstances present significant risk requiring significant strategic decisions. Often, these decisions will relate to developments that challenge the way in which the organization delivers customer solutions. Technological change can require speculative investment decisions and these decisions establish the tactics that will be implemented. The investment decisions may be

speculative because the technology may be untested or because there are competing technologies available.

A risk assessment of strategic options needs to be undertaken, including an analysis of stakeholder expectations, existing customer requirements and existing staff skills, as well as a strengths, weaknesses, opportunities and threats (SWOT) analysis. The strategic options available to the company might include joint ventures, outsourcing the work, sub-contracting or investing in new technologies.

Detailed risk assessment of strategic options will ensure that the board has the best available information in order to make correct strategic decisions. Events or circumstances that could reduce (or enhance) the successful delivery of strategy should be identified during the risk assessment. The organization will then be able to decide the controls that should be put in place to optimize the likely impact if any of these circumstances materialize.

Often, strategic objectives will relate to the development of a business sector and the reputation of the organization within that sector. In this way, the enhancement of reputation and the development of individual brands become opportunity risks for the organization. The fundamental importance of brand and reputation is considered in more detail in Chapter 21.

Tactics are the means by which the organization will deliver the business strategy. Tactics need to be correctly selected, implemented and controlled to ensure the effectiveness and efficiency of operations. They should also deliver reliability of financial reporting and compliance with applicable laws and regulations. The intended outcome is effective, efficient and compliant core business processes.

Changes to core processes are delivered by projects, and the importance of risk management in projects is discussed in Chapter 31 of this book. When undertaking a project, the organization needs to be concerned about the risks within the project that could stop it being delivered on time, within budget and to specification. However, there is a further consideration related to projects and that is the effectiveness of enhancements to core processes that the project is designed to deliver. There is little benefit in having a project delivered on time, within budget and to specification if the required increase in core process effectiveness and/or efficiency is not achieved. For example, the installation of a new business software system may be undertaken by a successful project, but if the new software system is inadequate, or does not deliver all of the additional benefits anticipated, then the improvement in core business processes may not have been achieved.

The main risk management inputs into tactics and projects will be risk assessment, risk response enhancement and the review and monitoring activities. The purpose in undertaking a risk assessment of a project is to identify necessary controls. When these controls have been implemented, the effectiveness and efficiency of the

controls will need to be reviewed. Overall, the intention is to ensure that tactics and projects are themselves effective and efficient.

Effective tactics mean that the core processes are the correct ones for delivering what is required. Established core processes may be fully efficient, but that does not mean that they are the correct or most effective core processes that the organization could employ. In order to ensure that core processes are fully effective, change will be required by way of projects that will be designed to ensure that strategy is delivered.

Developing more effective core processes will be the way by which the organization ensures that it continues to satisfy customers, financiers and other stakeholders. In order to ensure that effective core processes are in place, the business model and business objectives may need to change.

Effective and efficient operations

The overall objective of risk management input into operations is to achieve operational efficiency that is protected from unplanned disruption. Disruption of operations is likely to be caused by a hazard risk materializing. The design of efficient operational core processes that are free from disruption will provide the organization with significant competitive advantage or place the organization in a better position to deliver value for money.

Risk management can have a major impact on the operations of an organization. All stages of the risk management process are relevant to the continuity of uninterrupted efficient core business processes. Risk recognition and rating (risk assessment), responding to significant risks, resourcing controls, reaction planning, reporting on risk and review and monitoring are all critical inputs. In summary, risk management input into operations needs to be comprehensive if operations are to be efficient and uninterrupted.

Internal audit also has an important role to play in the delivery of efficient operations. Internal auditors frequently refer to the added value they bring related to the evaluation of control activities, especially in relation to operations. Not only should the operations be effective and efficient, but the controls that are in place should also be appropriately designed, effective and efficient. Internal audit activities have a significant role to play in providing the appropriate risk assurance and providing confirmation of compliance, where relevant.

All organizations need effective and efficient operations. In difficult financial and economic circumstances, it is important that existing operations continue to be delivered as efficiently as possible. The efficiency of operations will determine whether the annual budget, which includes the annual business objectives, is delivered. Part of ensuring the success of the organization will be to improve the

efficiency of operations. Delivering more efficient operations can be undertaken by developing activities so that they require fewer resources, and this may involve cost-cutting.

There is no point in operations being efficient if those operations are based on the incorrect activities or core processes for the organization. For example, it may be possible to arrange a very efficient means of travelling to your destination by car, so that the activity of travelling by car is as efficient as possible. However, it may be that the journey would be more effective if it was undertaken by train. In most busy cities in the world, it is possible to hire a taxi and travel to your destination quite efficiently. However, the more effective way of travelling may be to use the underground or metro system, which is likely to prove to be quicker and less costly.

The business model is described in more detail in Chapter 21. It defines the customer offering delivered by the resources of the organization and underpinned by the resilience of the finances and the reputation of that organization (CORR). The business model, therefore, represents the current (or existing) activities and operational core processes of an organization. Strategy and tactics will be designed to enhance and improve the business model by improving the effectiveness and efficiency of operational core processes. It is important to note that the business model represents the current status of the operational core processes in an organization.

Ensuring compliance

The reasons for undertaking risk management activities are described as mandatory, assurance, decision making, and effective and efficient core processes (MADE2). Core processes are identified as strategy, tactics, operations and compliance (STOC). There is a clear link between the reasons for undertaking risk management and the effectiveness and efficiency of core processes.

Mandatory requirements are fulfilled by organizations because they are required by stakeholders. Stakeholders who can impose mandatory requirements include regulators, customers/clients and financiers. Mandatory requirements have to be fulfilled and this will be undertaken by the organization by ensuring that effective and efficient compliance core processes exist within the organization. Failure to comply with stakeholder requirements can have significant implications for most organizations. In the extreme, failure to comply with the mandatory requirements of a licence may result in that licence being withdrawn by the regulator, and that could jeopardize the existence of the organization.

In almost all cases, there will be a number of ways in which the mandatory requirements imposed by stakeholders can be fulfilled. Although compliance core

processes need to be effective and efficient, there will be risks involved, and risk management input will have a significant role to play in designing the compliance processes, protocols and procedures. This is an example of how risk management expertise and support can enable an organization to achieve compliance in a way that is not only effective, but also can be efficient to the extent that it becomes a competitive advantage.

The culture within many organizations will be highly compliant, with a strong desire to comply with the mandatory obligations placed on the organization. This is a positive attribute and underpins the ethos of the organization, but if compliance is not achieved in an effective and efficient manner, wasted resources and competitive disadvantage will result. Part of the role of risk management professionals is to facilitate the development of effective and efficient compliance core processes that achieve compliance in the most cost-effective manner.

For example, most organizations will have mandatory health and safety requirements placed on them by legislation and enforced by a regulator. Some organizations may complain about the statutory obligations that are placed on them, and seek to avoid compliance if they believe there will be no consequences, or they think that they can ‘get away with it’. An organization with a more sophisticated approach to risk management, as illustrated in Figure 3.2, will adopt the approach that achieving compliance with health and safety requirements will not only improve operational efficiency, but a good safety record could be a factor in securing new contracts and new clients.

Reporting performance

Operational reports indicate how well the strategy is being delivered. Data needs to be available on an ongoing basis, so that management can respond and modify the business core processes as necessary.

Operational reports also provide information that can be used to prepare reports to stakeholders on the performance of the organization. However, the organization needs to decide what will be reported and disclosed to stakeholders and the format that will be used for those reports. To ensure accurate reporting and disclosure, appropriate control activities need to be applied.

In the United States, the Sarbanes–Oxley Act of 2002 (SOX) sets out duties that are primarily concerned with the accuracy of financial reports to shareholders. The main risk management input into reporting of performance is the risk assessment of the reporting lines and the data-handling procedures. The SOX duties have increased the attention paid to the control of reporting procedures. Section 404 of SOX requires that financial reports and the financial reporting procedures are attested by external auditors to confirm that they are accurate.

Stakeholder needs: Section 172 reports

Since 1 January 2020, all large companies operating under the UK's Companies Act 2006 have to include a separate statement in their strategic report that explains how their directors have had regard to wider stakeholder needs. This means (larger) companies will have to report on how they identified key stakeholders and their processes for engaging with and understanding stakeholder issues.

The organization's 21 business model, visions and values

Components of the business model

All organizations will have a business model that represents how they deliver the customer offering. Organizations that are public sector, third sector or would otherwise consider themselves to be non-commercial will still have a means of delivering their vision and/or mission statement. The means of delivering the defined customer offering is the business model of the organization. In summary, customers receive the offering from the organization because it utilizes the resources that it has available. The customer offering is underpinned by the resilience of the organization and by arrangements to ensure that the organization remains sustainable.

Figure 21.1 illustrates the components of the business model as customer, offering, resources and resilience (CORR). Each of these components is described in more detail in Figure 21.1, and they can be summarized as follows:

- Customer includes analysis of customer segments, recruitment and retention, as well as how products or services will be delivered.
- Offering refers to the customer value proposition and the related benefits that are delivered to those customers.
- Resources include the data, capabilities and assets of the organization, as well as partnerships and networks.
- Resilience of the organization is reputational (based on ethos and culture) and financial (based on expenditure and revenue).

The importance of the business model is that it represents how the operational and compliance core processes work together to deliver the customer experience. It is important for organizations to understand the business model, so that they can undertake a SWOT analysis of the existing business model. A risk assessment of the existing business model will enable the organization to evaluate the efficiency of the existing arrangements and identify the events that could disrupt the efficient delivery

of the offering, as well as identifying opportunities for improving operational and compliance efficiency.

It is important to note that the business model represents the existing mechanisms for the delivery of the customer offering and provides a description of operational and compliance activities. Risk assessment of the existing business model will enable the organization to identify options for improvements to the customer offering and/or the business model. The identification of an updated business model will represent the strategic position that the organization wishes to achieve. Tactics for implementing that strategy will need to be devised, as identified in Figure 21.1.

Business models can be quite complex and have a large number of dependencies, including suppliers and outsourced facilities. The weaknesses and inefficiencies in the existing business model need to be identified and analysis of the business model represents an additional way of undertaking a risk assessment. The importance of resilience within the business model is considered in the next section. Other factors that are important in the business model are related to reputation and ethical trading. A particular consideration for many organizations is corporate social responsibility within the supply chain. Analysis of the business model will enable an organization to assess the supply chain and identify embedded risks, including ethical risks that could damage the reputation of the organization.

Figure 21.1 Components of the business model



Risk management and the business model

Each component of the business model can be subjected to a risk assessment. The business model represents how the organization fulfils its vision and mission statement, as well as its aims and objectives. Although the offering is at the heart of the business model, the starting point is often an assessment of the customer segment at which the offering will be targeted. Risks are associated with identifying and securing customers and providing customer service and support. Distribution routes and channels are very important in the provision of the customer offering.

The offering itself is important and is at the heart of the business model. It is important that the offering draws on available resources and capabilities to deliver the intended customer with a value position and related benefits. The nature and use of the resources and how they are structured represents a number of risks and these should be evaluated during the risk assessment of the business model. An important part of the business model is the resilience of the organization, together with its reputation. There are many alternative versions of the business model, but some fail to give sufficient profile to the reputation of the organization.

Culture and ethics, as well as the reputation of the organization, are considered later in this chapter. Reputation is often a feature of the sector within which the organization operates. Reputation is often considered to be the most important aspect of any organization. Reputation also has a sustainability component in that an organization will wish to sustain and/or enhance its reputation.

All business models have to be sustainable, and this is normally represented by financial sustainability of resources and the need to balance expenditure against revenue streams. Sustainability has a wider context and has grown to include environmental considerations. In order to contribute to climate change sustainability, there is scope to address the business model to make this contribution. The scope of the sustainability requirements of the organization and its business model will need to be included in the risk assessment. Assessment of the business model will focus on the hazards or operational risks, together with compliance risks. In order to achieve an effective and efficient business model, operational risks will need to be mitigated and compliance risks will need to be minimized.

Having identified the business model and undertaken a risk assessment, an organization will then need to decide whether the existing business model is sustainable. If it is considered that there is scope to improve the business model, a new or modified business model will need to be identified. Achieving this enhanced business model becomes the strategy of the organization. The means by which the business model is modified to achieve the strategy can be considered to be the tactics of the organization and these tactics will be implemented by way of projects and/or programmes of work that achieve the required changes.

Strategic risks associated with improving the business model will need to be embraced and the risks associated with implementing tactics will need to be managed. The overall approach of embracing strategic risks, managing tactical risks, mitigating operational risks and minimizing compliance risks is referred to in this book as EM3. A component of a successful business model is that it is successful in recruiting new customers and draws the customer into a deeper relationship with the organization, so that the relationship is sustained and becomes more secure. Enhancements to the business model, therefore, need to not only recruit additional customers, but also retain existing customers at a constantly increasing level of customer satisfaction.

Ethics and corporate governance

Figure 29.1 illustrates corporate social responsibility (CSR) as a part of the overall corporate governance requirements of an organization. All types of organizations should be aware that good corporate social responsibility standards can enhance reputation and build stakeholder value. Conversely, incidents, events and losses associated with poor standards of social responsibility can create bad publicity and destroy stakeholder value.

The importance of good standards of corporate social responsibility is widely recognized and achieving good standards can enhance the organization by:

- protecting and enhancing reputation, brand and trust;
- attracting, motivating and retaining talent;
- managing and mitigating risk;
- improving operational and cost efficiency;
- giving the business a licence to operate;
- developing new business opportunities;
- creating a more secure and prosperous operating environment.

There are a variety of definitions available for corporate social responsibility. It is generally accepted that CSR is a wide-ranging agenda that involves organizations looking at how to improve their social, environmental and local economic impact and their influence on society and human rights. The CSR agenda also extends to consideration of fair-trade issues and the elimination of corruption. Before corporate social responsibility became a widely used term, several organizations used to refer to social, ethical and environmental (SEE) concerns. The CSR agenda includes all of the issues previously included in the SEE agenda.

There is no doubt that CSR is an issue for large multinational companies as well as for small, locally based businesses and the public sector. Indeed, it is relevant to all

types of organizations, including charities. The European Commission definition of corporate social responsibility is as follows:

Corporate Social Responsibility is the concept that an enterprise is accountable for its impact on all relevant stakeholders. It is the continuing commitment by business to behave fairly and responsibly and contribute to economic development, while improving the quality of life of the workforce and their families, as well as of the local community and society at large.¹

CSR and risk management

The scope of issues covered by CSR is set out in Table 21.1. The range of topics extends from health and safety concerns to broader considerations related to employees, customers, suppliers, the community, the environment and products/services provided by the organization. Both the CSR and risk management agendas are very broad, and they have significant overlap.

Many of the issues listed in the table are risk-based subjects, including health and safety at work and environmental impact. However, management of these issues simply as risks will fail to fully address the CSR agenda. Nevertheless, this is a good starting point. Many risk assessment workshops consider corporate social responsibility and social, ethical and environmental considerations within the topics that are evaluated.

Table 21.1 Scope of issues covered by CSR

Area	Scope
Health and safety	Commitment to a programme of activities to achieve continuous improvement in health and safety performance
Employees	Aim to deliver a competitive and fair employment environment and the opportunity to develop and advance – subject to personal performance
Customers	Strive to provide high-quality service and products and good value for money in all dealings with customers
Environment	Reduce impact on the environment, including factors contributing to climate change, through a commitment of continual improvement
Suppliers	Work with suppliers to ensure that worker welfare/labour conditions and environmental practices meet recognized standards
Community	Aim to be a responsible corporate citizen through support for appropriate non-political and non-sectarian projects, organizations and charities
Products/services	Designed not to unintentionally or by design cause death, injury, ill-health or social disruption, hardship or detriment

When assessing the CSR agenda, risk managers should take the opportunity to bring risk management tools and techniques to a broader agenda. The risk management approach of risk assessment, identification of control measures and auditing of compliance is an approach that can be transferred to corporate social responsibility and, indeed, to the broader corporate governance agenda.

Most organizations consider CSR to be a reputational issue and see the component parts of CSR as hazard risks. Such organizations will consider that they need to reform their core processes and procedures in order to comply with these requirements. This may well be an accurate starting point for many organizations. However, as Figure 3.2 illustrates, what starts off as a hazard risk can develop into a control risk and eventually into an opportunity.

As with other areas of risk management, organizations should seek to develop their level of sophistication in relation to CSR. Having got to the stage of complying with the CSR obligations, organizations should then look at the opportunities that are available. For example, it is now commonplace for supermarkets to offer goods that have been procured on a ‘fair trade’ basis and gain additional sales from offering this range of products.

Corporate social responsibility is an area of concern where it is likely that public opinion will be ahead of the thinking within many organizations. CSR issues therefore represent a great opportunity for an organization to develop corporate social responsibility plans and actions that respond to public opinion. Treating the CSR agenda as a dynamic, proactive set of issues will enable the organization to gain reputational advantage.

Many organizations have stakeholders that they do not necessarily want. This is certainly the case for several energy companies. Exploration for oil, coal and minerals is carefully scrutinized by environmental pressure groups. Even if they are ‘unwanted stakeholders’, environmental pressure groups are valid stakeholders in these organizations and can bring a considerable influence to bear on their activities. Environmental pressure groups have demands that are firmly within the CSR agenda.

The list of issues in Table 21.1 provides an indication of the stakeholders who are likely to have an interest in the CSR agenda. Employees, customers, suppliers and the general community are the key groups that are stakeholders in the CSR agenda of an organization. For CSR issues associated with the environment, it is fair to say that everybody is a stakeholder in the behaviour of organizations when that behaviour impacts the environment.

An example of the impact that a pressure group can exert is demonstrated by the impact of the ‘Black Lives Matter’ movement on many global corporations following the death of George Floyd in the USA, on camera. Walmart, Disney, and Facebook pledged donations to organizations such as the National Association for the Advancement of Colored People or launched diversity initiatives. Many organizations

felt compelled to comment, from the financial community, such as Blackrock, the Investment giant and JP Morgan Chase, to the leisure sector where Lego ‘told online affiliates to remove links to 31 mainly police-themed products, as part of its own stand “against racism and inequality”’.²

Supply chain and ethical trading

Failure to ensure appropriate ethical behaviour is increasingly recognized as a major business risk. Social media and press reports describing bribery and other forms of dishonesty have serious consequences for corporate reputation and future profits. The ease of access to information on the internet can result in organizations being investigated and exposed for unethical trading and/or unfair treatment of suppliers. Similarly, the dissemination and rapid spread of reports that achieve ‘viral’ status can be alarming.

If the unethical behaviour extends into illegal activity, this can undermine the organization itself. Illegal behaviour and condoning actions that are outside the governance rules of the organization can have serious consequences. The perceived need to bribe officials in certain territories is both unethical and illegal.

Boohoo and allegations of modern-day slavery

In July 2020 Forbes reported that ‘fast fashion entrepreneur Mahmud Kamani has endured a week he’d rather forget’ following the value of his fashion empire being hit by allegations of labour exploitation. The share value of Boohoo fell by nearly 50 per cent from a high of \$5.24 (£4.15) in mid-June to a low of \$2.64 (£2.09), wiping more than \$300 million off the value of Kamani’s stake.³

This was the result of an investigation by the *Sunday Times* of London that found workers at a UK factory that supplies clothing to Boohoo were allegedly being paid far less than the national mandated minimum wage.

This failure of compliance with the modern day slavery laws had a significant impact on investors’ view of the organization and, apart from regulator activity, the investigation focused investors’ attention on the corporate governance of the company. The company acted swiftly to try to repair the damage to their reputation risk by recruiting a senior, highly respected retired judge (Sir Brian Leveson) in November 2020 to review and lead the change required to bring Boohoo into compliance with the law. In January 2021 Boohoo purchased the Debenhams’ website to further extend its offering.

There are several areas where unethical trading can result in damage to reputation, the loss of future profitability and a refusal on the part of the customers and suppliers to deal with the organization. These issues include:

- failure to comply with rules and regulations;
- trading with undesirable overseas governments;
- excessive payments to political parties;
- tax evasion or dubious tax arrangements;
- inappropriate criticism of competitors;
- false allegations against competitors;
- unethical alliances with competitors.

Another feature of the supply chain that may result in allegations of unethical trading relates to the sourcing of products produced in socially unacceptable working conditions. Also, the quality of products and failure to provide value for money can result in damage to reputation and may be associated with unethical trading. Goods that fall short of current safety standards can result in serious adverse publicity and damage to reputation.

When a sports club decides that it wants all merchandise for sale to fans to be ethically sourced, it needs to look at the controls that can be placed on the importer to ensure that it only obtains merchandise from ethically produced sources. The club could require the importer to produce a routine CSR report as part of the contract terms and conditions. This report will include the following information:

- details of the policy that the importer has on ethical behaviour of suppliers;
- confirmation of the contractual terms and conditions of manufacture;
- statement that manufacturers do not sub-contract work, unless authorized;
- details of staff training, accident/absence rates and pay/conditions;
- results of audits/physical inspection of manufacturing premises.

The club can then advertise to fans that all goods are ethically sourced and encourage other teams in the league to do the same. This will gain good publicity and promote the club as having high CSR awareness.

Positive reporting on corporate social responsibility issues can be a significant benefit for an organization. This will be especially true when the organization operates in an area where the public are suspicious. The public may not be sympathetic towards an organization, because of perception of the business sector and/or the organization itself. When an organization operates in a sector that does not have universal public support, there may be benefit in producing an ethics policy. The importance of the ethics policy will be reinforced if the organization also undertakes an ethics audit.

For example, a sector that does not have full public support is gaming and gambling. Organizations operating in this area try to enhance the reputation of the sector by working with competitors on social responsibility standards for problem gambling. An individual organization can then gain further benefit by being able to demonstrate that it exceeds the minimum standards established for the sector.

This will need to be authentic, however, as such action can often be targeted as being a 'sticking plaster' and the minimum required of a company. In effect, its actions can quickly be negated if subject to further scrutiny and media attack.

Gambling firms increase funding to tackle addiction

In the UK the gambling industry has been under pressure from government and other public bodies to act in ways that are shown to discourage addiction. The largest firms in the sector agreed to pay an increased levy on their profits from 0.1 per cent to 1.0 per cent by 2023. On the face of it this appears to be a significant gesture and one that will increase the funding and support to tackle addiction to around £60 million annually. The companies involved include Bet365, William Hill, Sky Bet, Ladbrokes Coral and Paddy Power Betfair.

However, the announcement was questioned in a TV interview when 'William Hill chief executive Philip Bowcock admitted to Sky's Ian King that the money would be less than the companies spend on advertising'.⁴

Many organizations now include comments on corporate social responsibility in their annual report and accounts, and some produce a separate CSR supplement. The production of a report on CSR activities enables the organization to gain advantage from the CSR agenda.

Where an organization has a positive story to tell about a CSR achievement, it will have taken its CSR agenda from the need to reform to the position where the organization can demonstrate that it does conform. The next stage in this developing sophistication is for the organization to demonstrate that adherence to a CSR agenda enables it to perform better and more successfully fulfil stakeholder expectations.

Reporting on corporate social responsibility

The annual report should:

- include information on social, ethical and environmental risks and opportunities that may significantly affect the company's short- and long-term value and how they might impact on the business;

- describe the company's policies and procedures for managing risks to short- and long-term value arising from social, ethical and environmental matters;
- include information about the extent to which the company has complied with its policies and procedures for managing social, ethical and environmental risks;
- describe the procedures for verification of social, ethical and environmental disclosures, which should be such as to achieve a reasonable level of credibility.

Importance of reputation

Reputation is fundamentally important to organizations and they should make sure that they understand the basis of their reputation. Reputation is based on the size, nature and complexity of an organization, but it is useful to put more structure into what makes a good reputation. It is necessary also to assess from where the organization's reputation is being viewed, as is discussed at the end of this chapter.

There have been many attempts to identify the components of reputation. Table 21.2 shows the components of reputation and these are also illustrated as a spidergram in Figure 21.2. The four main components of reputation (CASE) are as listed below:

- capabilities, including purpose and resources;
- activities, including processes and finances;
- standards, including services/products and support;
- ethics, including values and integrity.

The organization will offer a range of services and products and the standards of service and service delivery will be a critical component of reputation. Finally, the organization will have business ethics that demonstrate its integrity. Integrity will be demonstrated, to some extent, by the monitoring of performance in order to learn and achieve continuous improvement in performance.

The use of a chart, such as that shown in Figure 21.2, will enable the organization to map its overall reputation, within the context of the sector in which it operates. For each of the four segments, or eight attributes, an organization should be able to plot its current status in a ranking of 1 to 4, representing poor, adequate, good and excellent. It will then be possible for the organization to identify the sectors that represent the greatest threats to its reputation.

This chapter has considered the importance of reputation in general and used corporate social responsibility as an example of one of the main pillars of reputation. However, reputation is a broader issue than just business ethics. Indeed, customers

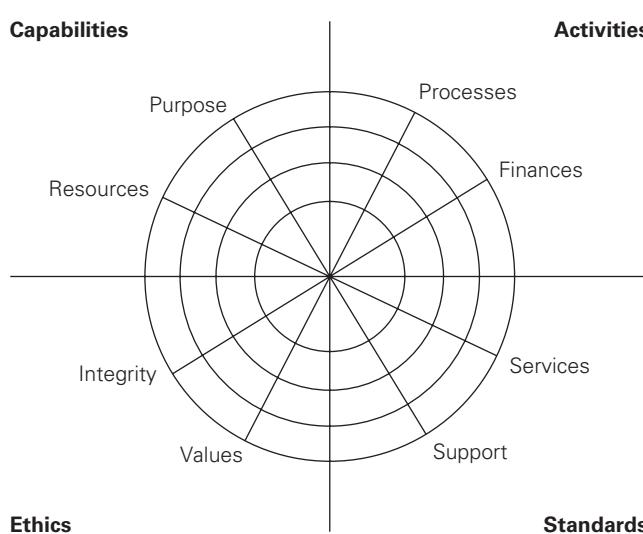
will often trade with an organization even though they do not believe it to have a particularly ethical business model. Although only a cursory insight and discussion of reputation has been included in this book, the overriding importance of reputation is fully acknowledged, especially in relation to risk management.

The importance of brand and reputation is recognized by all organizations. Several companies that deal directly with the public have sought to build a reputation based on trust and ethical behaviour. For many organizations, this is not a recent innovation, but is the ethos that underpins their customer offering.

Table 21.2 Components of reputation

Component	Comments
Capabilities	Does the organization have a clear purpose or resolve, together with the commitment, vision, capabilities and resources to deliver that purpose?
Activities	Which sector and what activities does the organization undertake, and does it have the financial resources and stability to support those activities?
Standards	What range of services or products does the organization offer, and what are the standards of quality, delivery, support, execution, innovation and investment?
Ethics	Does the organization adhere to appropriate CSR, integrity, values and governance, and continuously monitor performance to learn and achieve improvements?

Figure 21.2 Mapping the components of reputation



Different perceptions of reputation: Amazon

This traditional view of reputation can be enhanced by the use of technology to provide more nuance around the topic. In this case study technology has been used to identify various different groupings and their view of the reputation of Amazon.

Amazon is the third largest company globally by market capitalization, is feted as the 'most valuable brand' and regularly features in the top three most admired companies. Different reputation consultancies rank Amazon among the top one or two in their indices, while others, such as the Reputation Institute, indicate a decline in the firm's overall reputation.

It is becoming increasingly clear with the availability of sophisticated data analysis that 'multiple reputations' can be discerned amongst the various components of reputation. A study by Alva, a technology company analysing reputation and stakeholder perception, discerned from over 5,000 daily data points that:

- Customers consistently held strongly positive reputation scores for Amazon, driven by a mix of social media commentary, its prices, speed of delivery and ease of usage.
- Investors held more moderate and varied scores, reflective of daily shifts in share price but also residual concerns about its economic model and lack of dividends.
- Civil society was about neutral balancing of the benefits of employment against the poor view of low tax contributions.
- Employee perceptions were consistently low, as a result of perceptions of poor working conditions and pay disparity.
- Among government and regulators, Amazon held the worst reputation, with a growing hostility from this group

These findings are perhaps not unexpected, but the ability to quantify the sentiments portrayed enables the risks of damage as a result of worsening reputation to be monitored, and perhaps provides evidence to senior management of the value of trying to engineer a shift in the perception of the company. For more information see www.alva-group.com

Notes

- 1 EUR-Lex (2021) Corporate social responsibility (CSR), https://eur-lex.europa.eu/summary/glossary/corporate_social_responsibility.html (archived at <https://perma.cc/QP9E-Y2E7>)
- 2 McCulloch, A (2020) Global businesses embrace Black Lives Matter movement, Personnel Today, www.personneltoday.com/hr/global-businesses-embrace-black-lives-matter-movement/ (archived at <https://perma.cc/FBT9-FNGG>)

- 3 Dawkins, D (20020) Allegations of worker exploitation strike a blow to the fortune of Boohoo fashion line's founder, Forbes, www.forbes.com/sites/daviddawkins/2020/07/09/allegations-of-worker-exploitation-strike-a-blow-to-the-fortune-of-boohoo-fashion-lines-founder/?sh=700f446e6e18 (archived at <https://perma.cc/AMX4-EC7Q>)
- 4 Sky News (2019) Gambling firms agree more funding and support for addicts, <https://news.sky.com/story/gambling-firms-agree-more-funding-and-support-for-addiction-11754920> (archived at <https://perma.cc/DS2A-K9KX>)

How risk management adds value

Before discussing how risk management adds value, it is worth considering the evidence pointing to this conclusion. It is intuitively agreed that incorporating an ERM approach is of benefit; both regulators and credit agencies investigate and assess the ERM approach of individual companies. ISO, COSO and other bodies strongly support using a risk management approach that manages risk in an integrated fashion across the enterprise as a whole and not individual risks in isolation. It is, however, an approach that is still considered to be in its infancy in some sectors and which some on the boards of companies may fear involves excessive expenditure for limited gain.

What is the evidence?

Conclusively showing that companies using an ERM approach generate better financial and business outcomes than those without is challenging. The evidence appears to show that an ERM approach is beneficial across sectors and regardless of the development status of the economy in which the organization operates. In other words, ERM works in developed, developing and emerging economies.

These studies rely upon financial data as a ‘proof point’, and whilst this does not directly apply to not-for-profit or governmental agencies it might be argued that the beneficial effects in for-profit organizations reflect best practice management styles that can be transferred to other organizations. If ERM is beneficial in the commercial sector it is helping those companies to achieve their objectives. These companies appear to have a competitive advantage when compared with peers who do not use an ERM approach. Non-commercial entities might well look to this as a way of helping them to achieve their objectives in a better fashion too.

The challenge in proving a positive link between ERM and improved performance in the organization has always been how to categorize those organizations that operate using ERM and those that do not. Conclusive proof remains elusive, but the direction of travel is positive.

The challenge is compounded in developed economies where information on the value added to organizations has commercial value. Various consultants with risk management businesses such as Deloittes, McKinsey or Aon produce studies featuring examples of value added through the use of various techniques based on interview, survey or market data techniques. Each has merit and can be compelling, but it remains the case that such studies have an economic interest in the outcome.

Academic studies have been conducted in both developing economies (Brazil) and in emerging economies (Vietnam) which have the appeal of being less open to (however small it may be) accusation of bias in commercial studies. Firstly, after performing a detailed search of 80 Brazilian listed companies' financial statements to assess those with a CRO or a well-structured governance with a risk committee managed by the board of directors, Silva et al confirmed a positive association between firm value and the use of an ERM approach.¹ They used quantitative techniques involving financial and market metrics that reflected the future expectation of shareholders. This was found after reviewing each firm on a total of 673 occasions and concluded in reports from 2013.

Secondly, in reviewing the largest sample of companies in an emerging market economy using detailed statistical techniques, the finding again indicated that ERM adoption benefits a cross-section of industries. This study specifically noted that a 'key advantage is that ERM enables a highly significant increase in firm value'.² This study also revealed that some firms did not experience improved profitability over the short run and implied that the costs of setting up systems may have been the reason for this.

Improved performance and key risk indicators

The justification for using an ERM approach as outlined above is an attempt to place a cash value on risk events being avoided, although it does also point towards an element of organizational improvement being responsible for the enhanced value generated.

Changes in business performance are often measured by key performance indicators (KPIs) such as an increase in sales in retail, or passenger numbers in the airline industry. If a risk management approach has been implemented in an organization this technique can be replicated into the use of key risk indicators (KRIs). There are also ways in which KPIs such as financial, accounting or business management performance indicators may function as risk indicators (eg a high level of business growth can put pressure on governance systems and internal controls, increasing the potential for fraud, human error, etc). Indicators that relate to the performance of organizational systems, processes and human resources may also signal a change in operational risk.

Table 22.1 Key risk indicators

Causal indicators	Effect indicators
Number and type of causes identified in loss event or near miss data collection	The direct financial cost of operational loss events (asset write downs, provisions for liability claims)
Staff turnover as a % of staff	The indirect costs of operational loss events (eg lost market share, goodwill payments to customers, fines, etc)
Staff morale (collected from staff surveys)	Duration of staff absence due to health and safety incidents
Number of IT patches not implemented	Customer satisfaction scores
Number of attempted IT hacking attacks	Number and duration of disruptions to operational processes and systems
Number of overdue internal audit actions	Number of negative press reports following a loss event
Number of manual interventions to correct automated process failures	Number of negative social media posts following a loss event

Using these metrics will also provide an ongoing justification for the use of an ERM approach as a KRI acts as a proxy for risk exposure. A change in the value of the KRI will signal a change in probability and/or impact. In this regard, KRIs may relate to the causes or effects of operational risk events. Table 22.1 contains some examples of cause and effect indicators

The benefits of an ERM approach

It has been stated throughout this book that the perceived added value from an ERM approach is secure, compliant, legal and competitive operations that bring success to the organization (whatever the measures happen to be). As we have seen in Chapter 16, the cost of using these methods of control, or as implied in the Vietnamese study referenced above, the cost of implementing an ERM approach should be less than the benefits obtained.

COSO has stated that organizations that integrate ERM throughout their organization will realize many benefits, including:

- **Increasing the range of opportunities:** By considering all possibilities (both positive and negative aspects of risk), management can identify new opportunities and the challenges associated with current opportunities.

- **Identifying and managing throughout the risk organization:** Every organization faces risks and a risk can originate in one part of the organization but impact a different part. Management identifies and manages these organization-wide risks to sustain and improve performance.
- **Increasing positive outcomes and advantage while reducing negative surprises:** ERM allows organizations to improve their ability to identify risks and establish appropriate responses, reducing surprises and related costs or losses, while profiting from beneficial developments.
- **Reducing performance variability:** Performing beyond expectations may cause concern and ERM allows organizations to anticipate the risks that would affect.

These may perhaps be simplified into stating that an ERM approach encourages the organization to consciously consider the uncertainties it faces – in particular, to consider those uncertainties that might otherwise be overlooked, including, as we shall see later in this chapter, opportunities to improve and innovate.

In clarifying the risks, the organization will be better prepared and in applying mitigating techniques will be more resilient to changing circumstances. Using this approach should also provide an agreed framework for decision making which should reduce the potential for internal disputes and allow the prioritization of resources, including investments.

In Chapter 6 (see Table 6.3) the benefits of an ERM approach were considered against the process called FIRM (financial, infrastructural, reputational and market-place benefits). Table 22.2 outlines in more detail some key benefits.

Table 22.2 Benefits of ERM

Benefits	Aspects of ERM that help realize them
1 Enhanced value and resilience of the business	Greater awareness of threats and opportunities to the company's objectives, and the processes for dealing with them
2 Fewer unpleasant surprises and shocks for the company and its shareholders	Greater predictability of performance More confidence in the earnings guidance given to shareholders and the market
3 Greater shareholder confidence in the company	A structured and transparent risk management process, directly aligned to the company's objectives, that supports good governance (an aspect of benefit 1) An ability to demonstrate that shareholder capital is being protected and is being exposed to an appropriate level and type of risk

(continued)

Table 22.2 (Continued)

Benefits	Aspects of ERM that help realize them
4 An improved organizational culture	A move away from a prescriptive 'rule-book' approach Clear allocation of accountability for material risks and for the assurance of critical controls A requirement for managers to act with foresight and hindsight
5 Improved business performance	Greater risk management effectiveness, through a structured approach that provides more confidence that important threats and opportunities have been identified and addressed appropriately (supporting benefit 1)
6 Better and faster decisions, and prudent risk taking	Better and more focused information about threats and opportunities, and greater confidence that decisions are being taken on a sound basis (a driver for benefit 5)
7 Better allocation of resources and capital	Agreed risk management standards and guidelines that are applied consistently across the business, thus allowing 'competing' risks and treatment requirements to be compared more readily (an aspect of benefit 6 that supports benefit 1)
8 Better responsiveness and adaptability in the face of changing circumstances	Identification, monitoring and review of emerging threats and opportunities and potential drivers of change (an aspect of benefits 5 and 6 that support benefit 1)
9 Reduced operational costs and management effort	A more structured and efficient risk management process, built on existing organizational practices, that reduces effort and allows managers to focus on the things that really matter (supporting benefits 5 and 6)
10 Improved organizational learning	Monitoring and review processes, including post-investment reviews and lessons learned activities, that support the capture and dissemination of knowledge about the drivers of successes and failures (supporting benefit 6)
11 Enhanced and more efficient control	Better priority setting that assists managers (and internal audit) to focus their assurance activities on the controls that are the most critical for the business Fewer redundant or inefficient controls, because only controls that relate to material risks are needed (supporting benefits 1, 3, 12 and 13)

(continued)

Table 22.2 (Continued)

Benefits	Aspects of ERM that help realize them
12 Reduced losses and better incident management	Better identification, analysis and evaluation of what might cause loss of money or assets, or cause harm to people or the environment, leading to better treatment actions and improved controls (supporting benefit 1)
13 Reduced insurance premiums	A transparent and demonstrable process for identifying and treating potential threats, with supporting control improvement and assurance processes (supporting benefit 9)
14 Satisfy legal, regulatory and internal compliance and reporting requirements	A codified and transparent process, with associated reporting on risk management status and improvements (supporting benefit 3)

SOURCE Reproduced with permission from Broadleaf Capital International (<http://broadleaf.com.au/resource-material/showing-that-effective-risk-management-adds-value/>)

Climate change as a key risk

In light of changes to the climate in the past and forecast changes in future, there is a need to integrate the way that change is managed into the strategic initiatives for all organizations. The uncertainty around climate change means that the risk management function must have a role in how organizations respond to this risk. This is a developing area and one which is being driven by governmental initiatives.

This is manifesting itself in the financial sector where, in the UK, the Task Force on Climate-related Financial Disclosures (TCFD) has been established by the Financial Stability Board:

to develop recommendations for more effective climate-related disclosures that could promote more informed investment, credit, and insurance underwriting decisions and, in turn, enable stakeholders to understand better the concentrations of carbon-related assets in the financial sector and the financial system's exposures to climate-related risks.³

They recommend disclosure of information on investments in companies around four key areas:

- 1** Metrics and targets
- 2** Risk management

3 Strategy**4** Governance

In a similar vein, government is requiring moves to more sustainable transport by setting targets for the removal of fossil fuel-powered vehicles from manufacturers' sale catalogues by certain set dates. This has the effect of ensuring new research to develop electric power trains is brought forward. It is likely that similar regulation will be introduced in coming years to impact most activities.

In thinking about climate change as a risk, the impacts can be classified in three areas:

- 1 Physical risk:** This relates to the impact from the actual changes that will take place in temperature. These risks include forecast rise in sea levels, warmer and wetter seasons, impact on biodiversity, etc.
- 2 Transition risk:** This relates to the changes that will take place as activities move to a more sustainable approach. These risks include the loss of market by failure to offer sustainable product (such as electric cars), the inability to attract talent due to a reputation as a polluter, etc.
- 3 Legal risk:** This relates to the likelihood of future legal challenges to organizations that have knowingly continued to contribute to climate warming. These challenges could be significant in the future as a means of funding future change for wider society and retrospectively penalize companies.

This area of risk management is the subject of further research and is likely to be developing very rapidly in coming years. This Institute of Risk Management introduced a two-day training programme in association with the Grantham Institute of Climate Change (Imperial College) in 2021 and GARP introduced a certificate on Sustainability and Climate Change in 2020 for the financial sector (refer to TCFD above).

Becoming more strategic

In 2008 McKinsey identified a potential for boards of US companies to operate under a 'false sense of security' by using ERM primarily as a compliance tool, driven by the needs of Sarbanes–Oxley and the regulatory environment in the US following the ENRON and other financial scandals. In this paper they argued that their survey data showed boards had put in place processes to identify risks and directors were confident of their approach; and yet only 17 per cent of directors reported they had established a 'risk inventory' (sic) and less than half were able to prioritize risk effectively.

The paper further established that 75 per cent of directors who sit on multiple boards reported ‘significant variation’ in the way ERM was applied in different firms and industries, with financial firms leading the way in their application of ERM. The paper is interesting in that it identified a trend where more directors associated ERM as a core strategic function than those who considered it to be ‘low-value adding’ and related to compliance.⁴

This was perhaps an early indication of trends in ERM, but it presents a tightly argued case to add more value through ERM by moving from a ‘safeguarding’ function to a much more ‘strategic’ function in order to show real benefit. The requirements are shown in Table 22.3.

Table 22.3 From safeguarding to maximizing value

Safeguarding enterprise value	Maximizing enterprise value
Compliance focused	Value focused
Extensive risk mapping	Focusing on a few key risks driving disproportionate gains/losses
Risk mitigation	Risk optimization
Disconnected from strategic and operational decisions	Core to strategic and operational decisions
Lower-level staff activity	Line function, facilitated by highly skilled staff

Notes

- 1 Silva, J, da Silva, A and Chan, B (2018) Enterprise risk management and firm value: Evidence from Brazil, *Emerging Markets Finance and Trade*, 55 (3), pp 687–703
- 2 Kommunuri, J et al (2016) Firm performance and value effects of enterprise risk management, *New Zealand Journal of Applied Business Research*, 14 (2)
- 3 Task Force on Climate-related Financial Disclosure (2020) *Overview*, https://assets.bbhub.io/company/sites/60/2020/10/TCFD_Booklet_FNL_Digital_March-2020.pdf (archived at <https://perma.cc/7TUA-NPC4>)
- 4 Brodeur, A and Pitsch, G (2008) Making risk management a value-adding function in the boardroom, McKinsey Working Papers on Risk, 2, www.mckinsey.com/-/media/mckinsey/dotcom/client_service/Risk/Working%20papers/2_Making_risk_management_a_valueadding_function_in_the_boardroom.ashx (archived at <https://perma.cc/3B9E-AGGH>)

THIS PAGE IS INTENTIONALLY LEFT BLANK

PART SIX

Risk strategy and culture

LEARNING OUTCOMES

Having studied this section readers will be able to:

- Describe the key features of a risk-aware culture (LILAC) and how the key components are defined and can be measured.
- Describe the components of risk maturity of an organization (4Ns) and the influence on risk management activities (FOIL).
- Describe the importance of risk appetite and how this can be demonstrated on a risk matrix, together with the risk exposure and risk capacity.
- Review the nature of risk appetite statements and how these can be used to influence decision making within organizations.
- Explain the importance of risk training and risk communication, and the influence on the risk culture of an organization.
- Summarize the importance of risk training and risk communication, including the use of risk management information systems (RMIS).
- Explain the features of a risk competency framework and the relationship to plan, implement, measure and learn (PIML).
- Outline the people skills required by a risk practitioner summarized as communication (5Cs), relationship, analytical and management (CRAM).

Further reading

- ASIS International (2009) *Organizational Resilience: Security, preparedness and continuity management systems, ASIS SPC.1-2009. American National Standard*, www.ndsu.edu/fileadmin/emgt/ASIS_SPC.1-2009_Item_No._1842.pdf
- Hillson, D (2016) *The Risk Management Handbook: A practical guide to managing the multiple dimensions of risk*, Kogan Page, London
- Seville, E (2016) *Resilient Organizations: How to survive, thrive and create opportunities through crisis and change*, Kogan Page, London
- Sheffi, Y (2015) *The Power of Resilience: How the best companies manage the unexpected*, MIT Press, Cambridge, MA
- Taylor, E (2014) *Practical Enterprise Risk Management*, Kogan Page, London

CASE STUDIES

The student can review the following examples to illustrate further the areas discussed in Part Six and throughout this book.

Singapore Airlines: Response to pandemic

Singapore Airlines is the national airline of Singapore. It is majority owned by the government but with significant private backing. It operates in both the business and leisure travel sectors, with a low-cost subsidiary and significant earnings from the freight cargo it carries.

The airline was significantly impacted by the pandemic and reported in its annual report of 2020 that:

The Group began monitoring the situation closely at the onset of the outbreak so that measures are promptly implemented to safeguard the safety of employees and passengers, and to ensure business operations remain sustainable through the identification of emerging risks.

The measures taken included implementing their pandemic response plan and business continuity plans, which will have been written in light of the SARS outbreak in the region earlier in the decade. They also refer to being flexible and agile in their response by ‘making frequent adjustments to the Group’s operations to comply with the tighter measures implemented by governments to curb the transmission of the virus’.

The airline swiftly reduced its capacity due to the collapse of air travel demand, and re-financed to manage liquidity and protect the jobs of employees. Whilst alive to the losses it has suffered, the company also noted that there are plans in place to ‘seize opportunities at the first signs of recovery’.

Edited extracts from: Singapore Airlines (2020) Annual Report FY2019/20, www.singaporeair.com/saar5/pdf/Investor-Relations/Annual-Report/annualreport1920.pdf

Nokia plc: Business model and risk management function

Nokia provides a good example of a strategic shock to a business model when Apple released its iPhone with the result that Nokia was 'out-competed' in its mobile phone business. The swift change in the market required them to take prompt action, exiting the mobile and devices sector between 2011 and 2014 through a sale to Microsoft, albeit re-entering that market in a smaller way in 2016 through a lower-cost joint venture.

Since then, they have focused on other growth areas in technology where they held advantages through patents and focused acquisition in delivering increased network capability with infrastructure and mobile networks, including cloud services.

Their risk management system is one that identifies:

Key risks and opportunities... against business targets either in business operations or as an integral part of strategy and financial planning. Risk management covers strategic, operational, financial, compliance and hazard risks.

These risks and opportunities form part of their general business performance management across the enterprise, supported by their centralized 'enterprise risk management function'. They communicate this in their 'Nokia Enterprise Risk Management Policy, which is approved by the Audit Committee of the Board and which allows 'risk management and its elements to be integrated into key processes'.

They state that risk has a clearly identified 'risk owner, although all employees are responsible for identifying, analysing and managing risks' and they further state that their appetite is 'based on managing the key risks that would prevent us from meeting our objectives, rather than solely focusing on eliminating risks'.

Edited extracts from: Nokia (2021) Nokia in 2020, www.nokia.com/system/files/2021-03/Nokia_Annual_Report_2020_English.pdf

Financial Conduct Authority: Risk culture

This UK regulator is responsible for regulating financial services in the UK and has been chosen as a case study for its discussion of risk culture. In the reference below there is a link to papers they have published which include discussions from leaders in various banks as well as academics.

The Financial Conduct Authority (FCA) has become involved in this area since they state 'Firms' cultures have been a major root cause of conduct failures, and our work supporting firms in delivering real and sustainable culture transformations will help prevent harm caused by inappropriate behaviours'.

They are explicit in stating that the reason for extending the Senior Managers and Certification Regime (SM&CR) to all authorized firms was to transform culture in those firms by 'improving the accountability of individuals'.

This work has broad applicability and elements of the work done here will be useful in all sectors. It is also of interest to consider how a regulator interacts with the firms it supervises. They state that 'Culture is at the heart of how we authorize and supervise firms'. They will not 'prescribe what any firm's culture should be. It is the responsibility of everyone in financial services to focus on culture, and we expect leaders in firms to manage the drivers of behaviour in their firms to create and maintain cultures which reduce the potential for harm.'

The themes they have considered are: (1) 'psychological safety' – a culture where it is safe for employees to 'speak up', (2) leadership – the power of role models, (3) incentives – what motivates individuals.

*Edited extracts from: FCA (2020) Culture and governance, www.fca.org.uk/firms/culture-and-governance and FCA (2018) *Transforming Culture in Financial Services: Discussion paper DP 18/2*, www.fca.org.uk/publication/discussion/dp18-02.pdf*

Risk architecture and strategy 23

Architecture, strategy and protocols

This chapter discusses the risk architecture, strategy and protocols (RASP) for an organization. The RASP provides details of the risk management framework for the organization and this helps to define the risk management context. Figure 23.1 sets out its key features in more detail. The most important component of the RASP is the risk management policy statement. This policy statement will set out the overall strategy of the organization towards risk management. It will usually be the opening statement in a risk management manual, which will also define risk management roles and responsibilities and set out the protocols that should be followed.

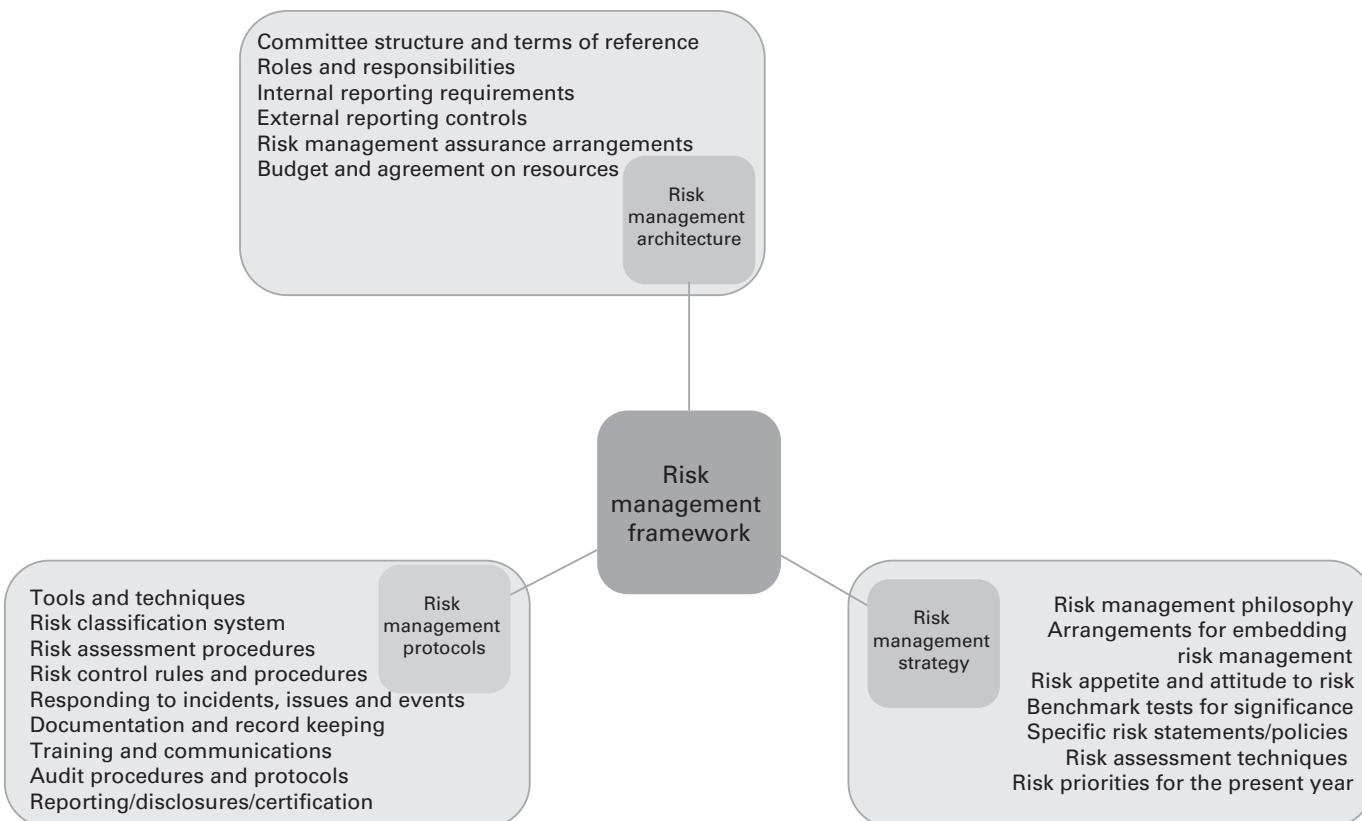
The risk management manual provides a framework to support the risk management process. BS 31100 states that it should include the objectives, mandate and commitment to manage risk (strategy), and the organizational arrangements that include plans, relationships, accountabilities, resources, processes and activities (architecture), and that the framework should be embedded within the organization's overall strategic and operational policies and practices (protocols).

In effect, the RASP represents the context for risk management within the organization. The risk strategy component will normally be set out as a high-level or one-page statement of what the organization is seeking to achieve with respect to risk management. Guide 73 refers to this one-page statement as the risk management policy.

Most large organizations will document their risk protocols as a set of risk management guidelines. The range of guidelines that are required will vary according to the size, nature and complexity of the organization. The types of documentation that will need to be kept are as follows:

- risk management administration records;
- risk response and improvement plans;
- event reports and recommendations;
- risk performance and monitoring reports.

Figure 23.1 Risk management framework



The risk architecture defines how information on risk is communicated throughout the organization and forms part of the risk management framework. The risk strategy defines the overall objectives that the organization is trying to achieve with respect to risk management. The risk protocols are the systems, standards and procedures that are put in place in order to fulfil the defined risk strategy. The risk management framework, in turn, is part of the overall risk governance arrangements within the organization.

The next box features a statement from the constitution of the Royal Borough of Kensington and Chelsea. This is the council that owned and outsourced management of the Grenfell Tower block, which caught fire in 2019 in the worst civil disaster in the UK since the Second World War. As can be seen from this, for a risk management statement to be of any practical use, there needs to be a commitment to operate it effectively.

A risk management policy for a council

The Constitution of the Royal Borough of Kensington and Chelsea

Part 8: Procedures; Section 3: Financial procedure rules; Sub-section 5: Risk management and control of resources

Risk Management and Internal Control covers risk management and insurance, internal control, audit requirements, preventing fraud and corruption, assets, treasury management, investments and borrowing, trust funds and funds held for third parties, banking, imprest accounts and staffing costs.

1.12 The Audit and Transparency Committee is responsible for agreeing the authority's risk management policy statement and strategy and for reviewing the effectiveness of risk management within the Council.

1.13 The Executive Director Resources & Assets is responsible for developing, maintaining and advising upon robust systems for risk management and the control of resources. This will be monitored through an effective internal audit function.

1.14 Executive Directors are responsible for establishing and operating sound arrangements within these systems to manage and mitigate risk and for notifying the Executive Director Resources & Assets of any suspected non-compliance.

Part 5: Committees and non-executive functions; Section 2: Terms of reference of council committees; Sub-section 5: Audit and Transparency Committee

5.1 The purpose of the Audit and Transparency Committee is:

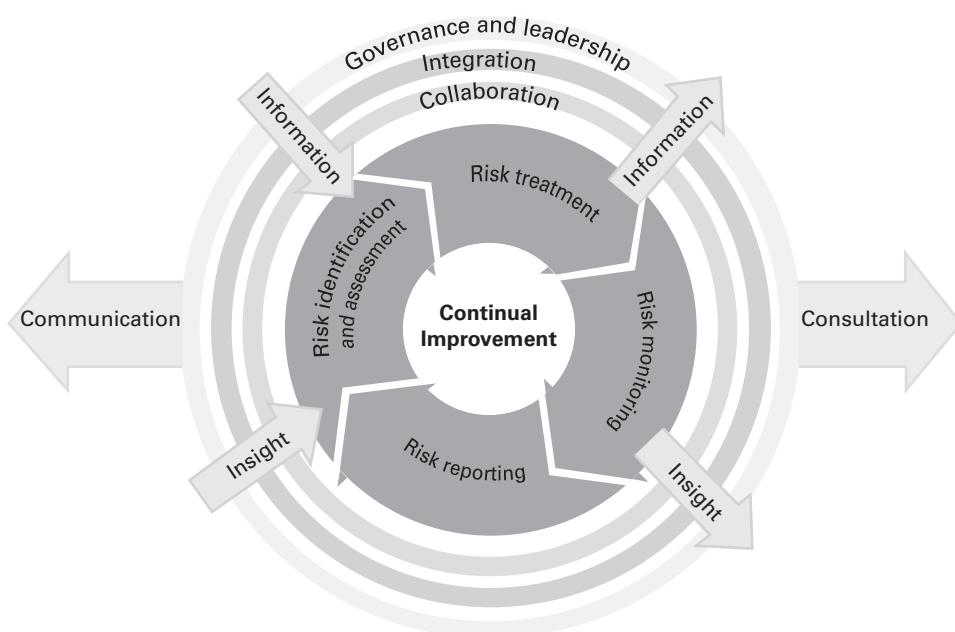
- i. to provide independent assurance on corporate governance arrangements; the adequacy of the risk management framework and the associated control environment; independent scrutiny of the authority's financial and non-financial performance to the extent that it affects the authority's exposure to risk and weakens the control environment; and oversight of the financial reporting process;
- ii. to oversee Council transparency; and
- iii. to consider any complaints against Councillors referred to it following an investigation.

5.10 Terms of Reference, item (xvi) To monitor the effective development and operation of risk management in the Council.

SOURCE Royal Borough of Kensington and Chelsea (2021) The constitution, www.rbkc.gov.uk/council-councillors-and-democracy/how-council-works/constitution

A graphic example of a risk management framework is shown in Figure 23.2 taken from *The Orange Book* 2020.

Figure 23.2 Example risk management framework



SOURCE HM Government (2020) *The Orange Book: Management of risk – principles and concepts*, p 6, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866117/6.6266_HMT_Orange_Book_Update_v6_WEB.PDF

Risk architecture

The risk management organization and arrangements of an organization can be described as the risk architecture. The risk architecture sets out lines of communication for reporting on risk management issues and events and allocating ownership of particular risks within the organization.

In order that risk management can be fully embedded into the core processes and operations of an organization, a clear statement of risk management responsibilities is required. Risk management responsibilities need to be clearly allocated to the following aspects of managing that risk:

- development of risk strategy and standards;
- implementation of the agreed standards and procedures;
- auditing compliance with the agreed standards.

The risk architecture can be represented diagrammatically as a means of identifying the committees with risk management responsibilities and the relationships between those committees. The risk architecture will include the terms of reference of the various committees, including details of the membership and responsibilities of those committees. The risk architecture should also provide information on how risk information is communicated between the various committees.

The risk architecture shows the relationships between various committees that have been established within the organization and will also include details of reports that are received and required by individual committees. An important aspect of the risk architecture is to ensure that risk escalation procedures are embedded within the organization, including appropriate whistleblowing arrangements.

When considering the range of documentation that needs to be produced, organizations should distinguish between the risk protocols that are recorded in the risk management manual and those documents or reports that are intended to track and monitor changes and improvements. The risk management manual will be a static record of processes and procedures, whereas the other documentation, for example the risk register, should be a dynamic record of actions that are planned or are in progress. In effect, the risk register should be considered to be the risk management action plan.

Risk management strategy

It is important for an organization to have a clearly established strategy in relation to risk management. The risk management strategy for the organization will be set out in the risk management policy statement. The strategy needs to be based

on the overall approach of the organization to risk and risk management. An important component of that risk strategy will be the requirement that there is risk management input into strategy, tactics, operations and compliance (STOC). In order to establish the risk management strategy, important decisions will need to be made about the risk appetite of the organization. The risk appetite will be based on the opportunity investment, control acceptance and hazard tolerance of the organization.

It is important that the risk appetite is within the total risk capacity of the organization. Decisions will need to be taken on how the risk capacity will be calculated and how the total risk exposure of the organization will be recorded and used in decision making processes. Measurement of the total risk exposure of an organization is an important feature of operational risk management, as discussed in Chapter 31.

There are important decisions to be made in relation to the risk processes that will be adopted by the organization, as well as decisions about the design and implementation of the risk management initiative that will be planned and implemented in order to fulfil the requirements of the risk strategy.

The risk management strategy will state what the organization is seeking to achieve. The strategy may set out what level of risk maturity is desired, together with the information on the level of contribution that is expected from risk management. In effect, risk management strategy will establish the way in which risk management activities are aligned with the other activities in the organization and the contribution that is expected from risk management activities.

Risk management protocols

The risk management manual will set out responsibilities for risk as well as the arrangements for implementing the policy. Risk management protocols will be set out in a series of risk procedures and guidelines, and these are described later in this chapter.

Procedures and protocols for undertaking the assessment of risks to strategy, projects and operations will need to be established in writing. The organization will also need to produce guidance on the frequency and nature of risk reports and who is responsible for compiling the information.

Typically, the risk management protocols will need to be reviewed on an annual basis, so that they are kept up to date and the organization is taking advantage of any new technology that may have become available. The risk protocols should also describe the extent of record keeping that is required. The range of risk management documentation that may be necessary is extensive and Table 23.1 provides an overview of the types of documents that may be appropriate.

Table 23.1 Types of RM documentation

Activity	RM documentation
Risk governance	Risk management policy (and priorities) Specific risk statements (health and safety policy) Terms of reference of the risk/audit committees Risk protocols and procedures Risk awareness training records
Risk response	Results of risk assessments (risk register) Risk control standards Risk improvement recommendations Risk assurance reports
Event reports	Loss/claim reports and recommendations Legal and litigation reports Enforcement action/customer complaints Incident and near miss investigations Business performance reports/key performance indicators Business continuity plans/disaster recovery plans
Risk performance	Control risk self-assessment returns Audit procedures and protocols Internal audit reports Unit risk management reports External disclosure reports

Risk management protocols define and describe the range of activities that are required and how they will be undertaken. Risk management guidelines normally refer to the standards that should be achieved. In some cases, they include details of the controls that are in place. This will be especially true for guidelines that identify procedures that must be undertaken. These procedures will provide direction for directors, managers and staff within the organization.

Risk management manual

The extent of the documentation produced by an organization in respect of risk management will vary significantly. The documentation that is produced should be proportionate to the level of risk faced by the organization, in accordance with the principles that apply to risk management, as set out in Table 3.3. Whatever is produced will need to be structured in a way that suits the organization and is aligned with the other activities that take place within the organization.

The risk management manual will contain the policy and details of all of the responsibilities, procedures, protocols and guidelines regarding the risk management process and risk management framework for the organization. An illustration of suitable contents for a risk management manual is set out in Table 23.2. The manual should confirm the protocols for undertaking the activities, as set out in the risk guidelines for the organization. The risk guidelines may be produced as a separate set of documents, so that they can be more easily updated.

The risk management manual will set out details of the systems and procedures that will be put in place to monitor performance, as well as the means for reporting and communicating on risk management. It will, in effect, define the context within which risk management activities take place.

A range of risk management protocols or guidelines will need to be produced, and a typical set of protocols is listed in Table 23.3. The risk protocols provide more information on how the risk protocols should be interpreted and how they should be delivered. The risk management protocols can be seen as the standing instructions relating to risk management. They will often require the keeping of records, for example the risk register. The detailed risk management protocols or guidelines will set out:

- risk assessment procedures;
- risk control objectives;
- risk resourcing arrangements;
- reaction planning requirements;
- risk assurance systems.

Table 23.2 Risk management manual

A risk management manual should include the following sections:

Risk management and internal control objectives

Statement of the attitude of the organization to risk (risk strategy)

Description of the control environment

Level and nature of risk that is acceptable

Risk management organization and arrangements (risk architecture)

Arrangements for communicating risk information

Standard procedures for risk recognition and rating (risk assessment)

List of documentation for analysing and reporting risk (risk protocols)

Risk mitigation requirements and control mechanisms

Allocation of risk management roles and responsibilities

Criteria for monitoring and benchmarking risks

Allocation of appropriate resources

Risk priorities and performance targets

Risk management calendar for the coming year

Table 23.3 Risk management protocols

1 Risk assessment procedures	Governance procedures Response to significant risks Projects and Capex approvals Procedures for strategy and budgets
2 Risk control objectives	Brand management guidelines Health and safety at work Environmental protection Contract risk management
3 Risk resourcing arrangements	Opportunity management Project resource allocation Insurance programme Captive insurance company
4 Reaction planning requirements	Loss and claims management Disaster and recovery planning Cost containment procedures Risk management record keeping
5 Risk assurance systems	Maintenance of risk register Corporate RM committee Terms of reference for audit committee Control self-certification arrangements

The framework or risk architecture that has been set up to achieve adequate management of risks should also be presented in the risk management manual. It will then be for the individual companies within the group to operate within the established framework and arrange their own additional procedures and protocols as necessary. Specifically, the risk management manual should include details of at least the following:

- the board member responsible for risk management;
- language and perception of risk in the organization;
- framework for identifying significant risks;
- terms of reference for the risk management committees;
- risk management structure or risk architecture.
- role of the risk manager and internal auditors.

The working relationship between risk management and internal audit is critically important. The RASP should set out the details of how this close co-operation will be achieved in practice. Risk management expertise rests in the assessment of risk

and the identification of existing and additional controls. Internal audit has its expertise in the evaluation of controls and the testing of their efficiency and effectiveness.

Many organizations find that it is necessary to update the risk management manual each year, even if the overall risk management strategy remains unchanged. This is undertaken for a number of reasons, including the desire to ensure that risk management activities and the overall risk management approach are in line with current best practice. Updating the risk management manual, including the risk management policy, every year also gives the organization the opportunity to identify the risk priorities for the coming year and ensure that appropriate attention is paid to the significant risks.

Issuing an updated risk management policy every year also ensures that the board pays appropriate attention to risk management and that the organization understands that it is a dynamic activity that requires constant management attention.

Risk management documentation

Table 23.3 indicates the extent of risk management guidelines or protocols that may need to be produced by an organization. This should not be seen as an exhaustive list and other types of protocols, guidelines or procedures may be necessary, depending on the exact nature of the organization and the risk strategy that it is following.

Preparation of a risk management manual, including the policy statement, is a good opportunity for an organization to establish detailed procedures on a range of risk management topics, as well as setting out the risk management priorities for the following year. For example, some organizations produce an annual health and safety and/or environmental policy and procedures, and this should be an integral part of the risk management documentation.

Other organizations face significant risks that need routine or even constant management attention. This is particularly true in the case of hazard risks, where the health and safety policy and procedures, business continuity plans and disaster recovery plans (for example) need to be routinely updated.

For many organizations, the risk guidelines will be established in writing. Other organizations will operate a more informal means of embedding risk management into management activities. The risk guidelines will often include details of the risk management structure in place in the organization. Also, details of the risk strategy and risk protocols will need to be included in the risk guidelines. They should also include details of the (internal) control responsibilities of managers.

The structure described in Table 23.3 reinforces the importance of the activities involved in the risk management process. Each of these activities produces several outputs, and the required outputs can be discussed in the risk guidelines.

The guidelines need not include a set of risk control or loss control standards, but should describe how risk control decisions will be taken, implemented and audited. The risk guidelines for a diverse group of companies may require each unit, division or department to set its own standards for risk control, including health and safety, fire safety, physical security, information security and environmental protection. This may be appropriate because of the diverse nature of the different units within the organization.

The risk guidelines should define the means by which embedded risk management is to be achieved in the organization. The setting of strategy, standards and procedures needs to be undertaken within the framework of the risk guidelines. The format for the risk guidelines will depend on the organization and the nature of the risks that it faces. Typically, these guidelines will contain information on at least the following:

- financial and authorization procedures;
- insurance arrangements;
- managers' control responsibilities;
- project risk management;
- incident reporting and investigation;
- event and reaction planning;
- physical risk control objectives and responsibilities.

Embedded risk management will be achieved when the cycle of risk management activities is fully aligned with the planning cycle of the organization. A primary purpose of risk guidelines is to help managers understand the risk management framework of the organization. This understanding will ensure that managers pay appropriate attention to risk implications when making decisions.

The risk guidelines for the organization also provide practical guidance to managers on how to fulfil their risk management responsibilities. Keeping necessary records will allow the organization to demonstrate the successful implementation of the risk guidelines, inform decision making, and confirm that necessary controls have been correctly implemented. This should not become an overly bureaucratic or burdensome task and could, for example, incorporate the use of technology applications that quickly update agreed records. The importance of record keeping is highlighted below.

The risk management administration documentation should extend to (at least) the items listed in Table 23.1.

The importance of records

There are many benefits to be gained from maintaining good records. It is a key driver in increasing organizational efficiency and offers significant business benefits.

Records management:

- reduces the time spent by staff looking for information;
- facilitates the effective sharing of information;
- reduces the unnecessary duplication of information;
- identifies how long records need to be kept;
- optimizes the legal admissibility of records to defend malicious litigation;
- supports risk management and business continuity planning.

In short, records management improves control over information assets, frees up staff time and other resources, and helps protect individuals and the organization from various risks. Records management means that too much reliance is not placed on the memories of a few individuals. Care should be taken to ensure that information stored in this way is compliant with regulation surrounding privacy, such as GDPR in Europe.

The only reason for undertaking a risk assessment is so that current controls can be validated and the need for any further actions to improve control of risk can be identified. The risk register is the means of recording information on current controls and details of intended additional controls. It is important that the risk register should not become a static document. It should be treated as a dynamic element and considered to be the risk action plan for a unit or the organization as a whole.

As well as risk response plans, information will also need to be recorded about the responsibility for individual controls. If additional controls are required, then the deadline, as well as the responsibility, for the implementation of those improved controls should be recorded.

For hazard risks and control risks, the risk register is the location for recording details of the significant threats. Detailed analysis of risk improvement plans will be required. Often, risk improvement plans will require capital expenditure, and this may need to be approved via the expenditure authorization procedures in the organization.

It has become standard practice to produce a risk register for projects, especially for construction and software projects. Risks to construction and software projects can create a lot of uncertainty and the risks will usually be control risks. Again, the record of the actions taken to minimize the uncertainty should be a dynamic one, and further actions should be planned.

It is a common criticism of risk registers that they are undertaken once or twice a year and represent a static snapshot of the risks facing the organization. In order to be effective and make a significant contribution, risk management needs to be a dynamic activity that produces outputs that have an impact on the organization. If this is going to happen, then the risk register needs to become a document that drives changes and improvements. There are applications available that can address this using technology.

Event reports, analyses and recommendations are related to recording details of the events that occur and managing the impacts and consequences of those events. Details of incident investigations and analysis of the performance of business operations, together with risk improvement recommendations, are all covered by this type of risk management documentation. Risk improvement recommendations address significant control weaknesses and aim to eliminate the potential for future material or significant failures.

Recording of events is an important activity, especially in relation to hazard risks. Also, recording and analysing events during a project will be vitally important. Event reports are most relevant to hazard and control risks. Annual evaluation of risk performance will also give rise to reports that require detailed analysis. Evaluation of risk performance is an important role for internal audit.

Clinical risk management is a well-developed branch of the risk management discipline. Accurate record keeping is vital in order to identify that appropriate risk mitigation actions have been put in place, as well as to provide records of any clinical mishaps that occur. The box below provides an overview of the importance of record keeping in relation to managing clinical risk.

Managing clinical risk

Even if all adverse clinical events could be avoided, the legal cost of malpractice litigation cannot be eliminated. While very few negligent injuries lead to claims, there are claims in cases where there was no injury and no negligence. Hospitals and doctors can rebut allegations of negligence and successfully argue that no compensation payment should be made if the right risk management processes and systems are in place.

The implementation of risk management activities in hospitals is the immediate responsibility of hospital management. Nevertheless, doctors have a vital role to play by developing an understanding of the importance of risk management and helping to devise a practical approach to recording that procedures have been followed and any incidents have been recorded.

Risk performance and certification reports include consideration and analysis of preliminary reports of the results of operations, as well as more formal declarations and certified reports to stakeholders. In some cases, certification of the results of operations of the organization will be undertaken as a formal attestation of the results of operations. This approach is required by the Sarbanes–Oxley Act in relation to financial reporting.

This attestation will often be undertaken by a third party, such as an external auditor. Such an attestation could also relate to an evaluation of the effectiveness of the control activities.

Management will be interested in receiving details of risk performance. This will be especially important when the organization is exposed to a portfolio of risks that bring the total risk exposure close to the limit of the risk appetite and/or risk capacity of the organization. For example, an organization may have budgeted for a certain level of loss in relation to hazard risks. If this budget is challenging, then careful monitoring of losses will be required in order to ensure that the exposure to the specific type of hazard risk is not being exceeded.

The hazard tolerance may be limited and so the organization will need to monitor hazard losses very carefully. For example, a transport company will need to monitor the number of motor vehicle accidents and the breakdown frequencies related to the vehicles run by the company.

Roles, responsibilities and documentation

24

Allocation of responsibilities

Everybody working for an organization will need to be made aware of their risk management responsibilities, as will contractors and suppliers. There are many professional people in large organizations who have an understanding of risk and a substantial contribution to make to the successful management of the priority significant risks. Unfortunately, there is not always a common view of risk management or the issues that are important to the organization.

Ownership of core processes, key dependencies and risks is key, because it enables the risk management and audit committees (see Part Eight) to monitor actions and responsibilities. This ownership is important for all risks, although the audit committee will only monitor the priority significant risks.

Any confusion of responsibilities and reporting structure must be eliminated. There should be clear statements of responsibilities for the following aspects of the management of each priority significant risk:

- setting required risk standards;
- implementing risk standards;
- monitoring risk performance.

A detailed set of responsibilities will ensure that the roles of risk owners, process owners, internal audit, risk management functions, members of staff, contractors and outsourced operations as well as all others are clearly defined and understood. The allocation of responsibilities to committees, as part of the risk architecture, is also an important consideration. The membership, responsibilities and reporting structure will normally be described in the terms of reference of each committee.

Information on ownership of each priority significant risk should be included in the risk register. It is important that the activities of the risk manager, risk management committee, audit committee, internal auditors and others do not reduce local

ownership of significant risks. Managers must see ownership of risks as integral to the management of core processes and business activities, not as a separate issue that is the responsibility of specialist professional risk management and/or internal audit practitioners.

Range of responsibilities

Table 24.1 sets out examples of the range of risk management responsibilities of line management, the main functional departments and individual employees involved in risk management. The risk management professionals involved will include the following individuals (at least), depending on the size of the organization:

- insurance risk manager;
- corporate treasurer;
- finance director;
- internal auditor;
- compliance manager;
- health, safety and environment manager;
- business continuity manager.

The structure of Table 24.1 is also important. Items 1, 2 and 3 allocate responsibilities to the management of the organization. Item 1 is concerned with the allocation of responsibilities to top management, being the board and executive. Item 2 is concerned with the allocation of responsibilities to heads of department or middle management. Item 3 is concerned with the allocation of risk management responsibilities to staff. Together, these three layers of management represent the first line of defence in ensuring that adequate attention is paid to risk management and internal control.

Item 4 of Table 24.1 describes the responsibilities of the risk manager for the organization. Item 5 sets out the responsibilities of specialist risk management functions, such as health and safety or business continuity. In providing specialist support to management, these functions may be considered to be the second line of defence in achieving satisfactory risk management and internal control. Item 6 of Table 24.1 sets out the responsibilities of the internal audit manager. Internal audit activities may be considered to be the third line of defence in ensuring adequate standards of risk management and internal control.

Externally, insurance brokers, insurance companies, accountancy firms and external auditors also have a contribution to make to the improved management of risk in their client organizations. It is important that risk management professionals work together. However, it is also important that the benefits of risk management are embedded into the core processes of the organization.

Table 24.1 Risk management responsibilities

Main risk management responsibilities for	Key responsibilities
1. The CEO	Determine strategic approach to risk Establish the structure for risk management Understand the most significant risks Consider the risk implications of poor decisions Manage the organization in a crisis
2. The location manager	Build risk-aware culture within the location Agree risk management performance targets for the location Evaluate reports from employees on risk management matters Ensure implementation of risk improvement recommendations Identify and report changed circumstances/risks
3. Individual employees	Understand, accept and implement RM processes Report inefficient, unnecessary or unworkable controls Report loss events and near-miss incidents Co-operate with management on incident investigations Ensure that visitors and contractors comply with procedures
4. The risk manager	Develop the risk management policy and keep it up to date Facilitate a risk-aware culture within the organization Establish internal risk policies and structures Coordinate the risk management activities Compile risk information and prepare reports for the board
5. Specialist risk management functions	Assist the company in establishing specialist risk policies Develop specialist contingency and recovery plans Keep up to date with developments in the specialist area Support investigations of incidents and near misses Prepare detailed reports on specialist risks
6. Internal audit manager	Develop a risk-based internal audit programme Audit the risk processes across the organization Provide assurance on the management of risk Support and help to develop the risk management processes Report on the efficiency and effectiveness of internal controls

Three lines of defence

An objective of operational risk management is not to remove operational risk altogether, but to manage the risk to an acceptable level, taking into account the cost of minimizing the risk as against the resultant reduction in exposure. Strategies

to manage operational risk include avoidance, transfer, acceptance and mitigation by controls.

To ensure appropriate responsibility is allocated for the management, reporting and escalation of operational risk, the group operates a ‘three lines of defence’ model that outlines principles for the roles, responsibilities and accountabilities for operational risk management.

The three lines of defence model and the policy standards apply throughout the group and are implemented taking into account the nature and scale of the underlying business. The standards provide the direction for delivering effective operational risk management. They comprise principles and processes that enable the consistent identification, assessment, management, monitoring and reporting of operational risk across the group. The objectives of the standards are to protect the group from financial loss or damage to its reputation, its customers or staff and to ensure that it meets all necessary regulatory and legal requirements.

There is a need to ensure that management of risks receives a sufficiently high profile. It will normally be a board member who sponsors risk management awareness at the board and presents risk management reports to the board. Typically, the risk manager will report to that board member, and have responsibility for the risk architecture, strategy and protocols (RASP).

One of the most important responsibilities to be allocated is that of ‘risk owner’. ISO Guide 73 defines a risk owner as a ‘person with authority and accountability to make the decision to treat, or not to treat a risk’. The guide also states that anyone who has accountability for an objective also has accountability for the risks associated with the objective and the implementation of the controls to manage those risks.

Statutory responsibilities of management

There has been a developing trend in many countries towards ensuring greater clarity in regard to the obligations of company directors. The general duties of directors have developed in the common law over many years in most countries. The Companies Act 2006 in the UK has consolidated the common law duties of directors and codified the general duties, as follows:

- act in accordance with allocated responsibilities;
- act in accordance with the constitution of the company;
- promote the success of the company;

- exercise independent judgement;
- exercise reasonable care, skill and diligence;
- avoid/declare conflicts of interest;
- not accept benefits from third parties.

The responsibilities of directors are important in relation to risk management, and adequate management of risk will assist in the successful fulfilment of these obligations. Risk management is particularly important in promoting the success of the organization and exercising reasonable care, skill and diligence. Directors of organizations need a good understanding of risk management so that they will be in a better position to fulfil their statutory and other duties.

Usually, board directors will be either executive or non-executive directors of the organization. In certain organizations, such as charities and most government departments, executive directors will meet separately as an ‘executive committee’ and the non-executive directors will form a ‘board of governors’. Typically, executive directors will be full-time employees of the organization with a specific area of responsibility.

Non-executive directors have an important role to play in risk management within the organization. However, this role will normally be restricted to audit, assurance and compliance activities. It may be inappropriate for non-executive directors to become involved in the management of the individual risks, because of the conflict with non-executive audit responsibilities and because executive directors are in a better position to understand and deal with the risks that the organization faces.

The next box provides an example of the role and expectations of non-executive directors. In general, non-executive directors should not become directly involved in the day-to-day management of the organization. In most cases, their role is to assist with the formation of strategy and the monitoring of performance. Implementation of strategy is the responsibility of executive directors.

Role of non-executive directors

The role of the non-executive director has the following specific key elements:

Strategy: Constructively challenge and help develop proposals on strategy.

Performance: Scrutinize the performance of management.

Risk: Challenge the integrity of the financial information.

Controls: Seek assurance that financial controls and systems of risk management are robust and defensible.

- People: Determine the appropriate level of remuneration for the executive directors and have a prime role in succession planning.
- Confidence: Seek to establish and maintain confidence in the conduct of the company.
- Independence: Be independent in judgement and promote openness and trust.
- Knowledge: Be well informed about the company and the external environment in which it operates, with a strong command of relevant issues.

Role of the risk manager

There is no single established reporting position in the structure of an organization for the risk manager. Risk managers may report the CEO, the finance director or treasury, the company secretary or group legal department or even to human resources or procurement.

The risk management facilitator and co-ordinator in most large organizations will be needed to enable the organization to apply risk management tools and techniques to a wide range of issues. Risks have in the past been seen as either insurable (pure) or non-insurable (speculative) risks. From this legacy, the risk management function has often grown from its main function of procuring insurance and has been termed as an insurance risk manager. The roles of the insurance risk manager are set out in Table 24.2. Traditionally, the role included assessing overall risk policy and procedures from the perspective of insured risks, and the provision of statistical analysis of insurance losses has been part of these historical responsibilities.

The insurance risk manager needs to have a good understanding of the insurance market. Its often cyclical nature has brought about a more sophisticated approach to risk financing and in many cases the insurance risk manager will propose buying less insurance and diverting savings to self-insurance vehicles such as captives.

Table 24.2 Historical role of the insurance risk manager

- | | |
|---|---|
| 1 | To establish the risk management strategy for protecting company property and people. |
| 2 | To co-ordinate company insurance programme, including use of captive insurance. |
| 3 | To maximize contribution made by any captive insurance company. |

(continued)

Table 24.2 (Continued)

-
- | | |
|---|--|
| 4 | To maintain key insurer relationships, monitor service providers and ensure cost-effective placement of insurance contracts. |
| 5 | To measure and monitor cost of risk performance of group and individual group companies. |
| 6 | To ensure safekeeping and adequate retention of all insurance contracts and agreements. |
| 7 | To supervise co-ordination of service provider activities and place group and global insurances. |
| 8 | To co-ordinate property survey programme, risk management procedures and incentive schemes. |
-

The risk manager should be responsible for the corporate learning that has to take place so that the organization can understand the benefits of risk management. As the person having responsibility for the risk architecture, strategy and protocols (RASP), the risk manager will be responsible for developing the strategy, systems and procedures by which the required risk management outcomes for the organization are achieved.

The role of a risk manager now requires a greater involvement in project management and strategy formulation and delivery than procuring insurance. The broad range of responsibilities enable the risk manager to obtain a better level of understanding and involvement than most other roles or functions achieve. The developing importance of organizational resilience may offer an opportunity for the risk manager to develop into the ‘risk and resilience manager’ and fulfil a much broader role that is designed to be more aligned with the success of the organization.

Many organizations in the finance and energy sectors have identified the benefits of bringing the management of credit, market and operational risks together. It has been the case for some time in the finance sector that risk management has been separate from the purchase of insurance. The development of the role of chief risk officer (CRO) reporting directly to the CEO reflects this fact.

Given that one of the key principles of risk management is that the approach to risk should be proportionate to the level of risk faced by the organization, it is unlikely that the majority of organizations will need to appoint someone of the seniority of a CRO. Nevertheless, organizations should, when reviewing their risk architecture, decide the appropriate range of responsibilities and level of seniority of the risk manager.

The introduction of the job title ‘chief risk officer’ is not universal, but it is becoming common in the specialist finance and energy sectors. The next box provides an overview of the developing role of the chief risk officer. For organizations where it is proportionate for a CRO to be appointed, the contribution that can be made by that individual will be substantial.

Role of the chief risk officer

As champion of the ERM process, the CRO plays a key part in bringing together disparate risk management processes to ensure that limited company resources are applied effectively. The COSO ERM cube defines the role of the CRO as working with other managers to establish effective risk management, monitoring progress, and assisting other managers in reporting relevant risk information up, down and across the organization.

Internal auditors should work with the CRO as part of their risk management duties. In this role, internal auditors are responsible for evaluating the accuracy of ERM reporting and providing independent and value-added recommendations to management about its ERM approach. The IIA International Standards specify that the scope of internal auditing should include evaluating the reliability of reporting effectiveness, efficiency of operations and compliance with laws and regulations.

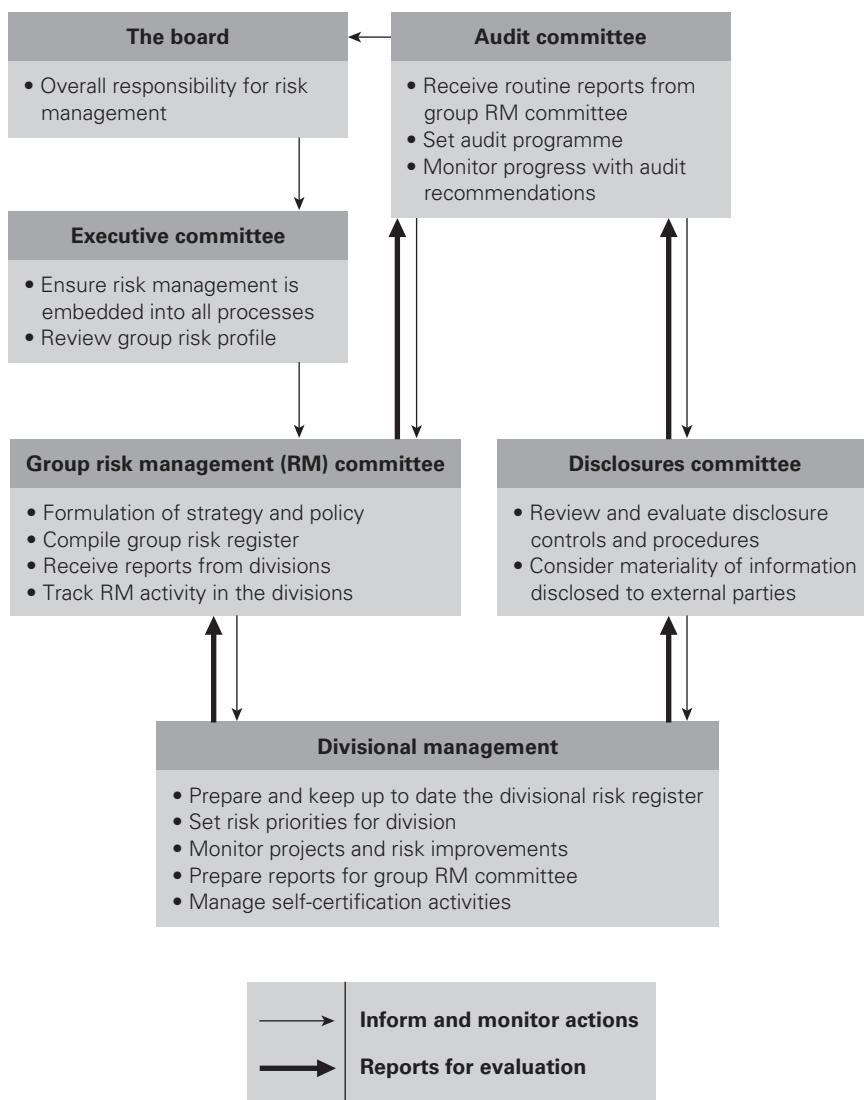
Risk architecture in practice

Figure 24.1 shows the risk architecture for a typical large corporate entity that is subject to the requirements of the Sarbanes–Oxley Act. This risk architecture should be set out in the risk management manual for the organization. Terms of reference of the various committees and a schedule of the activities should also be established, either in the risk management manual or in a calendar of risk management activities. This schedule of activities should be aligned with the other corporate activities in the organization.

For a large organization with non-executive directors, the audit committee should also be shown in the risk architecture. The role of the audit committee and the role of the head of internal audit are important in fulfilling the risk management strategy of the organization.

For organizations subject to the requirements of the Sarbanes–Oxley Act, there will also be a requirement to ensure that all information disclosed by the company is accurate. In many large organizations, this requirement has resulted in the

Figure 24.1 Risk architecture for a large corporation



establishment of a disclosures committee. The role of the disclosures committee is to check the source and correctness of all information that is disclosed by the organization. Sarbanes–Oxley requires that financial information is evaluated to a higher level of scrutiny.

The risk architecture of an organization sets out the hierarchy of committees and responsibilities related to risk management and internal control. In the structure shown in Figure 24.1, the corporate risk management committee focuses on executive risk management activities.

Risk management responsibilities for activities at divisional or unit level should be allocated to divisional management. Divisional management is responsible for co-ordinating the identification of significant risks at divisional level, compiling the risk register for the division and ensuring that adequate controls are identified and implemented.

Divisional management should be provided with guidance from the group risk management committee. If there is a divisional committee, it should be required to send reports to the group risk management committee, so that the corporate or group overview of risk management priorities can be established.

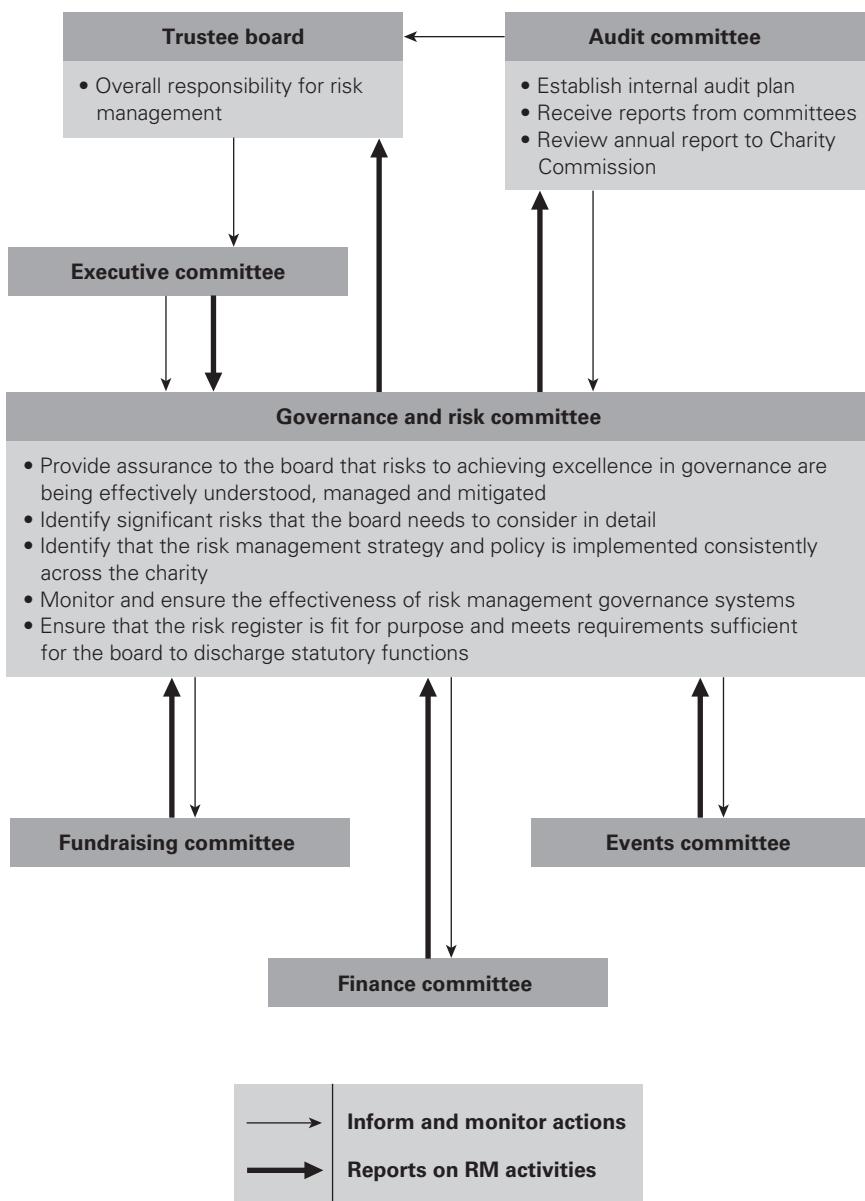
For a public sector or charity organization, the risk architecture will be somewhat different. Figure 24.2 sets out a typical risk architecture for a charity. In this case, risk management activities are focused on the governance and risk committee. The flow of information and the control of risk management activities are illustrated by the arrows in Figure 24.2.

It is clear from Figure 24.2 that risk governance for charities is a much higher-profile issue than in many other organizations. There have been reports that trustees of charities consider governance issues to be their primary concern. This implies that many trustees of charities consider that governance is more important than raising money for the charity that they support. This could be an example of concerns about risk management becoming so great that they deform the nature of the organization.

There are many ways for risk management reporting lines to be established. The reporting structure should be proportionate to the level of risk and the complexity of the organization. For high-risk organizations, such as those in the finance sector, the risk committee is likely to be a direct sub-committee of the board. In these circumstances, it is likely that the risk committee will be chaired by a senior director with other senior representation from the board.

For organizations that are not operating in such a high-risk environment, it may not be necessary for the risk committee to be a direct report to the main board. In these circumstances, the risk committee may be a sub-committee of the executive committee or the operations committee. In all cases, the corporate structure for the management of risk should be proportionate to the level of risk within the organization and the size, complexity, nature and risk exposure of the organization.

However, there are no specified correct structures for the risk architecture of an organization. Provided that the risk committee delivers the required outputs, the membership and terms of reference will be for the organization to decide. Nevertheless, the general point remains that management of risk is an executive function, whereas audit activities should be led by non-executive directors.

Figure 24.2 Risk architecture for a charity

Risk committees

Table 24.3 sets out typical responsibilities for a risk management committee (RMC). Most large organizations will already have an audit committee, chaired by a senior non-executive director. An option considered by many organizations is to extend the

Table 24.3 Responsibilities of the RM committee

- | | |
|---|--|
| 1 | To advise the board on risk management and to foster a culture that emphasizes and demonstrates the benefits of a risk-based approach to risk management. |
| 2 | To make appropriate recommendations to the board on all significant matters relating to the risk strategy and policies of the company. |
| 3 | To monitor the performance of the risk management systems and review reports prepared by relevant parties. |
| 4 | To keep under review the effectiveness of the risk management infrastructure of the company, including: <ul style="list-style-type: none"> ● assessment of risk management procedures in accordance with changes in the operating environment; ● consideration of risk audit reports on the key business areas to assess the level of business risk exposure; ● consideration of any major findings of risk management reviews and the response of management; ● assessment of the risks of new ventures and other strategic, project and operational initiatives. |
| 5 | To review the risk exposure of the company in relation to the risk appetite of the board and the risk capacity of the company. |
| 6 | To consider the development of risk management and make appropriate recommendations to the board. |
| 7 | To consider whether disclosure of information regarding risk management policies and key risk exposures is in accordance with financial reporting standards. |

role of the audit committee to include all aspects of risk management or to establish a separate risk management group chaired by an executive director.

There is a strong argument for the RMC to be an executive group, rather than part of any existing non-executive audit committee. This is necessary because risks need to be managed in a proactive manner as an executive responsibility. The audit committee may treat the management of risk as a reactive auditing of compliance. Separation of executive responsibility for the management of risk from non-executive responsibility for auditing and review of compliance will also be consistent with good corporate governance principles.

Some organizations have established the RMC as a sub-committee of the audit committee. If this is the case, actions need to be taken to ensure that risk is managed

as an executive responsibility, rather than audited as a compliance/assurance issue. In fact, establishing the RMC as a sub-committee of the audit committee could impair the work of the RMC because of increased bureaucracy and an unhelpful emphasis on auditing and compliance, rather than proactive management of risks.

Membership of the RMC is another question that needs to be addressed. The fundamental decision to be taken in large organizations is whether the committee should be a small senior executive group setting strategy and policy or whether it should be a knowledge-sharing group with representation from each of the units or departments within the organization. The answer will depend on the structure of the organization and the intended role of the committee.

The terms of reference and the position of the risk committee within the risk architecture of the organization have been the subject of much discussion. For some business sectors, the level of risk that the organization should take is a fundamental business strategy decision. This is certainly true in banks and other financial institutions. In these circumstances, deciding on a risk appetite and the monitoring of actual risk exposure becomes a high-profile board responsibility. Therefore, the risk committee will need to be a committee of the board with executive and non-executive membership.

The terms of reference of the risk committee and its position within the risk architecture are fundamentally important decisions for any organization. In all circumstances, the arrangements should be appropriate for the organization and aligned with business activities. Also, the nature of the risk committee will need to be appropriate and proportionate within the external, internal and risk management contexts of the organization.

There is no single answer that is appropriate for all organizations. In many cases, a separate risk management committee may not be proportionate to the level of risk faced by the organization. In these cases, the responsibilities that would have been undertaken by a risk committee will still need to be allocated to a committee of appropriate seniority. Some organizations allocate risk management responsibilities to the executive committee or the finance committee of the board.

The overall aim is to achieve a prioritized, validated and audited improvement in risk management standards in the organization. The risk management committee and the audit committee should, therefore, operate in a way that provides mutual support. However, combining the two committees into a single group, or placing one committee as superior to the other will not be the best way forward for most organizations. The major concern when combining risk and audit committees is that the organization will then be operating a two lines of defence model, rather than the three lines of defence model that will provide greater protection.

Culture and behaviours 25

Styles of risk management

We have already seen that there are four (complementary) styles of risk management, related to the nature of the risk under consideration. We identify the features of each in Table 25.1. To some extent, they define and describe the level of sophistication that is applied to risk management by an organization at a point in time.

The type of risk under consideration helps determine the style of risk management that will be applied. The measurements shown in Table 25.1 are the values that the organization is willing to put at risk, other than for compliance risk where there will be no tolerance to illegality. The hazard tolerance, control acceptance and opportunity investment added together will comprise the risk appetite of the organization and represent the total acceptable risk exposure of the organization. The total risk exposure is the sum of the risk exposures for the individual risks and this actual risk exposure may differ from the risk appetite of the board and/or the risk capacity of the organization.

Steps to successful risk management

Any sustained improvement in the risk management performance of an organization will require a planned approach. The nature of the plan will depend on the size, complexity and nature of the organization. There is no single correct approach to implementing risk management in an organization. The drivers for undertaking risk management and the expected outputs and impacts will vary between organizations.

Although there is no single correct approach, Table 25.2 sets out some of the key steps in achieving successful risk management.

The initial, and perhaps most important, step is ensuring that the risk management initiative is sponsored by a member of the board or a senior member of the executive committee of the organization. This support is likely only when the last step has been communicated and agreed: that implanting an ERM approach will contribute to the success of the organization. Information on the successful

Table 25.1 Styles of risk management and their features

Style	Main feature	Measurement	Key business area	Example application	Developed
Compliance	Legal obligations	Pass or fail	Group legal or health and safety	Interface with regulators Guarding of machinery	1970s
Hazard	Negative	Hazard tolerance	Insurance procurement	Managing motor vehicle losses Reducing premium spend	1980s
Control	Cost	Control acceptance	Internal audit	Avoidance of internal fraud	1990s
Opportunity	Positive	Opportunity investment	Strategic planning	Review of a merger or acquisition	2000s

Table 25.2 Achieving successful enterprise risk management

- 1 Engage senior management and board of directors to provide organizational support and resources.
- 2 Establish an independent ERM function reporting directly to a board member.
- 3 Establish the risk architecture at executive and board levels, supported by internal audit.
- 4 Develop the ERM framework that incorporates an appropriate risk classification system.
- 5 Develop a risk-aware culture fostered by a common language, training and education.
- 6 Provide written procedures with a clear statement of the risk appetite of the organization.
- 7 Agree monitoring and reporting against established objectives for risk management.
- 8 Undertake risk assessments to identify accumulations and interdependencies of risk.
- 9 Integrate ERM into strategic planning, business processes and operational success.
- 10 Contribute to the success of the organization by delivering measurable benefits.

introduction of a risk management initiative is also available in the various risk management standards and frameworks discussed throughout this book.

As risk management changes and develops, the steps that will be taken by different organizations will change. With the emergence of governance, risk and compliance (GRC), the risk management context has also changed. Risk management professionals need to be aware of these developments and ensure that their activities are always fully aligned with the other activities within the organization.

Although it is important to have an overall plan relating to the implementation of any risk management performance improvement, it is also vital that the risk manager identifies barriers to the implementation of the initiative in some detail. The potential barriers and enablers to the successful implementation of a risk management initiative are set out in Table 25.3. There are many factors that will influence the effectiveness of the approach, including:

- senior management influence within departments;
- external influences, including corporate governance;
- nature of the business, its products and culture;
- corporate attitudes, including previous RM experiences;
- legacy of previous risk management initiatives.

Table 25.3 Implementation barriers and actions

Barrier	Action
Lack of understanding of value of risk management	Establish a shared understanding, common expectations and a consistent language of risk in the organization
Belief that risks management will suppress entrepreneurship	Encourage a positive approach as an enabler of business actions
Lack of support and commitment from senior management	Identify a sponsor on the main board of the organization and confirm shared and common priorities
Seen as just another initiative, so relevance and importance not accepted	Agree a strategy that sets out the anticipated outcomes and confirms the benchmarks for anticipated benefits
Benefits not perceived as being significant	Complete a realistic analysis of what can be achieved and the impact on the mission of the organization

(continued)

Table 25.3 (Continued)

Barrier	Action
Not seen as a core part of business activity and too time-consuming	Align effort with core processes and achievement of the mission of the organization
Approach too complicated and over-analytical (risk overkill)	Establish appropriate level of sophistication for risk management framework and undertaking risk assessments
Responsibilities unclear and any external expenditure agreed (ie external consultants) resented	Establish agreed risk architecture with clear roles and accepted risk responsibilities
Risks separated from where they arose and should be managed	Include risk management in job descriptions to ensure that risks are managed within the context that gave rise to them
Risk management seen as a static activity not appropriate for a dynamic organization	Align risk management effort with the mission of the organization and with the business decision-making activities
Risk management too expansive and seeking to take over all aspects of the company	Be realistic: do not claim that all the business activities within the organization are risk management by another name

Identification of barriers, as set out in Table 25.3, leads to the ability to put in place actions to overcome them. These include the fact that successful risk management requires the commitment of all parties and that implementation will only be as good as the least committed member of a department. Analysis of these barriers within the context of the specific organization will lead to the identification of the best options to ensure that risk management delivers the optimum benefits.

There is no single action that will ensure adequate implementation and no single timeframe by which implementation will be fully achieved, although experience indicates a two- and five-year time horizon is realistic.

One of the important considerations regarding the timeframe for implementation will be the documentation methodology. If a comprehensive risk management information system (RMIS) is to be introduced, the timescale for successful and complete implementation may be extended.

Defining risk culture

The culture of an organization is difficult to define. However, it is generally accepted that it is a reflection of the overall attitude of every component of management

within a company. The culture of an organization determines how individuals will behave in particular circumstances. It will define how an individual feels obliged to behave in all circumstances.

A good risk culture will be the product of individual and group values and of attitudes and patterns of behaviour. This will lead to a commitment to the risk management objectives of the organization. Organizations with a risk-aware culture are characterized by communication founded on mutual trust and a shared perception of the importance of risk management. There also needs to be a sharing of confidence in the selected control measures and a commitment to adhering to the established risk control procedures.

Table 25.4 sets out the suggested components of a risk-aware culture. These components are suggested by recent UK Health and Safety Executive (HSE) research as leadership, involvement, learning, accountability and communication. This makes the acronym LILAC. Creating a culture where effective risk management is an integral part of the way people work is a long-term aim for most organizations.

If an organization decides to raise awareness of security issues, it may decide to launch a campaign to focus on the risks and the relevant controls. The campaign should use more than one means of communication if it is to be successful. The awareness campaign could include all of the LILAC components and may extend to, for example:

- risk awareness training;
- awareness poster campaigns;
- site inspections;

Table 25.4 Risk-aware culture

A risk-aware culture is achieved by LILAC	
Leadership	Strong leadership within the organization in relation to strategy, projects and operations
Involvement	Involvement of all stakeholders in all stages of the risk management process
Learning	Emphasis on training in risk management procedures and learning from events
Accountability	Absence of an automatic blame culture, but appropriate accountability for actions
Communication	Communication and openness on all risk management issues and the lessons learnt

- arrangements for reporting defects;
- leaflets and brochures;
- awards for success sponsored by the CEO.

A risk management initiative cannot be successful unless the culture of the organization is receptive to it. In order to be receptive, a risk-aware culture is required in the organization. A high level of maturity in relation to leadership will require senior management to actively promote a risk-aware culture and act in ways that support this. This will include setting risk management performance targets and ensuring that the commitment of senior management to the risk-aware culture is clear. This will require verbal and written communications.

The active involvement and participation of senior management is a necessary component of achieving a risk-aware culture. Involvement can be achieved by adequate training, so that ownership of risks is fully understood. Specialist risk functions should play an advisory or consultancy role. There should be feedback mechanisms in place to inform staff about any decisions that are likely to affect them.

The existence of a learning culture is vital to the success of a risk-aware culture. A learning culture enables organizations to learn, and to identify and change inappropriate risk behaviour. In-depth analysis of incidents and good communication of feedback enables a learning culture to develop. Workshops on risk issues are another key component of a learning culture.

Embedding risk management

Many educational institutions have set up committees to oversee the implementation of risk management practices and procedures. Often these are management committees, although they can sometimes be supported by members of the governing body.

One institution has established a group to advise on the development of risk management processes. Significantly, this group includes academics from the institution's business school, tapping into existing expertise. This practice is evident at another institution, where the group includes an academic expert in risk management from the local business school.

As risk management processes become embedded within the daily routines and management of the institutions, these committees will evolve or be replaced. Institutions with more effective risk management processes have increasingly charged their senior management teams with this role, rather than establishing separate committees. In such cases, risk management processes have become more effectively embedded because the senior management team is in a better position to identify and manage risk, and to promote risk management.

Accountability is vitally important if the risk-aware culture is to be successful. However, it is not the same as a blame culture. The organization should ensure that it moves from a blame culture to a non-discriminatory culture based on accountability. When investigating incidents, management should demonstrate care and concern towards employees. Employees should feel that they are able to report issues and concerns without fear that they will be blamed or disciplined personally.

A risk-aware culture requires good communication of risk information from senior management. Good communication also requires that reports from all employees, as well as reports from outside the organization, are welcome and well received. Information on risk performance should be included in the communication activities.

The next box provides an example of risk awareness and the embedding of risk management into the culture of an organization.

Risk awareness campaign

The embedding of risk management into the organization has been undertaken by following three routes: a risk awareness campaign, the implementation of new risk identification processes at directorate level, and the ongoing development of existing risk processes at a strategic level.

The primary aim of the awareness campaign was to make staff realize their responsibilities towards risk, whilst at directorate level the introduction of risk registers has been collaborative and inclusive. Strategically, further development of the corporate risk register aims to bring tighter control of risk and provides comprehensive evidence and assurance to the board that risks are managed.

Measuring risk culture

It can be difficult for an organization to gauge risk culture but this area is so important that measurements need to be taken. Audit committees will often ask how seriously a department or location takes risk management. In general, it will be easy to answer this question on a qualitative basis by reviewing the quality of the policy and details of the procedures contained in the risk guidelines or protocols. This will give an indication of the risk culture of the organization.

However, quantitative measurements are required, to identify and focus on areas of weakness to enable improvement actions to be planned. Frameworks for measuring culture can be found in, for example:

- audit committee evaluation;
- level of risk maturity;
- the Canadian criteria of control (CoCo) framework.

A later section of this chapter considers risk maturity models in more detail. Quantitative measures that indicate the level of risk maturity can be taken and areas for improvement can then be identified.

For many organizations, improvement in the risk culture is a valid strategic risk objective. This will be especially true when areas of weakness in the level of risk awareness have been identified.

When undertaking actions to improve the risk culture within an organization, it is important to acknowledge that improving the risk management processes must lead to improvements in risk management outputs. This, in turn, should have a positive impact that delivers greater benefits from risk management.

There is little point in improving the risk management processes as a means of improving the risk culture of the organization if the overall effectiveness of the risk management effort is not enhanced. There is a danger that enhancing and improving the risk management process in an organization is automatically assumed to have improved the risk culture.

It is possible for the risk management process to be enhanced without the risk culture of the organization being improved. For example, a more aggressive internal audit programme may improve compliance standards, but that does not guarantee that the risk culture of the organization has been enhanced. Improvements to the risk management process may not deliver any additional benefits, whereas improvements to the risk culture should be expected to provide an enhanced level of risk assurance.

ISO 31000 places considerable importance on context, and this is illustrated in Figure 4.2. Information is provided in the standard on the importance of the external context, internal context and risk management context for the organization. Context is closely related to risk management culture and the benefits that will be derived from enhanced risk management within the organization.

The Canadian criteria of control (CoCo) framework of internal control concentrates on the control environment in an organization. Additionally, the COSO ERM cube (2004) refers to the internal environment of the organization, rather than the control environment that is described in the COSO internal control cube (2013). The control environment and the internal environment are measures of the risk culture and the level of risk awareness within the organization.

An overall improvement in risk performance will be achieved through improvements in the internal context, risk management context, control environment or internal environment. The level of risk maturity, the achievement of a risk-aware culture and the fulfilment of the LILAC criteria set out in Table 25.4 are all means of improving the control or internal environment.

During the 1990s, a system called the balanced scorecard became a popular management tool. This is a management system that enables organizations to clarify their vision and strategy and translate them into action. Many large organizations use balanced scorecards as a means of establishing context for the various initiatives that

are undertaken within the organization. The government agency used as the basis for Figure 29.2 is an example of an organization that uses the balanced scorecard.

If an organization uses the balanced scorecard, it is sensible to use the same framework for risk management activities. When risk management processes and procedures are compatible with existing activities, the risk management requirements are more likely to be accepted and fulfilled. This represents an alignment of risk management activities with existing protocols, in order to embed risk management in the organization and create a more risk-aware culture.

Alignment of activities

Risk management activities and the risk architecture, strategy and protocols should be aligned with the core business processes within the organization. Risk information flows around the risk management framework and (if successful) this will produce various outputs. These outputs have already been described as mandatory obligations fulfilled, assurance provided, decision making enhanced and effective and efficient core processes achieved (MADE2).

Most risk management standards make reference to the upside of risk or discuss the management of opportunity risks. Project risk management, or the management of control risks, has become a separate discipline within risk management, and project risk management has become well developed, with separate guidance material.

When considering the contribution that risk management can make to the organization, it is important to decide whether the contribution will relate to strategy, projects and/or operations. This decision will enable the risk management activities within the organization to be aligned with the other business operations, activities and imperatives.

It is important that risk management activities are aligned with other operations, so that the risk management procedures can be fully embedded into the existing management procedures and activities within the organization. This will also ensure that risk management activities are undertaken in an efficient and embedded manner and are not seen as a separate activity detached from management of the organization.

There should also be alignment of the activities of internal audit with the culture or context of the organization. The approach followed by internal audit when deciding to design a risk-based audit programme has two components. Firstly, internal audit will look at the high-risk activities and focus the audit programme on those activities. Secondly, the risk-based audit programme will take account of the level of risk management maturity across the organization. If part of the organization has a less risk-mature approach, then internal audit may decide to undertake an increased amount of audit activity in that part of the organization.

Another measure of how well-embedded enterprise risk management is within an organization can be represented by the fragmented, organized, influential and leading (FOIL) approach. Table 25.5 describes the four stages of risk maturity (as identified by the 4Ns: naïve, novice, normalized and natural) and the characteristics associated with the FOIL approach, and it can be seen that the influence of enterprise risk management increases as the four levels are implemented.

A fragmented (or siloed) approach to enterprise risk management is present when different risks are managed in different departments by specialists who do not necessarily work together. For example, an organization can have excellent health and safety, security and business continuity standards, but the benefits of working together may not have been established. The next stage is for these activities to become co-ordinated, so that the approach to enterprise risk management becomes more organized. All risks are then considered together and the result is likely to be a comprehensive risk register.

Table 25.5 Four levels of risk maturity

Level	Status (4Ns)	Characteristics (FOIL)
1	Naïve	Fragmented
	Level 1 organizations are unaware of the need for enterprise risk management and/or do not understand the benefits that will arise.	Risk management activities are fragmented and focused on legal compliance activities, such as health and safety.
2	Novice	Organized
	Level 2 organizations are aware of the benefits of enterprise risk management, but have only just started to implement an ERM initiative.	Actions are planned to co-ordinate risk management activities across all types of risk, although plans may not have been fully implemented.
3	Normalized	Influential
	Level 3 organizations have embedded ERM into business processes, but management effort is still required to maintain adequate ERM activities.	Embedded ERM processes are influencing processes and management behaviours, but this may not yet happen consistently or reliably.
4	Natural	Leading
	Level 4 organizations have a risk-aware culture with a proactive approach to ERM and risk is reliably considered at all stages to gain competitive advantage.	Consideration of risk is a substantial factor in making business decisions, and strategy decisions are led by ERM considerations.

However, there is more benefit to be gained from enterprise risk management. Organizations that establish ERM activities that are influential on decision making gain these additional benefits. Risk management (and the risk manager) influence decision making and ensure that risk-related issues are taken fully into account as strategy and tactics are developed. The final stage is for risk management to lead the development of strategy and tactics within the organization. This will require the risk manager to be part of a senior management team, so that the development of strategy and tactics is led by risk considerations, rather than the risk implications being considered after the strategy and tactics have been decided.

Risk maturity models

Increases in risk management effectiveness can also be measured by the use of risk maturity models. The level of risk management sophistication provides an indication of the benefits that can be achieved from risk management. The level of risk maturity in the organization is a measure of the quality of risk management activities and the extent to which they are embedded within the organization.

Risk maturity models can be used to measure the current level of risk culture within the organization. The greater the level of risk maturity, the more embedded risk management activities will become within the routine operations undertaken by the organization. The hallmarks of successfully embedded risk management are considered later in this chapter.

Risk maturity is not the same as considering the level of sophistication that an organization achieves in respect to risk management. An organization may have limited expectations of risk management, but nevertheless have a very mature approach to the way in which it seeks to obtain the available benefits. The level of risk maturity within an organization is an indication of the way in which risk processes and capabilities are developed and applied. In an immature organization, informal risk management practices will take place. This may include a blame culture that leaps into action when things go wrong, potentially avoiding accountability for risk. Also, resources allocated to manage risks may be inappropriate for the level of risk involved.

When explicit risk management is in place, there will be attempts to keep the processes dynamic, relevant and useful. There is likely to be open dialogue and learning so that information is used to inform judgements and decisions about risks. There will be confidence that innovation and risk-taking can be managed, with support when things go wrong.

When an organization or an industry sector becomes obsessed with risk, there will be over-dependence on process, and this may limit the ability to manage risk effectively. There will be over-reliance on information at the expense of good

judgement, and dependence on process to define the rationale behind decisions. Individuals may become risk-averse for fear of criticism and procedures are followed only to comply with requirements, not because benefits are sought.

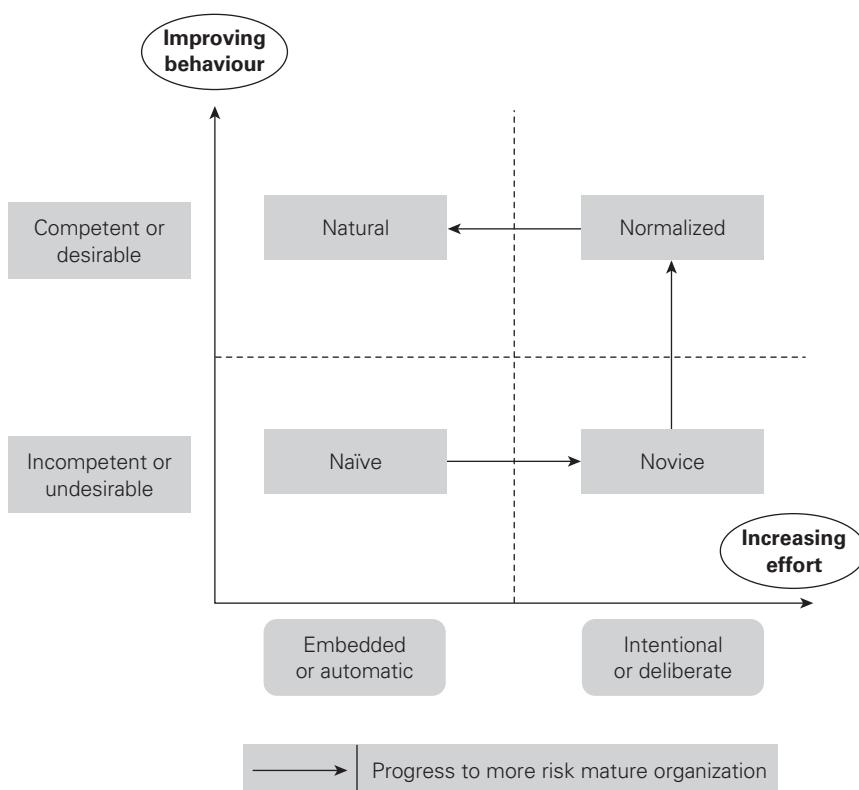
Table 25.5 sets out a system for determining the level of risk maturity within an organization with regard to risk management processes. This table sets out four levels of risk maturity, the 4Ns of naïve, novice, normalized and natural. The characteristics of each of these levels are described in the table. Table 25.5 also aligns the 4Ns model with the FOIL methodology for describing the level of risk maturity in an organization. Clearly, it is better for an organization to seek a higher level of risk maturity. However, the approach to achieving risk maturity in the organization should be proportionate to the level of risk that the organization faces.

The level of risk maturity within an organization will help define the level of sophistication that the organization has in its risk management activities. Figure 3.2 discusses the level of sophistication of the contribution that risk management can make to company activities. The greater the level of risk management sophistication achieved by an organization, the greater the benefits. Achieving an improved level of maturity in relation to risk management processes does not necessarily guarantee that a greater level of sophistication will be achieved, or that a higher level of benefits will be obtained.

Nevertheless, achieving an improved level of risk maturity may be one of the strategic aims for risk management within the organization. If that is the case, an established framework for measuring risk maturity is required. It is important that the organization uses a risk maturity model that aligns with its own ambitions in relation to risk management maturity and provides a practical approach that can be embedded within the organization.

Figure 25.1 provides an interpretation of the level of risk maturity of an organization, based on the 4Ns model. The figure suggests that there is a relationship between whether behaviour is embedded or automatic on the one hand, against competent or desirable on the other. A naïve organization will automatically accept incompetent or undesirable behaviours. A novice organization will become aware that the behaviours are incompetent or undesirable and will have started to make an effort to improve behaviour, but it will not yet have achieved change. However, as change is achieved, it will move towards improved normalized behaviours.

The status achieved by an organization with the natural state of risk maturity is that competent or desirable behaviours will automatically occur, with little management effort or enforcement. The achievement at this point is to ensure that behaviours are also consistent. One of the primary reasons for producing risk management policies and procedures is to ensure that appropriate behaviours are consistently achieved. Ensuring consistent desirable behaviours is one of the primary objectives of a risk management initiative.

Figure 25.1 Risk maturity demonstrated on a matrix

The normalized organization is successful in achieving competent or desirable behaviours, but these are not yet automatic. When the organization reaches the stage of being a natural in risk management, then the competent or desirable behaviours will become unconscious or automatic. This model provides a means of illustrating the four levels of risk maturity (4Ns) on a matrix and also indicates that the decline from natural behaviour back to naïve may be a short step for organizations that do not put sufficient effort into maintaining their level of risk maturity.

Several types of risk maturity approaches are in existence, including the criteria of control framework. The approach adopted by the CoCo framework focuses very heavily on the importance of risk maturity. The approach of this internal control framework is that if the risk culture and the risk architecture, strategy and protocols are correct then good levels of risk management and internal control will be achieved. Another risk maturity model that is frequently used is the European Foundation for Quality Management model.

Finally, the similarities between Figures 3.2 and 25.1 are worth considering. There is a need to inform a naïve organization and reform a novice organization. A normalized organization will conform with requirements and a natural organization will be successful and perform.

Risk appetite and tolerance 26

Nature of risk appetite

Risk appetite is the immediate or short-term willingness of an organization to undertake an activity that involves risk, be that a threat or an opportunity. It is a vitally important concept in the practice of risk management. However, it is difficult to precisely define and apply in practice.

One of the fundamental difficulties with the concept of risk appetite is that, generally speaking, organizations will have an appetite to continue a particular operation, embark on a project or embrace a strategy, rather than a direct appetite for the risk itself. Most risk management standards say that risk should be managed within its context and, as such, an organization's risk appetite can only be answered within the context of the strategy, tactics, operations and compliance activities. Decisions on risk appetite should be taken within the context of other business decisions, rather than as a stand-alone evaluation.

Risk appetite is the total value of the corporate resources that the board of the organization is willing to put at risk. Most organizations have not determined the value they should risk (risk appetite), nor calculated how much value is actually at risk (risk exposure), nor the capability of the organization to take risk (risk capacity). A range of definitions of risk appetite is shown in Table 26.1, all of which show similarities.

An organization should be able to decide how much it wishes to put at risk, based on its attitude to risk. Agreeing the risk appetite will ensure that the organization does not put too much (or too little) value at risk. The risk capacity of the organization needs to be fully understood and utilized to ensure that risk taking is at the optimal level and delivers maximum benefit. Similarly, the organization should not put more value at risk than is appropriate, given the sector in which it operates and prevailing market conditions.

The portion of risk appetite that is associated with opportunities is the opportunity within the investment that the organization is willing to embrace. Organizations will be willing to invest resources in opportunities if it is felt they are likely to produce

Table 26.1 Definitions of risk appetite

Organization	Definition
IRM (2011)	The amount of risk that an organization is willing to seek or accept in the pursuit of long-term objectives.
ISO Guide 73 (2009)	The amount and type of risk that an organization is willing to pursue or retain.
Risk Appetite Guidance note HMG (2020)	The level of risk with which an organization aims to operate.
CIIA (2005)	The level of risk that is acceptable to the board or management. This may be set in relation to the organization as a whole, for different groups of risks or at an individual risk level.

a positive gain. However, it should be recognized that value put at risk in this way could also destroy value, and may result in losses. Incorrect strategic decisions have destroyed more value than hazard, control or even compliance risks.

The organization may have an appetite for investing resources in an opportunity, but it needs to be sure that it has the capacity to endure any loss that may result. It also needs to be sure that the total amount invested, or value at risk, is not beyond the capacity of the organization. The example of RBS's ill-fated takeover of ABN Amro in 2007 is an example of a firm overreaching its ability to absorb such an investment. Careful identification of the nature of the risks and calculation of the actual risk exposure associated with the opportunity should be undertaken.

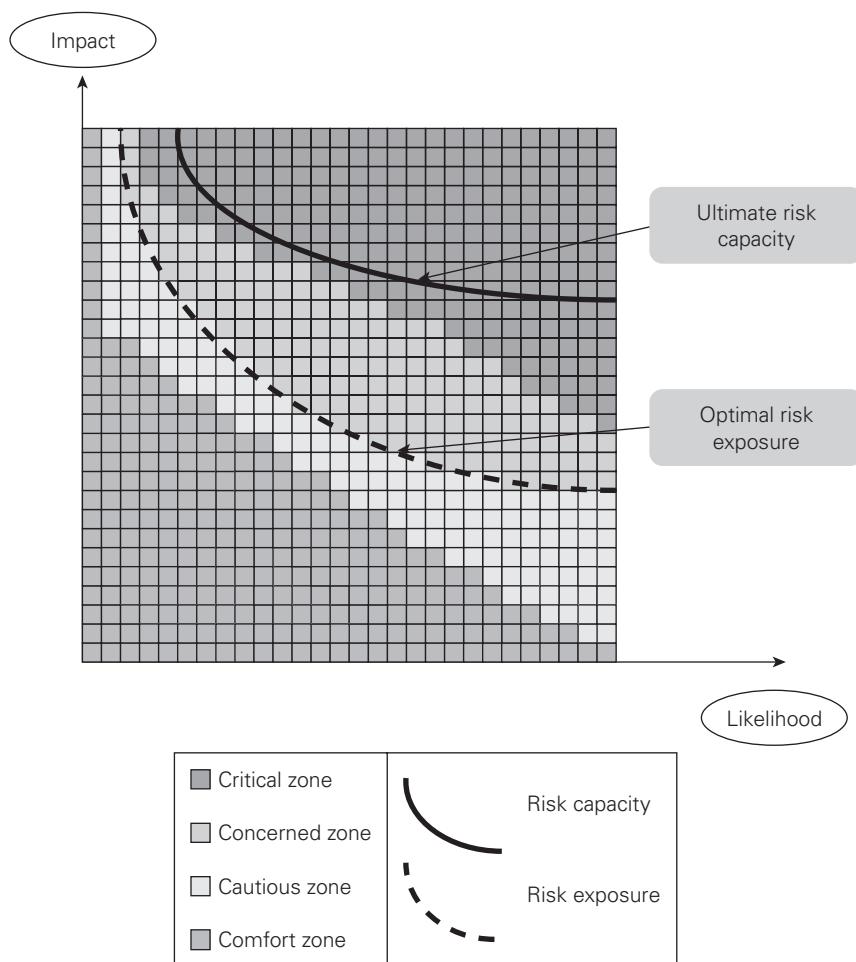
Risk appetite and the risk matrix

Figure 26.1 illustrates the concepts of risk appetite, risk exposure and risk capacity. Risk appetite is illustrated by way of shaded squares on the risk matrix and the overall risk exposure of the organization is shown as a curved line. This illustration represents risk appetite, exposure and capacity for a risk-averse organization.

The medium-shaded area represents a situation where the organization is comfortable with taking the risk. The lighter areas represent the cautious and concerned zones, where management judgement is required before the risk is accepted. The risks shown in the darkest area are critical risks, and these risks will only be accepted when there is a business imperative.

The curved lines in Figure 26.1 represent the overall risk exposure of the organization and this is the optimal position, where the overall exposure cuts through the lighter section. The risk capacity of the organization is shown as higher than both the

Figure 26.1 Risk appetite, exposure and capacity (optimal)



risk appetite and the risk exposure and is embedded well within the darker area. This represents an optimal state of affairs. This ensures that the organization is taking risks that are within the appetite of the board and not exceeding its ultimate risk capacity.

Total cost of risk calculations were commonplace in the 1980s and were often undertaken by organizations or their insurance brokers. They enabled an organization to determine the total cost of hazard risks to the organization and comprised insurance premiums, cost of claims not covered by insurance, and money spent on loss-control actions. Tables were published on the total cost of risk in various organizations, and it was possible to benchmark the performance of an organization against other companies in the same sector. This type of risk calculation was often used as a justification for setting up an in-house or captive insurance company, as discussed in Chapter 18.

The difficulty with this type of calculation is its ‘backward-looking’ nature, as it depends on historical information, which is not necessarily a good guide to future loss performance. This approach also drives organizations to seek the lowest immediate cost for the management of hazard risks, rather than an optimized approach across time.

Organizations should be aware of the limitations of these total cost of risk calculations which only apply to the management of hazard risks in relation to insurance purchase. Buying too much insurance could represent the lowest risk position for the organization but will be achieved at a high overall cost.

The type of total cost of risk calculation that is now undertaken by organizations is somewhat different. It consists not just of those risks that can be insured, but will include all types of risks. The actual risk exposure in this calculation is used to identify the level of risk that the organization is willing to accept. The risk appetite of the board can then be compared with the actual risk exposure that the organization faces.

As discussed in the introduction and throughout this book, it should be recognized that the business environment is more volatile and processes undertaken by public sector or other bodies are being disrupted by the opportunities that technology presents. Under these conditions, all organizations are forced to increase their risk exposure. As a consequence, risk management has become more important and boards of organizations are faced with the reality of increasing the total value that they are willing to put at risk or to find mechanisms to reduce the total risk exposure.

When an organization decides whether to embark on a merger or acquisition, its risk exposure will be affected. Organizations need to undertake an opportunity analysis of all acquisition opportunities, and this analysis should include consideration of at least the following features of the acquisition opportunity:

- financial strength and reputation of the proposed acquisition;
- potential for developing further revenue/profit from the acquisition;
- risks associated with suggested purchase contract terms and conditions;
- anticipated profitability and sustainability of the proposed acquisition;
- investment required to deliver the anticipated future plans for the acquisition;
- impact on existing investment and business development plans.

Risk exposure is the cumulative total at risk, but is often calculated on a risk-by-risk basis, without consideration of whether the risks are correlated. When calculating the total actual risk exposure of the organization, it is important that the cumulative total of the values at risk is adjusted to take account of whether risks show any correlation.

Risk and uncertainty

There will be a range of outcomes for different risk exposures. In relation to opportunity investment, this will range from complete loss of the invested resources to a substantial gain. Sometimes, the losses may exceed the initial investment if the total negative risk exposure associated with the investment is not correctly calculated.

An organization may decide that it has a risk appetite such that it is willing to tolerate a hazard risk at a certain level as part of its normal operations. In setting a risk appetite, the organization will realize that a range of outcomes for that risk appetite is possible. This range can be analysed at various confidence levels. There will be a cost associated with this risk, both in terms of the cost of incidents that do occur and also in terms of the cost of loss-prevention, damage-limitation and cost-containment activities, including insurance costs. For each hazard risk, there will be a range of possible outcomes, all of them negative.

The organization will need to quantify the possible hazard risks and costs associated with those risks. It should be able to decide how much hazard risk it will tolerate, and this is part of the total risk appetite. Although the organization may decide how much hazard risk it will tolerate, the actual exposure to hazard risks may be greater than anticipated. Many hazard risks are subject to legislation and organizations therefore face the compliance risks associated with that regulated hazard. Almost all organizations tend to have a zero-risk appetite for non-compliance with legislation.

All organizations face uncertainties and the control risks that give rise to these uncertainties. These are risks linked to events that, if they materialize, will have uncertain outcomes. As an example of control risks, if all fraud controls in an organization were removed, there would be a net saving represented by the cost of the controls. However, this may result in an increase in unidentified fraudulent behaviours and substantial losses might be suffered, but there would be uncertainty about how much fraud would actually result from the removal of all controls.

There will be control risks embedded within the projects that the organization is currently undertaking. The cost of necessary controls may be part of the overall budget for a project. When planning a large project, it would be unwise not to include the cost of necessary controls in the budget for the project. The cost of the controls within the project budget represents the control acceptance of the organization.

Risk exposure and risk capacity

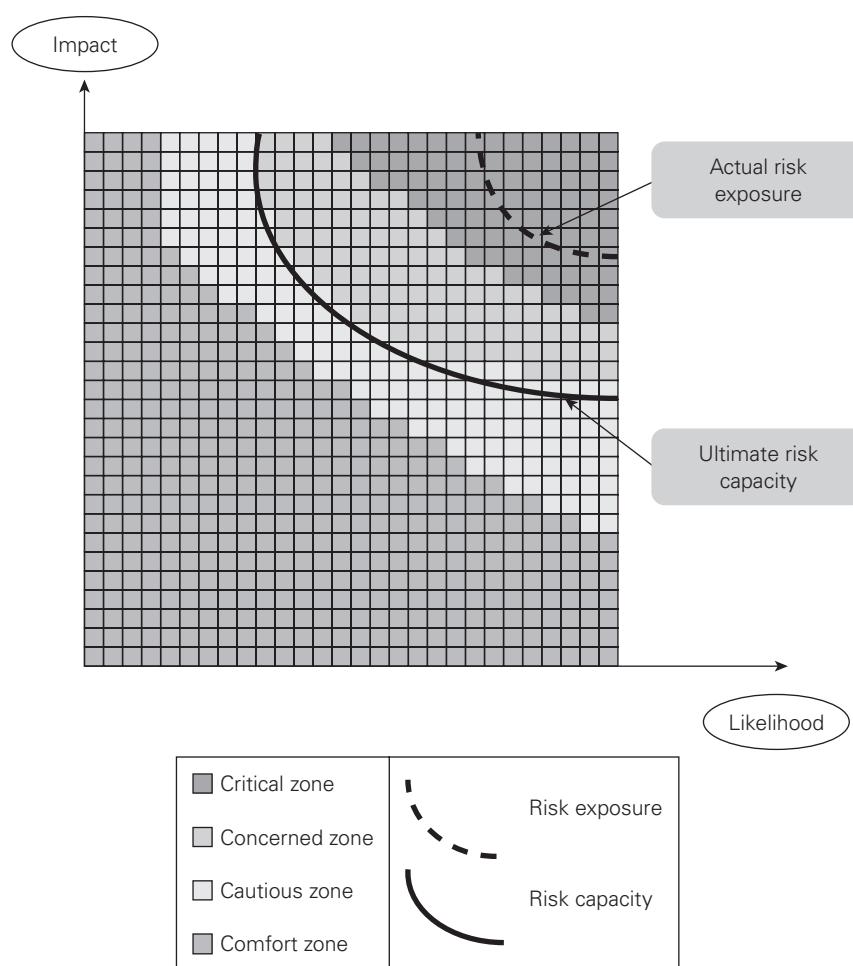
Figure 26.2 represents a risk-aggressive organization with a much larger comfort zone for accepting risk than the organization represented in Figure 26.1. The cautious

and concerned zones are smaller and the darkest zone is an even smaller part of the overall matrix. This situation can be described as representing an approach that has a very limited universe of risk. The universe of risk for the organization is represented by the darkest squares and it is only in this area that the board of the organization will consider that the risks are significant.

The organization represented in Figure 26.2 has a greater risk appetite simply because it has a more aggressive attitude to risk. By adopting a more aggressive attitude to risk, the organization will have fewer risks in the critical zone. In this case, the ‘universe of risk’ for the board of the organization will be very restricted. The ‘universe of risk’ shown in the diagram represents those risks that will be considered at board level. It can be seen in Figure 26.2 that a risk will have to be of very high likelihood and impact before it receives boardroom attention.

In Figure 26.2, the ultimate risk-bearing capacity of the organization is shown as within the lighter-shaded zones. This represents a situation where the organization

Figure 26.2 Risk appetite, exposure and capacity (vulnerable)



may be taking risks that are beyond the ultimate risk capacity of the organization. To make circumstances worse, the actual risk exposure of the organization is shown as well within the darkest area. This makes the organization vulnerable to risk, because its actual risk exposure is shown to be well beyond its ultimate risk-bearing capacity.

The identification of the risk appetite for the organization requires judgement, and this judgement can be exercised at different levels within the organization. Consideration of risk appetite will be a strategic driver at board level. Risk appetite is likely to be an operational constraint at line-manager level because line managers will be expected to operate within the risk appetite policy that has been established by the board.

At the individual level, it is likely that consideration of risk appetite will be a behaviour regulator. This is because individual members of staff should only operate within the risk appetite framework that has been developed at board level and is implemented by line managers.

The definition and application of the concept of risk appetite remains a considerable difficulty for risk management practitioners. It is the case that many current risk management standards, as well as those that are under development, all state that organizations should recognize their risk appetite at an early stage. Although ISO 31000 does not explicitly use the phrase 'risk appetite', it suggests that an organization should establish the risk criteria at an early stage.

There can be no doubt that the topic of risk appetite will receive more attention in future, and risk management practitioners need to get a better understanding of what this concept means and how it can be applied. Organizations, just like individuals, do not actively seek risk. An individual may be described as a risk taker, but the reality will be that such a person enjoys activities that have a high level of risk attached. It is the activity that appeals to the individual in the first instance, not the actual risk. People may be identified as risk takers because they have a high-risk hobby or pastime. That does not mean that the risk taking for this individual will extend to crossing a busy road without looking. In other words, risk taking has to be seen within the context of the activity and the intended rewards.

Organizations are similar in that it is the strategy, project or activity that appeals to the board, not the actual risk. An organization may embark on a risky strategy, approve a risky project or be operating risky activities or core processes. However, it is the business drivers and imperatives that are the primary concern for board members, not the level of risk involved. It is more often the case that the level of risk comes with the defined strategy, rather than the risk appetite defining the strategy.

Risk appetite statements

Risk appetite can be a driver of strategy, a planning guide for tactics or a set of operating constraints. It will normally relate to a range of possible outcomes which can be considered as zones of risk exposure or levels of risk. This may be referred to as the risk tolerance range for exposure to that particular risk. COSO ERM (2004) defines risk tolerance as:

The acceptable level of variation relative to achievement of a specific objective, and often is best measured in the same units as those used to measure the related objective. In setting risk tolerance, management considers the relative importance of the related objective and aligns risk tolerances with risk appetite. Operating within risk tolerances helps ensure that the entity remains within its risk appetite and, in turn, that the entity will achieve its objectives.¹

For some organizations, risk appetite may be a driver of strategy. This will be true for organizations such as banks and other financial institutions. For banks, risk is at the heart of the business and the appetite of an organization to, for example, lend money to particular companies or groups of people will be a reflection of its risk appetite and will be the main driver of the business. If risk appetite is a driver of the business, then the organization will wish to embrace risk in order to gain the benefits.

For other organizations, risk is not a driver of the business, but it is a consequence of the strategy, tactics, operations and compliance core processes that the business undertakes. In this case, risk appetite is unlikely to be a driver for the business but will be a planning mechanism for the organization to decide whether it wishes to adopt certain tactics, given the risks that would be embedded within those tactics, projects or changes. Where an organization is using risk appetite as a planning tool, the organization will wish to operate within certain tolerance levels and manage the uncertainty associated with risk.

In other circumstances, risk appetite may simply reflect the constraints that are placed on staff in the organization. Authorization levels, expenditure limits and other constraints are often established in a delegation of authority within an organization. Levels of authority are a clear indication of the risk appetite of the organization. In these circumstances, exposure to risk is a consequence of the size, nature and complexity of the organization, and the organization will wish to set limits that define risk appetite and thereafter mitigate or minimize the risk exposure and possible impact and consequences.

In simple terms, if risk management is about achieving the most favourable outcome and reducing uncertainty, then risk appetite is about identifying the optimum level of risk that will achieve the most favourable outcome. Risk appetite is a reflection of the risk attitude and the risk criteria that have been established by the organization and the risks that it is willing to take.

Many organizations have attempted to produce risk appetite statements without clearly focusing on whether risk is a driver, planning guide or set of operating constraints. If all three approaches are applied, the risk appetite statement will reflect the complexity of that approach. Table 26.2 provides a set of risk appetite statements that could be in place for a college or educational establishment.

The stages that would be involved in developing this risk appetite statement are as follows:

- 1 Identify stakeholders and their expectations, making reference to the possible range of stakeholders, as defined by CSFSRS.
- 2 Define the company-wide risk exposure through an analysis of strategy, tactics, operations and compliance, as set out in the risk register.
- 3 Establish the desired level of risk exposure that will lead to a risk appetite statement that provides a set of qualitative and quantitative statements.
- 4 Define the range of acceptable volatility or uncertainty around each of the types of risks, leading to a statement of acceptable risk tolerances.

Table 26.2 Risk appetite statements for a college

Assessment	Description
High risk appetite	The college accepts opportunities that have an inherently high risk that may result in reputation damage, financial loss or exposure, major breakdown in IT systems, significant incidents of regulatory non-compliance or high potential risk of injury to staff and students.
Moderate risk appetite	The college is willing to accept risks that may result in reputation damage, financial loss or exposure, major breakdown in IT systems, significant incidents of regulatory non-compliance, potential risk of injury to staff and students.
Modest risk appetite	The college is willing to accept some risks in certain circumstances that may result in reputation damage, financial loss or exposure, major breakdown in IT systems, significant incidents of regulatory non-compliance, potential risk of injury to staff and students.
Low risk appetite	The college is not willing to accept risks in circumstances that may result in reputation damage, financial loss or exposure, major breakdown in IT systems, significant incidents of regulatory non-compliance, potential risk of injury to staff and students.

- 5 Reconcile the risk appetite and risk tolerances with the current level of risk exposure and plan actions to bring exposure in line with risk appetite.
- 6 Formalize and ratify a risk appetite statement, communicate the statement with stakeholders and implement accordingly.

Logically, risk appetite statements should be structured to align with the risk classification system used in the organization. Risk appetite statements may be structured on the basis of risk sources, components of the organization that may be impacted by the risk event and/or the impact or consequences categories, such as the FIRM risk scorecard, or the strategy, tactics, operations and compliance (STOC) of the organization. The UK government's guidance note on risk appetite statements is shown in the next box. Risk appetite statements can also be structured in a way that reflects the bow-tie approach to risk management shown in Figure 11.1. Table 26.3 shows an example of a risk appetite statement from a manufacturing organization.

UK government guidance note on risk appetite statements

Risk appetite statements should:

- provide a structure for an organization to work within. When correctly applied, statements describe acceptable outcomes relating to decisions being taken;
- drive thinking about results and outcomes the organization seeks to realize, as well as about what would need to change if outcomes were not acceptable;
- describe the organization's typical challenges and the basis on which different outcomes are justified;
- describe the organization's acceptable behaviour in reasonable circumstances. In circumstances where a decision is to be made and there are no directly comparable situations, risk appetite statements can provide illustrative guidance that can be adapted, documented and applied;
- be set against a five-point scale, with descriptors that are relevant to the organization. The five-point scale should demonstrate and reinforce the range of outcomes that are acceptable in different situations. These scales should be separate from scales used to assess the likelihood and impact of a risk;
- be dynamic and updated as necessary to reflect any significant changes in the context their organizations operate within, whether driven by societal, economic or political changes, for example.

SOURCE Government Finance Function (2020) *Risk Appetite: Guidance note v1.0*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/929385/Risk_Appetite_Guidance_Note_v1.0_FINAL.pdf

Table 26.3 Risk appetite for a manufacturing organization

Business component	Risk appetite statement
Target credit rating	Maintain a credit rating of at least BBB+
Earnings per share	Maintain an earnings per share level within the upper quartile of the peer group
Target capital ratio	Maintain a debt-to-capital ratio in the range 45% to 50%
Self-sustaining growth	New business will not dilute target capital ratio and maintain a capital working ratio in the range 1.5% to 2%
Financial strength	Maintain an earnings-before-interest and taxes-to-interest ratio between 5% and 7.5%
Customer dependence	No single customer will exceed 15% of total sales
Regulatory compliance	Score in the upper quartile of the peer set in regulatory reviews
Social responsibility	Seek a position in the upper quartile of the peer group in a social responsibility index

Risk appetite and lifestyle decisions

There is a relationship between personal risk appetite and lifestyle decisions. Decisions will be taken about, for example, long-term health issues, depending on family history and personal lifestyle. Individuals will take lifestyle decisions based on risk attitude, risk appetite, risk exposure and risk capacity.

There is a tendency for people to take a course of action when the outcome is immediate, positive and certain. There may be a certain appetite for risk, but the exposure that an individual actually suffers may be greater than their appetite. For example, people smoke cigarettes but may also wish to develop a healthier lifestyle. The smoker wants a cigarette because the nicotine effect is immediate, positive and certain. In contrast, developing a healthier lifestyle will result in benefits that will be delayed and uncertain, and this will also be combined with the negative feelings of being without nicotine.

The attitude of people to risk taking will vary considerably depending on the type of risk that is being considered. For example, individuals may be very risk-averse in the way they drive their cars, but accept significant risk factors in relation to their health, such as weight gain due to poor dietary choices. Risk appetite statements related to the risks that individuals are willing to take are, perhaps, just as difficult

to construct as risk appetite statements for organizations. In both cases, a clearly defined risk attitude would help define the appetite for a range of risk factors.

The willingness of individuals to take risks will depend on the nature of the risk and the ability to put effective controls in place. These factors will also combine with the costs to control the risks, such as gym memberships or smoking cessation programmes. Overall, the level of expenditure that an individual is willing to allocate to funding a control will be an indication of the risk attitude and risk appetite of that individual.

On a personal level, we can consider whether to implement the EM3 approach – to embrace, manage, mitigate and minimize risks related to strategy, tactics, operations and compliance (STOC). The overall approach to personal and organizational issues should be to:

- embrace opportunity risks (strategy);
- manage uncertainty risks (tactics);
- mitigate hazard risks (operations); and
- minimize compliance risks (compliance).

Note

- 1 NC State (2004) COSO's enterprise risk management – integrated framework, <https://erm.ncsu.edu/library/article/coso-erm-framework/> (archived at <https://perma.cc/3T8Y-99GZ>)

Risk training and communication 27

Consistent response to risk

One of the main reasons for communicating risk information and providing risk training is to ensure that a consistent response to similar risk events is always achieved. This can only be ensured by sharing information and experience. A consistent response is required in relation to hazard, control and opportunity risks. This is usually achieved through development of an organization's intranet to include detailed policies and procedures on risk management.

As well as a consistent response to individual risks, consistent risk protocols also need to be defined and communicated. Part of ensuring a consistent response is to identify risks in advance and confirm the controls that will be in place for them. This approach is relevant to strategic, project and operational risks, and training and communication protocols should be introduced to increase the consistency of response to risk across the organization.

It should be a requirement of every organization that a risk assessment is attached to each capital expenditure request. This risk assessment should include both the risks that the project is seeking to manage and the risks within the project itself. The risks within the project may affect the ability to deliver the project on time, within budget and to specification.

Risk assessment attached to strategic analysis is also a vitally important issue and is part of ensuring a consistent response to risk. Production of an 'issues manual' as a means of communicating risk across the organization and ensuring a consistent response to risks may also be valuable. The issues manual will identify risks, circumstances and other events where a response is required. The provision of adequate information, supervision and training will ensure that consistent and appropriate risk management procedures are more likely to be followed.

An important consideration related to the need for consistent responses to risk is when a new risk appears or an existing risk changes substantially. In these circumstances, risk escalation may be required so that the changed circumstances are viewed by senior management. The design and introduction of robust risk escalation procedures is required, with appropriate training provided in these procedures.

A consistent response to risk is vitally important in a crisis. When a disaster recovery plan has been produced by an organization, training for directors, managers and

staff is essential. Also, the requirements of the business continuity plan will need to be communicated to all persons who may be affected if the plan is implemented. Again, the importance of training in order to ensure a consistent response to adverse circumstances is essential.

Risk training and risk culture

As set out in Table 25.4, the risk culture of the organization can be defined by leadership, involvement, learning, accountability and communication (LILAC). The LILAC headings also provide an indication of the components of a successful initiative to embed risk management in the organization. The involvement, learning, accountability and communication components of a risk-aware culture are all highly relevant to risk training and risk communication.

Appropriate risk management documentation will provide managers and staff with information on the involvement that is required and the level of accountability that the organization expects. A good level of learning and communication can be established by adequate risk training and this will enhance the risk-aware culture of the organization.

Consider the example of a publisher facing libel and slander risks for its magazine publishing, including reference to its social media presence. The company should prepare risk guidelines, protocols and procedures including reference to awareness training for all staff. Comprehensive procedures for managing libel and slander risks should reflect the level of risk exposure. The level of attention paid to such risks will depend on each magazine title and the following suite of controls may be appropriate:

- all journalists to be given basic libel and slander training;
- specific review procedures introduced for political titles;
- legal evaluation of every issue of a satirical magazine.

Training needs to be provided for staff in the revised procedures, and information should be included on the company intranet site. Managers and staff need to be encouraged to comment on the new procedures, so that they may be improved further as part of the learning culture within the company.

Risk training is a key part of learning and communication and it is essential for manager, staff and other stakeholder engagement. It should cover a wide range of topics and achieve a greater understanding of all the risk-related issues, as well as providing information on the control measures that are in place and the vital role played by staff in the successful implementation of these controls. Risk management training is required on a continuing basis, but Table 27.1 provides some examples of when risk management training might be particularly relevant and/or necessary.

Table 27.1 Risk management training**Examples of when to undertake risk training**

When a manager is newly appointed or has been given new or additional responsibilities.

When an individual member of staff has been given a new role and/or procedures have been updated.

Following a recent incident or loss at the organization or at a competitor's premises or location.

On a refresher basis – and this may be a legal requirement in certain circumstances.

Risk information and communication

Component 7 of the COSO ERM cube considers the importance of risk information and communication. Risk communication starts with the identification of the stakeholders that have an interest in the particular risk under consideration. Once the stakeholders have been identified, the nature of the risk information that needs to be communicated must be decided. Finally, the purpose of communicating risk information to each group of stakeholders should be analysed.

Stakeholders will already have a perception of risks, so risk communication should be provided against the background of that existing perception. The guidelines relevant to risk communication set out in Table 27.2 should be followed. These guidelines seek to establish rules for communicating risk issues to a broad range of stakeholders.

Clearly, these rules become more important when the communication about risk is with external bodies. Nevertheless, they provide a useful set of guidelines for risk communication with internal as well as external stakeholders. Internal stakeholders have additional reasons for being provided with risk information. There will normally be an expectation by the organization that managers and staff will play a role in the future management of the risk, whereas this may not always be the case for external stakeholders.

The provision of risk training should be aligned with other activities within the organization. As with all other types of training, the content must be consistent with the requirements of the job. Training on risk matters will be required in a number of circumstances, including when new risks have appeared or existing risks have changed significantly. Training will also be required when an individual takes a new job or assumes additional responsibilities. Also, risk training will be important after an incident has occurred and new or enhanced procedures are introduced.

Table 27.2 Risk communication guidelines

-
- Know the stakeholders, by identifying both external and internal stakeholders and finding out their interests and concerns.
- Simplify the language and presentation, although not the content if complex issues need to be communicated.
- Be objective in the information provided and differentiate between opinions and facts.
- Communicate clearly and honestly, taking account of the level of understanding of the audience.
- Deal with uncertainty, discuss situations where not all information is available, and indicate what can be done to overcome these problems.
- Be cautious when putting risks in perspective, although comparing an unfamiliar risk with a familiar one can be helpful.
- Develop key messages that are clear, concise and to the point, with no more than three messages communicated at any one time.
- Be prepared to answer questions and agree to provide further information if it is not currently available.
-

An important part of risk information and communication is ensuring that there are adequate arrangements in place for ‘whistleblowers’. This has been part of the public interest disclosure legislation in UK since the late 1990s but has taken new life since the global financial crisis and in particular the EU Directive on Whistleblowing, effective from 2021 – the year after the UK left the EU, so it is uncertain as to its full applicability. However, there is a clear trend to more strictly enforce whistleblowing rules and this is a key area for the risk manager to make clear to management, especially in light of the following case study.

Barclays fine for whistleblowing breach

In December 2018 Barclays was fined \$15 million by New York State’s Department of Financial Services for violating the State banking laws, as well as being found to have contravened its own procedures in handling a whistleblowing complaint. The responsibility for such action lay at the feet of the Chief Executive, Jes Staley, who was found to have attempted to unmask the author of an anonymous letter sent to senior management within Barclays and which should have been dealt with under whistleblowing rules.

As well as the fine in the USA, Mr Staley was personally fined £642,430 by the UK regulator and had his bonus pay cut by £500,000.

SOURCE DFS (2018) DFS fines Barclays Bank PLC and New York branch \$15 million following whistleblower investigation, www.dfs.ny.gov/reports_and_publications/press_releases/pR1812181; FCA (2018) FCA and PRA jointly fine Mr James Staley £642,430 and announce special requirements regarding whistleblowing systems and controls at Barclays, www.fca.org.uk/news/press-releases/fca-and-pra-jointly-fine-mr-james-staley-announce-special-requirements

Although members of staff and other individuals may collect confidential information about an organization that would not normally be disclosed, there need to be arrangements in place for staff and other stakeholders to raise concerns if they have reasonable grounds for believing there has been serious malpractice. This is taken so seriously that in the USA the law permits the regulator to award a whistleblower up to 40 per cent of any fine that results from their actions.

Shared risk vocabulary

Part of communicating successfully on risk matters is the development of a common language of risk. Appendix B provides the vocabulary that is used in this book, as well as making reference to the definitions used in ISO Guide 73, which provides internationally recognized terms related to risk management. However, it is sometimes necessary for an organization to develop its own risk vocabulary, for aspects that may be particular and unique to it. A common understanding of risk based on the use of terminology within the organization is more important than arguments about precisely what a term means to different risk management practitioners.

In fact, as part of aligning risk management effort and embedding risk considerations into routine operations, it may be appropriate for the risk manager to use the terminology already in place in an organization. Even if the vocabulary of the organization conflicts with strict risk management definitions, communication will be more successful if the established vocabulary is used.

In this book, a standard vocabulary has been used in order to assist with the introduction and explanation of concepts relevant to risk management. Sometimes, this vocabulary contradicts ISO Guide 73, but it has been used to aid communication and understanding. The subject of a risk vocabulary and agreeing definitions can take a great deal of time and effort, and compromise is usually required.

A common language and agreed definitions are important so that all parties to a discussion have the same understanding of the terminology being used. This is illustrated by the summary in the next box.

A common language of risk

The first reason an organization needs a risk language is to underpin its risk culture. Everyone in the organization has a role in an effective risk management process. Most organizations have many layers (eg executives, line managers and employees) and 'silos' (eg technology, treasury, operations, quality management and compliance). A common language is needed to cut through the layers and break down the silos.

Conversely, without a common language, the risk management team will spend too much time resolving communication issues at the expense of their primary responsibilities.

Technology to support risk management process and procedures

Risk information can be made available to stakeholders by a variety of means. Many organizations produce brief guides and leaflets for stakeholders to communicate the current risk issues and concerns. The appropriate means of communication will vary according to the nature of the stakeholder and the nature and complexity of the message to be communicated.

Formal means of risk communication exist where the organization has to report to financial stakeholders. When risk communication is required, a range of communication techniques can be used. A formal report to the stock exchange or to other financial stakeholders may be backed up by an informal video, slide presentation and/or a telephone conference call, as appropriate.

For many large organizations, it is common for their intranet to be used to communicate risk management, health and safety information and business continuity plans. Information can be provided on the intranet about the generic risk assessments that have been undertaken and the control measures that have been identified. The intranet can also be used to communicate urgent risk information, as well as providing updates on risk assessments, control measures and the current level of any particular risk.

An important consideration in the collection, retention and supply of risk information is that it should be aligned with other management information systems within the organization. Providing risk information as a separate management information stream is likely to result in risk management activities failing to be aligned or embedded within other activities. The danger that risk information will become irrelevant to managers in the organization is greater when the organization has a dedicated risk management information system (RMIS).

A common language of risk

The first reason an organization needs a risk language is to underpin its risk culture. Everyone in the organization has a role in an effective risk management process. Most organizations have many layers (eg executives, line managers and employees) and 'silos' (eg technology, treasury, operations, quality management and compliance). A common language is needed to cut through the layers and break down the silos. Without a common language, the risk management team will spend too much time resolving communication issues at the expense of their primary responsibilities.

Risk management information systems

The distribution of risk management guidelines, protocols and procedures may be undertaken by way of a risk management information system software package. The RMIS could be placed on the intranet of the organization. The RMIS will also facilitate the collection and communication of risk information, including the reporting of events by local management as they occur. Typically, the RMIS could include a wide range of information, as summarized in Table 27.3.

Table 27.3 Risk management information system

The following types of information may be handled, stored, managed, distributed and communicated using a risk management information system (RMIS):

- Risk management policy and protocols
- Risk profile data, values and information
- Emergency contact arrangements and contact details
- Insurance values and cost of risk data
- Insurance claims handling and management protocols
- Historical loss/claims experience/information
- Insurance policy coverage and other information
- Risk management action plans (risk register)
- Risk improvement plans and implementation
- Business continuity plans and responsibilities
- Disaster recovery plans and responsibilities
- Corporate governance arrangements and reports

RMISs have been used for some time to record details of insurance claims. The use of an RMIS has become more sophisticated and is now likely to enable the recording of details of the risk exposure, risk control and risk action plans. In many cases this is also linked to measures of the activity being undertaken to act as a ‘dashboard’ to ‘measure’ risk across different timeframes.

RMISs were initially developed in order to enable more efficient administration of insurance policies and provided documentation, and in some cases analysis of insurance claims. Such systems were also used to pool risk exposure information and report accidents or other events that could have led to an insurance claim.

There are now a number of software products that support a broader enterprise-wide approach. These include software packages that can undertake risk register reviews from lower divisional units to produce reports of significant risks to the board level through a cascading upwards process. RMISs also produce detailed risk analysis and dependency modelling reviews.

These systems are becoming more useful as more data becomes available. In the past, these models were less scalable as they required detailed input of data, which is now available through databases, whether public or private. As RMISs become more developed and sophisticated, they can offer a significant benefit to organizations that use them.

Risk information needs to be shared throughout an organization to enhance risk awareness and ensure improved risk performance. It is almost always the case that individuals within an organization will have the best understanding of the risks, as well as detailed practical knowledge of the actions that should be taken to mitigate risk events. Communication is also important to share information about incidents that have occurred, including lessons that were learnt and the actions that were taken to ensure that the event is not repeated.

An analysis of the advantages and disadvantages of RMIS is set out in the next box. In general, an RMIS becomes more valuable when the risks are complex or the amount of data that needs to be recorded is substantial.

Advantages and disadvantages of RMIS

There are many risk management information systems available commercially, although the market is consolidating as investment in new technologies causes separate firms to combine forces. Initially, these systems required large amounts of separately held data to cross-reference activity in the company with loss activity or risk exposure, and were tailored to the individual companies concerned. The systems were largely aimed at larger companies that had the resource and data to make the pursuit worthwhile.

Improvements in their ability to manage and analyse diverse datasets mean these systems are now becoming more competitive. Advanced technology enables risk managers to integrate techniques of modelling and scenario simulations to suit their individual context.

Whilst the cost of developing systems is reducing, it must be shown that benefits will exceed whatever cost is involved. The costs are immediate and tangible; the benefit is difficult to estimate or demonstrate. It is a potential future benefit, not an assured, immediate expense reduction.

Whether the risk assessments from an RMIS are likely to lead to enough marginal benefits to offset the cost of data tracking and analysis depends on the risk profile of the company. Ultimately, an RMIS may pay for itself by enabling an organization to avoid or effectively finance that one catastrophic loss that would otherwise slash the financial results of the company.

This has fuelled a debate on the use of the risk register in many organizations, and that debate was raised in the section on risk registers in Part One. Technologies are being developed that integrate risk assessment, risk recording and risk action plans within the management information that is used for the day-to-day management of the organization.

Risk practitioner competencies 28

Competency frameworks

Risk management has become a profession, rather than a set of activities. For any profession, it is essential that a set of competencies is established that defines the activities that practitioners within the profession will need to display. There are several styles and formats for competency frameworks, but most are based on the stages that are involved in the practice of the profession. Having identified the stages that are involved in the profession, the levels of competency required at different stages of seniority are then described. The IRM Professional Standards provide these levels and competency requirements and can be found at www.theirm.org/what-we-do/about-us/professional-standards

It is generally accepted that both technical/hard skills and people/soft skills are required to become a successful practitioner in the profession. The risk practitioner needs both these skills in order to successfully assist an organization with the design and implementation of a risk management framework.

Two areas of technical skills are required by a risk practitioner. Firstly, and most obviously, the practitioner needs to have competency across a range of risk management issues and activities. A range of business skills in order to understand the context (both external and internal) within which the organization operates is useful. An understanding of business and the development of appropriate business skills is essential if the risk management practitioner is to successfully develop an appropriate risk management process and supporting risk management framework.

This textbook is not about the development of business skills, so the greater focus is placed on the risk management technical skills that will be required by the risk practitioner. These risk management technical skills will be closely aligned with the stages in the implementation of a risk management initiative, as set out in Chapter 7. Table 28.1 provides an overview of the risk management technical skills that will be required by a successful risk management practitioner.

Table 28.1 Risk management technical skills

<i>Skills associated with planning risk management strategy</i>	
Evaluate status	Evaluate the organizational context and objectives and map the external and internal risk context
Develop strategy	Develop risk strategy and risk management policy and develop the common language of risk
<i>Skills associated with implementing a risk management architecture</i>	
Design architecture	Design and implement risk management architecture, roles and responsibilities
Develop processes	Develop and implement the risk management processes, procedures and protocols
Build awareness	Build a culture of risk awareness aligned with other management activities
<i>Skills associated with measuring risk management performance</i>	
Facilitate assessments	Facilitate the identification, analysis and evaluation of risks, and design record-keeping procedures
Evaluate controls	Evaluate existing performance and evaluate efficiency and effectiveness of existing controls
Improve controls	Facilitate the design and implementation of necessary and cost-effective control improvements
<i>Skills associated with learning from risk management experience</i>	
Evaluate framework	Evaluate risk management strategy, policies and processes, and introduce improvements
Design reports	Develop understanding of reporting requirements, design reporting formats and produce appropriate reports

Range of skills

The range of skills required by a successful risk management practitioner includes both technical or hard skills and people, inter-personal or soft skills. Technical skills can be divided into risk management technical skills and business technical skills. The risk management technical skills can be set out as a competency framework, in the way described in Table 28.1.

The range of business skills that will be required will vary according to the type of organization. In general, they will include skills related to accounting, finance, legal affairs, human resources, marketing, operations and information technology.

The importance of people skills has increased considerably as communication within and between organizations has changed. People skills are often referred to as soft skills. Technical skills are usually considered to be associated with intellectual intelligence, whereas soft or people skills are associated with emotional intelligence. To be successful, the risk practitioner needs a combination of both types of intelligence and both sets of skills.

As well as technical and people skills, the successful risk manager will also require the skills associated with self-management and self-development. Typically, these will be the skills expected of all technical professionals and will often be underpinned by adherence to a code of ethics or conduct together with a requirement to maintain knowledge through continuous professional development once certified. Self-development covers activities that enhance talents and potential, as well as increasing job satisfaction and future employability. Self-development also includes developing other people, and this may include activities such as teacher, mentor, training provider and/or professional coach.

Table 28.2 describes the range of people skills that are required in the business environment. These skills can be classified as communication, relationship, analytical and management (CRAM) skills. Technical skills can be acquired through a combination of training and experience, but people skills are far more reliant on the personality of the individual. Therefore, it is a greater challenge for risk practitioners to master the range of people skills that are required in order to be successful.

Table 28.2 People skills for risk management practitioners

Key skill	Skill requirements
Communication	Excellent written and oral skills Presentation and public-speaking skills Committee and meeting participation skills
Relationship	Influencing skills to work with 'challenging' behaviour Negotiating skills to defuse conflict and identify solutions Networking skills across organizational silos
Analytical	Strategic thinking skills and creativity skills Data-handling skills to get to the heart of a problem Research skills to present arguments based on facts
Management	Time-management skills to manage teams and projects Leadership skills to motivate and develop staff Facilitation skills to assist with setting priorities

The benefits of people or 'soft' skills

While labelling them 'soft' may make them sound less important than technical skills, in fact people skills are essential for all businesses, and can actually mean the difference between success and failure. Employing staff with good people skills will mean they are more effective when interacting with people. This is particularly important if your business is largely based on face-to-face contact with clients.

Just as technical skills can be learnt and developed, so too can people skills. In fact, people skills are continuously developed over the course of a lifetime, but there are ways that you can encourage this in your business. These include workshops, seminars and encouragement to staff to provide input, suggestions and advice in business discussions.

Communication skills

Accurate communication on risk issues is vitally important. Internal communication within the organization will be undertaken through the risk architecture. This is the formal risk communication structure related to risk control activities and the collecting of information for external risk reporting purposes. Such communications may be required to address board-level concerns, such as the performance of loss control programmes. The board of the company may require a report at every board meeting in the form of a 'dashboard' showing key risk metrics. These reports will enable the board to benchmark the performance of the company, in comparison both with competitors and with historical data for the company itself. In this case, the board is monitoring performance, whereas the management of the improved risk performance remains an executive responsibility to be delivered by line management.

Risk communication may also be more informal, taking place, for example, during risk assessment workshops or at risk training courses. Communication arrangements are part of the risk culture. External risk communications will need to take place with external stakeholders, including the media, the general public and pressure groups.

For example, if a road haulage company wishes to extend its vehicle storage depot, there will be a need to communicate with stakeholders, as well as local authority planning departments. The company will need to gain agreement from a number of stakeholders in order to enact the development and will need to prepare communications that provide an evaluation of the risks and opportunities for the community when the depot is extended. The public perception of what is proposed and their view of the impact on the vicinity will be vital to achieving acceptance. Accordingly, the company will need to prepare an honest, open and detailed case

that provides a full explanation to all interested parties, and in particular illustrate the risk control arrangements that are in place.

The next box describes risk communication in relation to nuclear and chemical industries in the United States. It suggests that for the messages to resonate there needs to be an appeal to emotion as well as logic. The public perception of risk may not be aligned with the scientific evidence if the public is wary and afraid of any development. Information communicated by an organization needs to address these emotional concerns if it is to be heard.

Development of risk communication

The formal development of risk communication as a subject began in the late 1970s with efforts by the nuclear and chemical industries in the United States to counteract widespread public concern about those technologies. It was believed that clear, understandable information was all that was needed to make people see that the risks were lower than many feared.

For decades this approach has failed, and most risk communication experts say it is inadequate. Perceptions of risk, and the behaviours that result, are a matter not only of the facts but also of our feelings, instincts and personal life circumstances. Communication that offers the facts but fails to account for the affective side of our risk perceptions is simply incomplete.

Risk communication is also commonly thought of as what to say under crisis circumstances, but this is inadequate. While it is certainly true that communication in times of crisis is important in managing the public response, countless examples have taught that a great deal of the effectiveness of risk communication during a crisis is based on what was done beforehand.

The transmission of logical and evidence-based argument is made more problematic by the rise of the ‘fake news’ culture and disdain of ‘experts’ in favour of beliefs that appear attractive by appealing to the emotions of individuals who are vulnerable to these cries. This is discussed in more detail in Chapter 21, which considers reputation.

An important consideration in relation to communication skills is the ability to facilitate education internally about risk management through, for example, training courses or seminars and by facilitating risk assessment workshops. There are a number of basic skills that are required in running a successful workshop, but the starting point is to establish its structure and format. In general, the key will be to ensure that the discussion is well structured and that all attendees have an opportunity to contribute on an equal basis. It is assumed that the need for physical location at workplaces

of the future will be diminished, although some physical interaction will undoubtedly be needed. The skills of the risk manager in facilitating workshops and training sessions will be needed to embrace online and remote working methods accordingly.

Techniques that have been used during workshops include the use of sticky notes to capture ideas from delegates. These can be transposed to the use of a remote 'whiteboard' in some applications but whichever process is used the risk management practitioner will need to consolidate the many ideas into a small number of agreed issues. This requires skill to identify similarities in the ideas and consolidate compatible ideas into a smaller number of issues or, more specifically, identified risks.

Running training courses requires a different set of skills, although the overriding requirement to engage all attendees remains a top priority. Preparation is critical to the success of such courses. A possible structure is set out in Table 28.3.

Other communication skills relate to verbal and written presentation. These will include the ability to write reports, both for internal and external distribution. Depending on the organization, the style of written reports will vary greatly. Most organizations require short summary reports for the board with substantial back-up information available for 'drilling down' if required. It is important that the risk practitioner adopts the style of communication that fits within the culture of the organization, and increasingly this will be dominated by using online data and libraries that can be searched at will.

It is often challenging to present information about risk in an engaging way through narrative or text. Visualization of risk in the form of graphical analysis presenting data in meaningful ways can enable better decision making by making issues clearer.

Table 28.3 Structure of training courses

Stage	Intention
1 Set up	This stage will describe what the course will provide. It is often achieved by delegate introductions and expectations, a group exercise or a simple quiz to get everybody thinking about the topic of the day.
2 Set out	This stage provides the detailed information that the training course is intended to impart. It can be a combination of structured inputs, group tasks, discussion exercises, feedback sessions and training films.
3 Set down	This stage summarizes what the course has covered and confirms general understanding. It will often ask delegates to confirm what they have learnt and/or indicate what actions they will take following the course.

When making any presentation, it is important for the risk practitioner to decide what the purpose of the presentation is and who will be receiving it. When communicating a message, it is useful to think about the ‘5Cs’ of communication. The message should be clear, concise, coherent, credible and complete:

- Clear: Ensure that the recipient understands the purpose of the communication.
- Concise: It is more likely to be listened to.
- Coherent: It is logical and relevant to the main topic.
- Credible: There is substantiating evidence to address the audience’s concerns and priorities.
- Complete: It provides the audience with everything they need in order to take necessary action.

Relationship skills

There is a range of relationship skills that are required, as indicated in Table 28.2. Perhaps the most important are influencing and negotiating skills. Other relationship skills that are important include motivation and political skills. As with other people skills, relationship skills need to be exercised within the culture of the organization and in a way that pays full regard to its internal context.

Listening skills are vitally important to influencing a change of behaviour such as mitigating risky activities. The point of view of an individual you are negotiating with or are seeking to influence must be clearly understood, and if possible, repeated back to them. Successful influencing is best achieved by individuals who have the ability to gain support, inspire others, create relationships and engage the imagination of other people. Generally speaking, influence is achieved by using positive energy and enthusiasm about the issues that need to be changed. Achieving improvements in risk management standards often requires continuous negotiation. The means of achieving successful negotiations are well established, and risk practitioners need to be aware of and embrace negotiating techniques.

In being a good influence, the successful risk practitioner needs to understand the importance of ‘political’ skills. This usually means the need to understand the background or context of an individual who may be challenging and who displays inappropriate behaviours. The risk practitioner should be aware of the group dynamics and be able to negotiate so that those individuals can find some benefit from their stance, or as a minimum they do not ‘lose face’ in the discussion. It is important therefore to defuse conflict and negotiate solutions in a flexible way, including by being aware of cultural influences and differing stakeholder requirements.

In many ways, political skills are at their most important when the risk practitioner is chairing a meeting. All persons attending the meeting are entitled to voice their opinion in full, for as long as their message is clear, concise, coherent and credible. The role of a chairman, especially when present in a non-executive role, is to stay neutral and remain unbiased whilst guiding the meeting to an appropriate consensus.

The essence of relationship skills is to build relationships with various stakeholders. A risk practitioner must engage with stakeholders who will be many and varied, as discussed in Chapter 30. The range of stakeholders in an organization will include customers, staff, financiers, suppliers, regulators and society (CSFSRS). With such a wide range of stakeholders, not all of whom will be interested in risk and risk management, it is obvious that the risk practitioner needs excellent communication and relationship skills.

Analytical skills

Analytical skills range widely and require strategic and logical thinking. On occasions, when problem solving is involved, creative lateral thinking is also a key requirement of the risk practitioner. Many risk practitioners are involved in quantification of risks, either regulatory requirements or as part of an analysis to determine the appropriate level of insurance that is required.

However, analytical skills are not always mathematically based and well-developed problem-solving skills will be of considerable benefit to a typical risk practitioner. In addition to analytical skills, research skills are often a requirement of many risk practitioners. The ability to locate and analyse information quickly and efficiently will be of considerable benefit to a risk practitioner.

Risk practitioners are often required to evaluate a great deal of information about a specific topic, find the common thread within that information and present the findings in a concise and logical manner. This will almost invariably be a requirement when the risk practitioner is drafting a written report or preparing a training course or presentation. The benefit of being skilled in analytical activities is at its greatest when the risk practitioner is seeking to facilitate a risk assessment workshop.

It is often the case in risk assessment workshops that the delegates will have different views of the level of risk presented by a specific situation. A skilful facilitator is able to listen to these conflicting views and identify the underlying presumptions that have resulted in the different conclusions. Having identified the presumptions and assumptions, the skilled facilitator will then be able to challenge the different parties with the reasons for their differing opinions. This will be the most successful way of coming to a common view.

Analytical skill involves the ability to understand, challenge and articulate problems and concepts and thereby make decisions based on the available information. These skills include the ability to demonstrate and apply logical thinking to the gathering and analysis of information, as well as the designing and testing of solutions to problems. The output from analytical skills is the ability to formulate appropriate alternative solutions and challenge the alternatives so as to develop the most logical plan of action.

Problem solving and decision making are important skills for business life. Problem solving often involves decision making, and decision making is especially important for risk management. There are activities and techniques to improve decision making and the quality of decisions. Decision making is more natural to certain personalities, so these people should focus more on improving the quality of their decisions. People who are less natural decision makers are often able to make quality assessments, but may need to be more decisive in acting upon the decisions made.

Problem solving and decision making are closely linked and each requires creativity in identifying and developing options. Brainstorming techniques are particularly useful and these will include SWOT and PESTLE analysis structures. Good decision making requires a mixture of skills, including creative development and identification of options, clarity of judgement, firmness of decision and effectiveness of implementation.

Management skills

Some risk managers have a small number of people directly reporting to them; others may be in charge of large departments monitoring risks in all forms. Whichever situation they may be in, there is a need to understand management skills either to manage their team or understand the needs of other managers to persuade those managers to take a different course of action.

Many of the people skills described in this section are also relevant as management skills. Firstly, the skill of self-management includes the ability to set appropriate priorities, meet necessary deadlines and maintain motivation. Time management, organizational and self-motivation skills will remain important for the risk practitioner throughout his or her working life.

Perhaps the most important of these people skills as a manager is that of being able to motivate others. Such motivational skills are important for risk practitioners where a change in behaviour or a development of risk-aware culture is required. The risk practitioner will need to motivate individuals, managers and directors to behave differently.

Perhaps it is worth reflecting on the fact that there is a difference between management and leadership. An individual may be able to manage a department by

exercising tight control over the activities of individuals. This is not the same as the leader who has established a set of priorities and empowers members of the team to manage their own activities towards fulfilment of those priorities. Ideally, the leader will have ensured that the priorities have been developed in full consultation with the individuals responsible for delivering those priorities.

Leadership versus management

The biggest difference between managers and leaders is the way they motivate the people who work for them and this sets the tone for most other aspects of what they do.

Managers have subordinates, a position of authority, and the subordinates who work for them largely do as they are told. Managers are paid to get things done and pass on this work focus to their subordinates. Managers seek control, which indicates that they are relatively risk-averse, and they will seek to avoid conflict where possible.

Leaders have followers, rather than subordinates. Many organizational leaders do have subordinates, but only because they are also managers. When they want to lead, they give up formal authoritarian control. Leaders consider it natural to encounter problems that must be overcome. They are comfortable with risk and will see routes that others avoid as potential opportunities, but may break rules in order to get things done.

THIS PAGE IS INTENTIONALLY LEFT BLANK

PART SEVEN

Corporate

governance and

risk management

LEARNING OUTCOMES

Having studied this section readers will be able to:

- Describe the key features of a corporate governance model and describe the links to risk management in different types of organizations.
- Outline the importance of evaluating the performance of the board and board committees and how this relates to corporate governance.
- List the different types of stakeholders of a typical organization (CSFSRS) and explain their influence on risk management.
- Explain the importance of stakeholder expectations and how these can be managed by effective dialogue and communication.
- Summarize the key features of operational risk as practised in financial institutions such as banks and insurance companies.
- Describe the key sources of operational risk in financial institutions and provide examples of how these risks are managed.
- Produce a brief description of the project lifecycle and the importance of risk management at each stage.
- Describe the key features of a project risk management system, such as the project risk analysis and management (PRAM) approach.

- Describe the importance of the supply chain and the contribution of supply chain risk management to the success of the organization.
- Produce examples of the risks associated with outsourcing and how these risks can be successfully managed.

Further Reading

- Association for Project Management (2010) *Project Risk Analysis and Management Guide*, 2nd edn, APM Publishing, Princes Risborough
- ISO (2021) ISO 37000 Governance of Organizations – Guidance, www.iso.org/standard/65036.html
- London Stock Exchange (2012) *Corporate Governance: For main market and AIM companies*, <https://docs.londonstockexchange.com/sites/default/files/documents/guide-corporate-governance-pdf.pdf>
- Single Source Regulations Office Corporate Governance Framework*, (2021) – the UK Government advice, found at <https://www.gov.uk/government/publications/ssro-corporate-governance-framework/corporate-governance-framework> *The impact of the highly improbable*, Penguin, Harmondsworth
- Woods, M (2011) *Risk Management in Organizations: An integrated case study approach*, Routledge, Abingdon

CASE STUDIES

The student can review the following examples to illustrate further the areas discussed in Part Seven and throughout this book.

Capita: Structure of board and stakeholders

Capita is a business processing outsourcing company involved in supplying professional services largely in the UK to both the government and the private sector. It has operations also across Europe, Africa and Asia.

Firstly, Capita is an interesting example of the pioneering use of employee non-executive directors in UK companies. In some ways this mirrors the 'workplace council' (or two-tiered) approach of many European entities but seems to go further by maintaining a unitary board structure for all matters. Capita states that the 'non-executive employee directors are appointed from the workforce to contribute an employee perspective to Board discussions. This is a key element of the Board's approach to employee engagement.'

Secondly, Capita sets out in its Section 172 statement its position on stakeholders. These are identified as employees, clients, suppliers, investors and society. Pages 38–39 of their annual report provide details of the company's engagement with each party and some metrics that will make it possible to track the company's success in stakeholder management.

In their risk management section they clearly identify how they apply the three lines of defence model to their business.

Edited extracts from: Capita plc (2020) Annual Report 2020, <https://www.capita.com/sites/g/files/nginej291/files/acquiadam/2021-03/capita-annual-report-2020.pdf>

Pioneer Food Group: Mergers and regulation

Pioneer Food Group had an independent market capitalization of ZAR 23.5 billion at 30 September 2019 and agreed a takeover by PepsiCo Group, which was allowed by regulators in March 2020. The Group operates a number of facilities producing and distributing a range of food and beverage products in South Africa and throughout the region. PepsiCo wished to acquire the business to focus its growth into Africa through them.

The South African regulators allowed the purchase to go ahead with a number of caveats, for example:

- maintaining the head office in South Africa;
- local employment and investment guarantees in South Africa;
- increasing the proportion of South African sourced agricultural products and packaging;
- establishing a development fund to expand the number of black farmers in their supply chain;
- establishing board representation from their Workers' Trust onto the Pioneer Group board.

Their integrated annual report from 2019 is worthy of review to compare with other reports that require more disclosures, for example on Section 172. Without those requirements, the statements offered, whilst doubtless welcomed by investors and others, do seem to be less meaningful. For example, in this report stakeholder engagement is reported as follows:

Success in modern business means responding swiftly and accurately to fast changing market realities. Staying in contact with key stakeholders and proactively engaging their feedback informs the Board in reviewing risks, challenges and opportunities. In this period, we regularly engaged major stakeholders such as unions, employees, shareholders, communities and regulators.

Edited extracts from: Pioneer Foods (2019) Integrated Report 2019, www.pioneerfoods.co.za/wp-content/uploads/Integrated-Annual-Report-2019.pdf and South African

Government (2020) Trade and Industry concludes agreement on acquisition of Pioneer Foods, www.gov.za/speeches/government-and-pepsico-conclude-agreement-acquisition-pioneer-foods-8-mar-2020-0000#

UK Department for Work and Pensions: A chief risk officer

The Department for Work and Pensions (DWP) is the UK department responsible for welfare, pensions and child maintenance policy. It is the UK's biggest public service department, administering the State Pension and a range of working age, disability and ill health benefits to around 20 million claimants and customers. It is the second largest governmental department in terms of employees, and the largest in terms of expenditure (£187 billion).

Clearly the principal risk to this unit of government is fraudulent applications from members of the public abusing the system to receive benefits to which they are not entitled, an operational risk for DWP. Since funds are handled and paid, this applies to internal employee fraud also. DWP operates a 'three lines of defence' model and shows its risk management approach along the PIML lines, but reframed for them in terms of identify, assess, address, review and report.

They appointed 'A Chief Risk Officer... towards the end of 2018–19. During 2019–20, in the first full year in post, the role has driven improved oversight and visibility of principal risks with risk management embedded in senior leadership conversations.' They then implemented a new risk management strategy following the release of the 2020 edition of *The Orange Book*. It is our understanding that the DWP contributed to the development of the new *Orange Book*.

Also of interest to the student is the report-on whistleblowing in the annual report, where 29 cases were noted in 2019 compared to 56 in 2018, although they also established an HR mediation service in that year, which received 158 calls anonymously, and may be a reason for the decline in the number of cases of whistleblowing.

Edited extracts from: Department for Work and Pensions (2020) Annual Report and Accounts 2019–20, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896268/dwp-annual-report-and-accounts-2019-2020.pdf

Introducing corporate governance

29

Corporate governance

Corporate governance is defined as the system by which companies are directed and controlled. Principle O of the UK Corporate Governance Code states:

The board should establish procedures to manage risk, oversee the internal control framework, and determine the nature and extent of the principal risks the company is willing to take in order to achieve its long-term strategic objectives.¹

Most countries in the world place corporate governance requirements on organizations. These requirements are particularly strong in relation to companies quoted on stock exchanges, organizations that are registered charities and government departments, agencies and authorities.

There are two main approaches to the enforcement of corporate governance standards. Some countries treat corporate governance requirements as ‘comply or explain’. In other words, the organization should comply with the requirements or explain why it was not appropriate, necessary or feasible to comply. If appropriate, an organization could explain that an alternative approach was taken to achieve the same result. In these countries, the requirements may be regarded as one means of achieving good practice, but equally effective alternative arrangements are also acceptable.

Other countries require full compliance with detailed requirements, although limited alternatives for achieving compliance are sometimes included within these requirements. In these countries detailed compliance is expected and exceptions would not be acceptable.

Corporate governance requirements should be viewed as obligations placed on the board of an organization. These requirements are placed on board members by legislation and by various codes of practice. Often, these corporate governance requirements are presented as detailed codes of practice. To start the task of enhancing corporate governance standards, an organization may develop a code of ethics for

company directors, together with appropriate delegation of authority documents. An annual statement of any potential conflicts of interest should be required from directors, and training should be provided for the board on corporate governance.

The organization should set up appropriate committees (as listed below) with established terms of reference and membership of each of these committees, which may be established as sub-committees of the board. Reports on corporate governance standards, concerns and activities should be received at every board meeting, and these papers will often be presented by the company secretary. Such committees may include:

- risk management committee;
- audit committee;
- disclosures committee;
- nominations committee;
- remuneration committee.

What happens if corporate governance is weak?

Better practices in corporate governance were called for in the UK from the 1980s following the unexpected collapse of a number of companies: Bank of Credit, Commerce & Industry, the Mirror Group, Polly Peck International and Barings Bank. In each case, there were serious accounting and financial reporting irregularities and inadequate internal controls and risk management.

In 2001 these examples became nothing when a company called Enron collapsed with a loss to shareholders of \$74 billion, caused by the main executives withholding information on company debt that should have been reported to investors and employees. The fraudulent activity was reported by a whistleblower and had not been revealed by auditors. This scandal led to the Sarbanes–Oxley Act and the demise of Arthur Andersen, who were at the time one of the main global accounting firms.

OECD principles of corporate governance

Corporate governance is concerned with systems, procedures, controls, accountabilities and decision making at the highest level and throughout an organization.

Because corporate governance is concerned with the way that senior management fulfil their responsibilities and authority, there is a large component of risk management

contained in the overall corporate governance structure of every organization. Corporate governance is concerned with the need for openness, integrity and accountability in decision making, and this is relevant to all organizations, regardless of size or whether in the public or private sector.

The Organisation for Economic Co-operation and Development (OECD) is an international body helping governments tackle the economic, social and governance challenges of a globalized economy. The OECD updated (in 2015) the set of principles for corporate governance and these are set out in Table 29.1. These principles focus on the development of an effective corporate governance framework that pays due regard to the rights of stakeholders.

The principles require the equitable treatment of all stakeholders and an influential role for stakeholders in corporate governance. They also require disclosure and transparency. There have been a number of standards published on corporate governance including by the British Standards Institute, which published *BS 13500:2013 Code of Practice for Delivering Effective Governance of Organizations*, which states: ‘It is increasingly obvious that society’s expectations of organizational behaviours and performance, and thus “governance”, are rising. This rise in expectations is partly in response to a steady flow of major incidents and perceived abuses of

Table 29.1 OECD principles of corporate governance

Principle	Definition
I. Effective corporate governance framework	Promote transparent and fair markets, efficient allocation of resources and be consistent with the rule of law and support effective supervision and enforcement.
II. Rights and equitable treatment of shareholders	Protect and facilitate the exercise of shareholder rights and ensure equitable treatment of all shareholders, including minority and foreign shareholders.
III. Institutional investors, stock markets and other intermediaries	Sound incentives throughout the investment chain and provide for stock markets to function in a way that contributes to good corporate governance.
IV. Role of stakeholders in corporate governance	Recognize the rights of stakeholders established by law or through mutual agreements and encourage active co-operation between corporations and stakeholders.
V. Disclosure and transparency	Timely and accurate disclosure is made on all material matters, including the financial situation, performance, ownership and governance of the company.
VI. Responsibilities of the board	Strategic guidance of the company, the effective monitoring of management by the board and board accountability to the company and the shareholders.

authority.' This standard will be superseded by ISO 37000 which at the time of writing had not been published but is anticipated to follow along similar lines.

The approach in BS 13500 is based on the evidence that good governance promotes the success of organizations and society. Therefore, the scope of the code goes beyond the avoidance or mitigation of problems. It defines different accountabilities to different stakeholders and is intended to be used as a basic checklist to ensure that all the elements of a good governance system are in place. The point is also made that having a corporate governance system in place does not guarantee effective governance, but it does encourage and support positive organizational values and behaviours.

Future direction of corporate governance

The various codes that define good corporate governance are under constant review: the FRC code has been updated every two or three years since 1992 and the UK government proposed eight reforms across the three areas of pay, employee and stakeholder voice, and the governance of large private companies in 2018. One proposal was to replace the FRC with a statutory body accountable to Parliament, but subsequently this became a request for:

the FRC, the Financial Conduct Authority and the Insolvency Service to conclude new or, in some cases, revised letters of understanding with each other before the end of [2020] to ensure the most effective use of their existing powers to sanction directors and ensure the integrity of corporate governance reporting.²

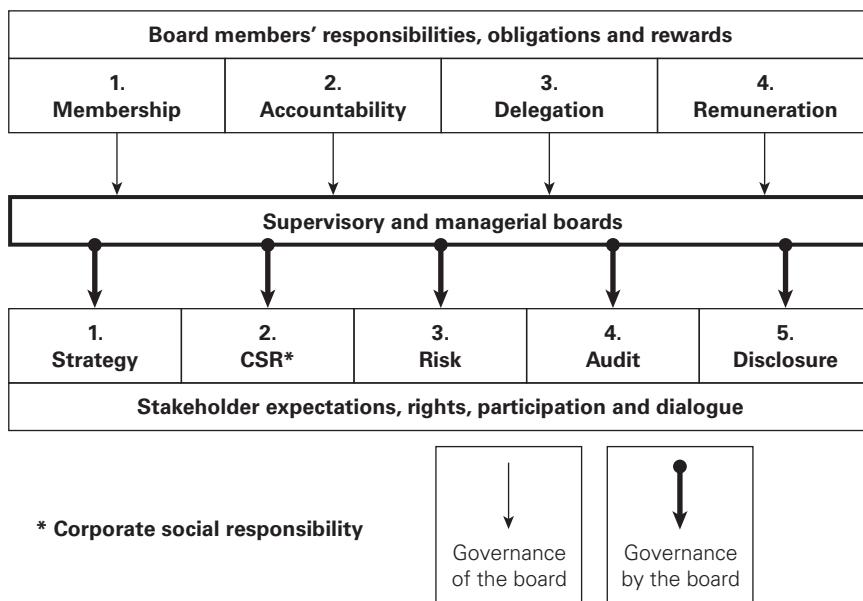
The government has retained the right to involve itself further if further action is required.

London Stock Exchange corporate governance framework

The London Stock Exchange (LSE) has produced guidance on corporate governance, the focus of which is on the effectiveness of the board. In the view of the LSE, corporate governance is about the effective management of the organization, the appropriate responsibilities and the role of the senior managers and board members within the organization.

Figure 29.1 provides a summary representation of the LSE governance framework. Governance activities are centred on the board of the organization and the LSE guidance refers to these boards as supervisory and managerial boards. The corporate governance framework has two main components: 1) the responsibilities, obligations and rewards of board members; and 2) the fulfilment of stakeholder expectations, rights, participation and dialogue.

Figure 29.1 LSE corporate governance framework



The importance of board members' responsibilities, obligations and rewards are emphasized and include arrangements for:

- determining membership of the board;
- accountability of board members;
- delegation of authority from the board;
- remuneration of board members.

The responsibilities of board members must be fulfilled in five important areas, in respect of the fulfilment of stakeholder expectations, rights, participation and dialogue. In summary, these five areas are:

- strategic thinking, planning and implementation;
- corporate social responsibility;
- effective management of risks;
- audit and risk assurance;
- full and accurate disclosure.

The OECD principles and the LSE corporate governance framework provide the overall requirements and framework within which corporate governance must be delivered. However, the activities that are employed to deliver each of the five areas of stakeholder expectation will vary.

Risk management activities should be viewed within the wider framework of corporate governance. Although risk management is presented as a separate component of corporate governance in the LSE framework, risk issues also underpin strategy, corporate social responsibility, audit and disclosure.

Non-executive directors play an important role in corporate governance. Generally speaking, the audit committee will be a non-executive group and may represent the third line of defence when appropriate, as described in Chapter 34. It should be noted that here there will be some consideration required as to context. For financial services entities, the third line of defence provides independent assurance to the board of the appropriateness of the risk framework. Basel Committee principles are that:

This function's staff should not be involved in the development, implementation and operation of operational risk management processes by the other two lines of defence.

The third line of defence reviews generally are conducted by the bank's internal and/or external audit, but may also involve other suitably qualified independent third parties.³

Generally, it is accepted that an effective non-executive director will:

- uphold the highest ethical standards of integrity and probity;
- support executives in their leadership of the business;
- monitor the conduct of executives;
- question, debate, challenge and make decisions objectively;
- listen to the views of others inside and outside the board;
- gain the trust and respect of other board members;
- promote the higher standards of corporate governance;
- seek compliance with the provisions of applicable governance codes.

Corporate governance for a financial services organization

Corporate governance and risk management activities within a financial organization are strictly governed and regulated. Most financial organizations, including banks, produce their own internal corporate governance guidelines. Typically, these guidelines will cover director qualifications, director responsibilities and the responsibilities and delegated authority of board committees. The guidelines should also consider arrangements for the annual performance evaluation of the board and the arrangements for senior management succession.

The corporate governance structure will normally be a set of governing principles for the conduct of the board of directors. These governing principles will include

information for board members on dealing with conflicts of interest, confidentiality and compliance with laws, rules and regulations.

A major part of ensuring satisfactory corporate governance for a financial institution will be adequate training and induction for board members. Typically, the orientation programme for new members of the board will include details of:

- the legal and regulatory framework;
- risk management;
- capital management and group accounting;
- human resources and compensation;
- audit committee, internal audit and external audit;
- communication, including branding.

The global financial crisis resulted in banks and other financial institutions reviewing their corporate governance standards. The discussion in the next box provides an overview of a large national bank and sets out criticisms of that bank in relation to failures of corporate governance.

The Walker review of bank governance and regulation

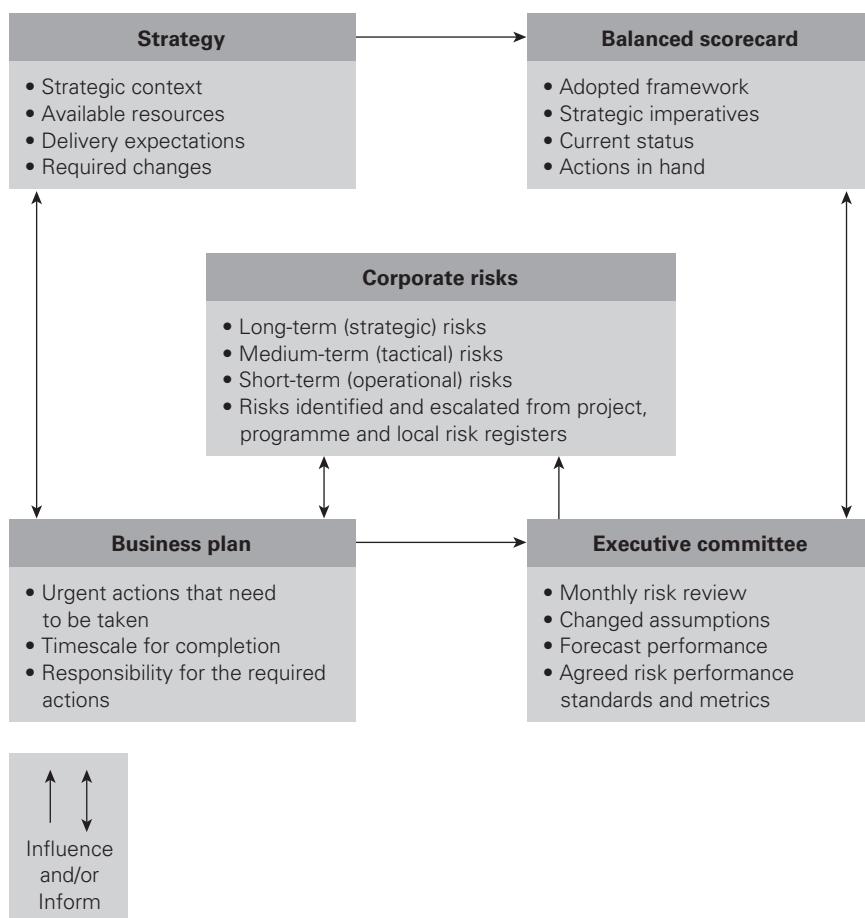
In 2009 Sir David Walker conducted a review of corporate governance in UK banks following the financial crisis. He gave the context for the review as follows:

[T]here were also material deficiencies in the effectiveness of boards in the well-publicized cases of some financial institutions and, albeit less directly, inadequate capability within major investing institutions to protect the interests of those for whom they act. Inadequate oversight by the boards and shareholders of the executive management of these BOFI entities and their collective failure to understand the new complex products resulted in spiralling enterprise-wide risk.

SOURCE Walker, D (2009) *A Review of Corporate Governance in UK Banks and Other Financial Industry Entities: Final recommendations (The Walker Review)*, https://webarchive.nationalarchives.gov.uk/ukgwa/+/www.hm-treasury.gov.uk/d/walker_review_261109.pdf

Corporate governance for a government agency

For government agencies, robust corporate governance arrangements are usually mandatory. Also, for many government agencies, the main reason for paying attention to risk management is to ensure that adequate corporate governance arrangements

Figure 29.2 Corporate governance in a government agency

are in place. In other words, the main motivation for ensuring good standards of risk management in a typical government agency will be the desire to support the corporate governance arrangements of the agency. Figure 29.2 shows the corporate governance components for a typical government agency.

For commercial organizations, corporate governance and risk management are designed to assist the organization to achieve its objectives, including commercial or marketplace objectives. The motivation for government departments to ensure good standards of corporate governance is narrower and is often focused on accountability.

In government agencies, the driving principles include value for money and avoidance of inappropriate behaviour. Corporate governance is often seen by government agencies as establishing a framework of control that supports innovation, integrity and accountability and encourages good management throughout the organization.

Within the corporate governance framework, responsibilities of individual members of staff are frequently specified. The reporting structure for risk issues is also outlined. Linking risk management efforts to corporate governance can also enable specific areas of risk to be identified for particular attention. Typically, these will include value for money, business continuity, fraud prevention and IT security assurance. Underpinning corporate governance activities within a government department, agency or authority will be the principles of public life, often referred to as the Nolan principles. These principles are set out in Table 29.2.

These principles have been in place since 1995 but they appear to have come under considerable strain during the Covid-19 health crisis in the UK in 2020 with the award of contracts to high-profile donors to the Conservative Party and with little (and often no) due diligence. The box below is an extract from the guiding principles for risk management set out by the UK government in *The Orange Book* under the section concerned with governance and leadership.

Table 29.2 Nolan principles of public life

1 Selflessness

Holders of public office should act solely in terms of the public interest and should not seek benefits for themselves, their family or friends.

2 Integrity

Holders of public office should not place themselves under any financial or other obligation to outside individuals or organizations.

3 Objectivity

In carrying out public business, the holders of public office should make choices on merit.

4 Accountability

Holders of public office are accountable for their decisions and actions to the public and must submit themselves to appropriate scrutiny.

5 Openness

Holders of public office should be as open as possible about all the decisions and actions that they take and give reasons for their decisions.

6 Honesty

Holders of public office have a duty to declare any private interests relating to their public duties and to take steps to resolve any conflicts.

7 Leadership

Holders of public office should promote and support these principles by leadership and example.

The Orange Book 2020 – Governance and leadership

Main principle

Risk management shall be an essential part of governance and leadership, and fundamental to how the organization is directed, managed and controlled at all levels.

Supporting principles

Each public sector organization should establish governance arrangements appropriate to its business, scale and culture. Human behaviour and culture significantly influence all aspects of risk management at each level and stage. To support the appropriate risk culture, the accounting officer should ensure that expected values and behaviours are communicated and embedded at all levels.

SOURCE HM Government (2020) *The Orange Book: Management of risk – principles and concepts*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866117/6.6266_HMT_Orange_Book_Update_v6_WEB.PDF

Evaluation of board performance

The board has overall responsibility for the organization in terms of setting strategy and ensuring satisfactory governance. Management of the organization is the responsibility of the executive management, and top management, by way of the executive directors of the organization, will often be members of the board. When executive and non-executive directors are members of the same board, this is referred to as a unitary board. In many organizations, the board comprises non-executive directors only, and is referred to as the supervisory board. Where a supervisory board is in place, the executive directors will meet as an executive committee. The separating of non-executive and executive directors into separate committees is sometimes referred to as a two-tier board structure.

The two-tier board structure is more common in some countries than in others, and often includes representation from the workforce as a mandatory requirement for large companies. It is usual for a two-tier board structure to be in place in charities and public sector organizations. Regardless of whether the structure is unitary or two-tier, the board will have a range of responsibilities. It is standard practice for the board to identify those issues where it will retain ultimate authority and responsibility. These issues are usually referred to as matters reserved for the board. A key area of responsibility for the board that is usually not delegated is setting the risk appetite of the organization.

Having decided the matters that are reserved for the board, it will then be necessary to decide how authority and responsibility will be delegated in respect of other

issues. It is common for large organizations to produce a statement of the delegation of authority, which will be an important document related to the governance structure in the organization.

Executive directors, managers and staff represent the three levels of management within an organization, and together these are the first line of defence in ensuring satisfactory standards of governance, including risk management and internal control. The board should be aware of specialist risk oversight functions within the organization and should be made aware of the activities of these functions and their role as the second line of defence. Non-executive members of the board would be the members of the audit committee and they should be aware of their functions as the third line of defence in ensuring adequate risk governance.

Evaluation of board performance is a critically important part of the corporate governance arrangements for any organization. Table 29.3 provides a checklist of issues that should be included in the evaluation of the effectiveness of a board.

Table 29.3 Evaluating the effectiveness of the board

Key area	Issues
Membership and structure	<p>Does the board have the necessary range of knowledge, skills and experience?</p> <p>Is there appropriate turnover of board membership to ensure new ideas?</p> <p>Are the sub-committees of the board effective, with appropriate delegated authority?</p> <p>Are board decision-making processes satisfactory, with adequate information available?</p> <p>Do communication processes exist between board members outside board meetings?</p>
Purpose and intent	<p>Do all board members understand and share the vision and mission?</p> <p>Do members of the board understand the objectives and position statements?</p> <p>Is there sufficient knowledge and understanding of the significant risks?</p> <p>Are board members sufficiently involved with the development of strategy?</p> <p>Have measurable budget and performance targets been put in place?</p>

(continued)

Table 29.3 (Continued)

Key area	Issues
Involvement and accountability	<p>Does the board have shared ethical values, including openness and honesty?</p> <p>Are the established policies unambiguous and consistent with the ethics?</p> <p>Do board members understand their duties, responsibilities and obligations?</p> <p>Is there a feeling of mutual trust and respect at board meetings?</p> <p>Are adequate delegation and authorization procedures in place?</p>
Monitoring and review	<p>Is there sufficient monitoring of performance using appropriate measurements?</p> <p>Does the board challenge planning assumptions when and where appropriate?</p> <p>Does the board demonstrate the ability to respond rapidly to changes?</p> <p>Is there a mentality that demands continuous improvement in performance?</p> <p>Does the board assess financial and other controls and seek assurance on compliance?</p>
Performance and impact	<p>Is there a satisfactory level of attendance at board, committee and other meetings?</p> <p>Are board decisions and actions fully recorded and actions tracked and confirmed?</p> <p>Are the agreed targets and performance indicators evaluated and assessed?</p> <p>Is the impact of board decisions and actions evaluated in a timely manner?</p> <p>Is there an emphasis on accuracy, honesty and open reporting to external agencies?</p>

The checklist set out in Table 29.3 focuses on corporate governance efforts and on the level of performance of the board. It can be supplemented by the FRC's *Guidance on Board Effectiveness* published in 2018, where 'questions for the board' include:

- What proportion of board time is spent on financial performance management versus other matters of strategic importance?

- Is the balance between the focus on immediate issues and long-term success appropriate?
- Is sufficient board time allocated to idea generation, opportunity identification and innovation?
- Are we securing the benefits of ‘big data’ to give us a competitive edge?
- Are shareholders driving the company to act in a way that is out of line with its purpose, values and wider responsibilities?
- How do we demonstrate ethical leadership and display the behaviours we expect from others?
- Is the board clear on what sort of culture is needed to underpin the company’s purpose and its long-term success?
- How consistent is company strategy – for example, on tax and capital allocation – with our purpose and values, and our responsibilities for long-term success and to contribute to wider society?⁴

When deciding issues related to strategy, tactics, operations and compliance, the board will need to ensure that adequate procedures are in place for reaching decisions. These decisions will result in a course of action and the implementation of that course of action needs to be monitored.

The course of action will result in some outputs, and these need to be evaluated in terms of the impact that is achieved. When evaluating the effectiveness of the board, the impact of its decisions is the ultimate test. The level of impact can then be evaluated against the vision, mission and objectives of the organization.

Notes

- 1 Financial Reporting Council (2018) *The UK Corporate Governance Code*, www.frc.org.uk/getattachment/88bd8c45-50ea-4841-95b0-d2f4f48069a2/2018-UK-Corporate-Governance-Code-FINAL.PDF (archived at <https://perma.cc/W6PM-JSTS>)
- 2 Mor, F and Browning, S (2020) *Corporate Governance Reform*, House of Commons Library Briefing Paper, 8143, <https://researchbriefings.files.parliament.uk/documents/CBP-8143/CBP-8143.pdf> (archived at <https://perma.cc/4H7T-FQ6B>)
- 3 Basel Committee on Banking Supervision and Bank for International Settlements (2012) *Core Principles for Effective Banking Supervision*, www.bis.org/publ/bcbs230.pdf (archived at <https://perma.cc/7822-8V4G>)
- 4 Financial Reporting Council (2018) *Guidance on Board Effectiveness*, www.frc.org.uk/getattachment/61232f60-a338-471b-ba5a-bfed25219147/2018-Guidance-on-Board-Effectiveness-FINAL.PDF (archived at <https://perma.cc/KC2B-8384>)

Stakeholders, ethics and corporate social responsibility

30

Range of stakeholders

The term ‘stakeholder’ applies to the many constituencies impacted by an organization. ISO Guide 83 suggests that the term ‘interested party’ is preferred, but stakeholder is an acceptable alternative. ISO Guide 73 defines a stakeholder as a ‘person or group concerned with, affected by, or perceiving themselves to be affected by an organization’.

There will be a wide range of stakeholders in a typical organization that can be summarized as CSFSRS, as follows:

- customers;
- staff;
- financiers;
- suppliers;
- regulators;
- society.

Stakeholders can be less directly related to the operations of a corporation than they initially expect, for example the taxpayers who funded the government rescue of banks during the financial crisis, and also funded businesses such as hospitality and events organizations during the health crisis, are all stakeholders.

Stakeholders may have contradictory expectations of the organization; for the boards managing those organizations this can lead to an ethical dilemma. For example, a traditional ‘theory of the firm’ in economics suggests companies exist to maximize profit making in any way that is legal. It has been argued that this attitude led to many of the scandals considered in the previous chapter. Certainly, it seems to have been the attitude that encouraged the high-risk strategy followed by HBOS (see Chapter 3). In this case the poor decision making of Mr Crosby hurt many millions of stakeholders.

Other examples can be found in manufacturing or chemical operations which were allowed, in the past, to discharge effluent and pollute rivers and lakes, making the water undrinkable and uninhabitable for fish and animals. In 2014 the water supply to residents of Flint, Michigan was changed from the Detroit Water and Sewerage Company to be sourced from Lake Huron to save costs. The subsequent lead poisoning inflicted on the population appears to have caused significant long-term problems for the childhood population as well as being a potential cause of Legionnaires' disease.

For organizations in different sectors, the range of stakeholders will be different. For government agencies, the general public will be a major stakeholder. Specific groups within the general public will be stakeholders in different agencies, depending on the purpose of each particular agency. For organizations that have significant environmental interests or exposures, a different range of stakeholders would need to be considered.

Rio Tinto, one of the world's largest mining companies, wrestled with such an ethical dilemma as shown in the next box.

Destruction of a 4,000-year-old Aboriginal heritage site to create new mine

In 2013, Rio Tinto received permission to conduct blasts at Pilbara mine site, Australia, under Section 18 of the WA Aboriginal Heritage Act. This removed the legal impediment to excavating ancient sites and legally allowed the destruction of ancient relics with proven genetic links to the present-day traditional owners, the Puutu Kunti Kurrama and Pinikura (PKKP) peoples. Archaeological digs conducted between 2013 and 2020 recovered richer finds than had been expected and the site was subsequently considered to be the oldest site of human occupation on the continent, with some of the earliest artefacts showing animal bones fashioned into tools.

In May 2020 the caves forming this ancient site were blown up to enable the mining activity to take place. This act caused outrage in the wider community, leading to intense criticism on social media and damage to Rio Tinto's reputation. This also led directly to an investor backlash, which caused the board to request the resignation of Chief Executive Jean-Sébastien Jacques, the head of the business unit concerned and also the head of corporate affairs. These three senior executives were forced to leave within five months of the explosion taking place.

The Chairman of Rio Tinto, Simon Thompson, was forced to apologize as he publicly stated the following 'We have listened to our stakeholders' concerns that a lack of individual accountability undermines the group's ability to rebuild that trust and to move forward to implement the changes identified in the board review.'¹

From the examples above it can be seen that the expectations placed on businesses have become wider than the pursuit of profit. There is now a greater need to balance the expectations of all stakeholders, and this will form the basis of the ISO 37000 standard. Additionally, this has also been led by the investor community which, far from requiring greater profits for their own sake, is calling for sustainable profitability with more emphasis on the ethical dimensions to that profit. The requirement to balance different stakeholder needs is one that falls squarely on the board and one that, as we can see, has an impact on the reputation of the organization. As has been seen, an organization's reputation is often its most valuable asset and therefore damage to this prized asset should be of concern to the risk management practitioner.

In March 2020 the FCA published proposals relating to the need for financial firms to disclose climate-related targets and their approach to investing in carbon activities and contributing to carbon reductions. It is very likely that these requirements will extend beyond the financial community into all other organizations and that boards will have not only an ethical duty to take climate-related activity into account but, increasingly, a legal duty to do so.

In May 2020 George Floyd was killed in Minneapolis, USA, during his arrest for allegedly passing off counterfeit currency. His death was seen by millions on social media and the brutal way in which the local police callously disregarded his call to be allowed to breathe instigated uprisings not only in the USA but across the globe. The event caused a mass outbreak of questioning around racism in society which may have been the only 'good thing' to have resulted from the poor man's demise. Organizations both large and small, public, listed and private have been forced to confront their approach and explain why there are so few black and ethnic minority representatives in the upper echelons of their management. The Black Lives Matter movement has, it seems, succeeded in raising this topic to the board level, where boards are now reporting (in a voluntary way to start with) their diversity component and differentials in pay amongst different ethnicities.

Stakeholder dialogue

Dialogue with stakeholders should be based on a mutual understanding of the objectives of the organization. The board is responsible for ensuring that the dialogue is satisfactory. Although specific members of the organization may have the day-to-day responsibility for communications with particular groups of stakeholders, the board will retain overall responsibility. Table 30.1 provides a summary of the information that should be provided to shareholders of a company. This information will focus on the provision of accurate financial data.

Table 30.1 Data for shareholders

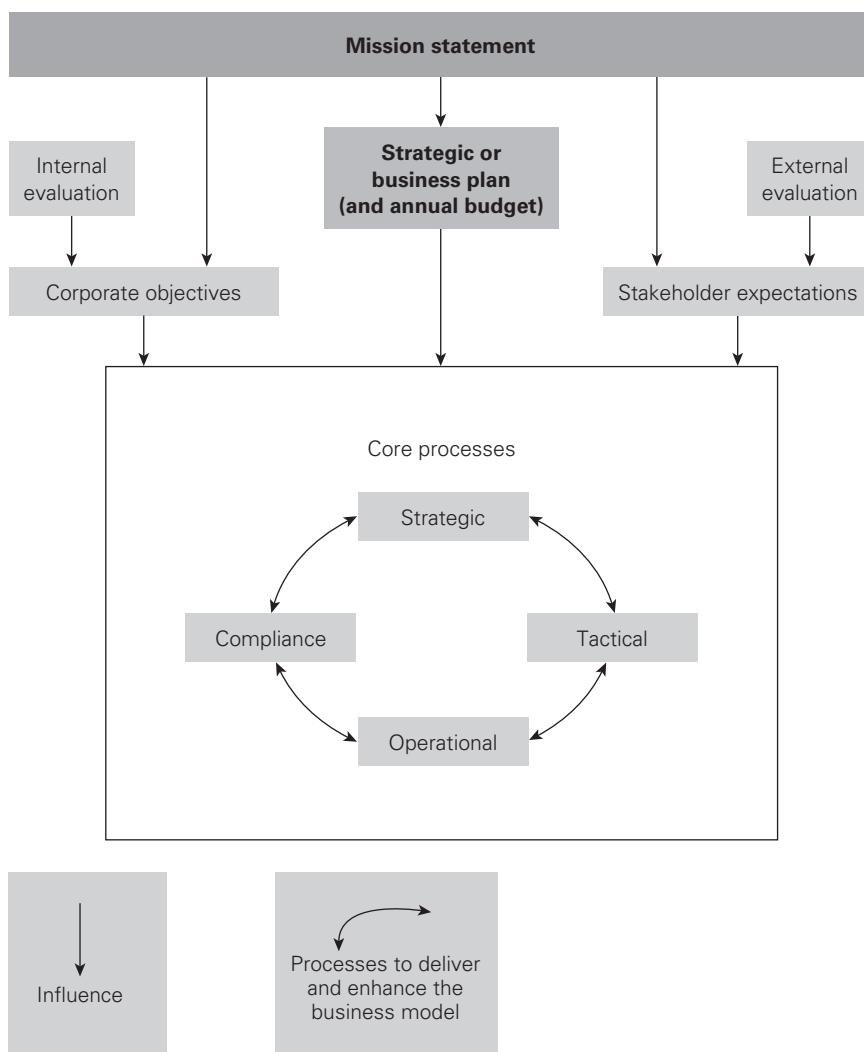
General	A clear statement of strategy and vision Corporate profile and principal markets
Financial data	Annual report and financial statements Archived financial information for the past three years
Corporate governance and CSR	Information related to compliance with Combined Code Information on the company CSR policies
Shareholder information	Shareholder analysis by size and constituent Information on directors' share dealings
Relevant news	Access to all news releases and presentations Developments that might affect the share value

The level and nature of dialogue with stakeholders will depend on the particular interests of the stakeholder in the operations of the organization. To obtain the full picture of the risks facing an organization, analysis of stakeholders and their expectations is necessary. The identification of stakeholder expectations is one output from the external evaluation stage of the business cycle. Different stakeholders may have expectations that are contradictory or even mutually exclusive in terms of the demands placed on the organization. The reporting of stakeholder engagement for larger companies has now been formalized, with Section 172 statements being required in strategy statements in the UK.

Stakeholders and core processes

Core processes deliver stakeholder expectations and are related to the internal and external context of the organization. Therefore, a risk can be defined as an event with the potential to impact the fulfilment of a stakeholder expectation. This approach has the advantage that both internal and external stakeholders can be identified, together with their short-term, medium-term and long-term expectations. Figure 30.1 provides a graphical illustration of the relationship between stakeholder expectations and the core processes of the organization. The figure illustrates that the core processes of an organization can be strategic, tactical, operational or compliance (STOC). Figure 30.1 shows compliance core processes as separate processes, although compliance core processes should also underpin and support the other types of core processes.

This classification of core processes as strategic, tactical and operational is acknowledged in British Standard BS 31100 when it discusses risk management perspectives.

Figure 30.1 Importance of core processes

Strategic perspectives set the future direction of the business; tactical perspectives are concerned with turning strategy into action by achieving change; and operational perspectives are related to the day-to-day operations of the organization, including people, information security, health and safety, and business continuity. Again, compliance processes are assumed to underpin the other types of core processes.

An approach based on stakeholder expectations has many advantages. It facilitates a full and thorough validation of the core processes of the organization in relation to the expectations that each stakeholder places on each core process. An important aspect of managing an organization is balancing the various stakeholder

expectations. There are dangers inherent in achieving this balance, and a risk identification procedure based on analysis of stakeholder expectations is the most robust way of ensuring that these dangers are recognized, analysed and minimized.

The analysis of stakeholder expectations is also one of the fundamental requirements of the business process re-engineering (BPR) approach. BPR is a technique to ensure that an organization has the most effective and efficient processes and operations. A starting point for many BPR exercises is to identify stakeholders and their expectations. The delivery of shared stakeholder expectations is then undertaken by the core processes of the organization. Core processes are the high-level collections of activities that are fundamentally important to the organization.

The stakeholders in the current and future activities of the organization can be identified. The expectations of each stakeholder in relation to each stated objective and the corporate mission can then be evaluated. Shared expectations will emerge and the core processes of the organization can then be defined (or refined) specifically in terms of the delivery of these shared expectations.

Although the analysis of stakeholder expectations can be one of the most robust ways of identifying risks, there are implications in terms of the time and effort required for this approach to be successful. BPR can be a very time-consuming exercise when undertaken thoroughly. The benefits of taking a BPR or core processes approach include the ability to identify the core processes that are most vulnerable to risk events. This will enable the identification of stakeholders who are more likely to be dissatisfied because their expectations have not been delivered.

Stakeholders and strategy

It has been clearly established and demonstrated by research that incorrect risk management decisions related to strategy can destroy more value for an organization than incorrect risk management decisions associated with the operations or projects undertaken by the organization.

Stakeholder expectations are delivered by the core processes of an organization. The core processes that deliver stakeholder expectations can be strategic, tactical, operational or compliance (STOC), shown in the bow-tie representation of the risk management process in Figure 11.1. Strategic core processes need to be the most robust processes in the organization, and indeed this will be required by major stakeholder groups. Such stakeholders include financiers and other shareholders who are interested in the long-term success of the organization. These may be termed primary stakeholders. In using stakeholder analysis to inform strategy, all stakeholders should be identified who may affect relationships with primary stakeholders. For example, an environmental pressure group may influence customers by suggesting that the products made by an organization fail to meet ecological standards.

Primary and secondary stakeholders could include:

- Primary stakeholders:
 - shareholders;
 - employees;
 - customers;
 - suppliers.
- Secondary stakeholders:
 - government – central or local government bodies;
 - media – press, broadcasters, online and especially social media;
 - consumer groups, pressure groups, community groups;
 - competitors.

Once identified, all stakeholders can be mapped and details of their level of interest and influence documented in order to consider the actions taken in respect of each stakeholder.

Stakeholders and tactics

Tactical stakeholders of an organization may be very different from those who are concerned with the organization's operations. If the tactics of an organization involve improvements to products, investment in new production techniques, response to technological changes or other developments that require a project, then finance is likely to be required. This means that financial bodies are likely to be key stakeholders in projects and similar tactical changes. Other stakeholders in projects may include building contractors and providers of other specialist professional support, such as architects.

The importance of employees in the implementation of tactics should not be underestimated. Staff will also have an interest in operational issues and be major stakeholders in the organization's operations. If changes to work practices or product features are to be successfully incorporated into the operations of the organization, then the support of staff is vitally important and good communication with them is essential.

It is important to consider the effect that changes, developments, projects and tactics will have on the full range of stakeholders. By considering the interests of stakeholders in detail, many unexpected surprises can be avoided. The impact of the project, both in execution and after delivery of the project, should be considered in detail. This consideration should extend both to internal and external stakeholders

for whom the changes that the project will bring may be significant. These changes could relate to environmental factors during the construction project and after the work has been completed, as well as changes to the working arrangements for staff.

It may be a good idea to bring some people who are not directly involved in the activities of the organization into the project planning. This will enable the organization to fully understand the impact of the work that will be undertaken. When considering stakeholder management, the level of detail will often dictate whether engagement with stakeholders is successful. Even with successful projects, being able to minimize negative impacts by early attention to key stakeholders and their expectations may prove invaluable.

Stakeholders and operations

There may be many stakeholder groups involved in the operational activities of an organization. For example, pharmaceutical companies have a very diverse range of stakeholders, and especially so during the health crisis caused by Covid-19. Both Astra Zeneca and Pfizer were involved in producing vaccines of different types for Covid-19 and had an obligation to ensure a constant availability of that medication. Governments were the main customers but stakeholders included all patients and wider society as a whole.

The stakeholder groups that have an interest in the operational activities of an organization are likely to be customers, suppliers and others that may be affected by disruption to the normal efficient operation of the organization. For example, customers are likely to be affected if a hazard risk were to materialize. Likewise, suppliers are stakeholders in the organization and they will suffer if the organization is disrupted to the extent that their supplies/produce/components/services are no longer required.

Other stakeholder groups that are likely to be affected by hazard risks will also have an interest in the continuity of the activities of the organization. For financial organizations such as banks, customers would be immediately affected if critical IT systems fail. The Bank of England, FCA and Prudential Regulation Authority (PRA) published a policy statement on ‘Operational resilience: Impact tolerances for important business services’ in March 2021, specifically referencing the need for organizations to:

- identify their important business services by considering how disruption to the business services they provide can have impacts beyond their own commercial interests;
- set a tolerance for disruption for each important business service; and

- ensure they can continue to deliver their important business services and are able to remain within their impact tolerances during severe (or in the case of FMIs, extreme) but plausible scenarios.²

The regulators also specifically require the board to approve the important business services identified for their firm and the impact tolerances that have been set for each of these.

Corporate governance models require the involvement of stakeholders and adequate stakeholder dialogue. In several countries, employees are recognized as stakeholders in the organization to the extent that employee representation on the board may be mandatory.

Notes

- 1 Rio Tinto (2020) Juukan Gorge, www.riotinto.com/news/inquiry-into-juukan-gorge (archived at <https://perma.cc/E4NB-UK9V>)
- 2 Bank of England, PRA and FCA (2021) *Operational Resilience: Impact tolerances for important business services*, www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/publication/2021/building-operational-resilience-impact-tolerances-for-important-business-services.pdf?la=en&hash=D6335BA4712B414730C697DC8BEB353F3EE5A628 (archived at <https://perma.cc/MK4H-EM27>)

Different approaches to risk management

31

In this chapter we will review the specialist approaches to risk management for operational risk management, project risk management and supply chain risk management. Operational risk management covers a variety of risk types, which include cyber, ICT and change management, the individual specifics of which are beyond the scope of this book. Additionally, specialist areas such as credit risk management are beyond the scope of this book.

Operational risk management

The importance of managing operational risk is well established. Operational risk may be considered to be the type of risk that will disrupt normal everyday activities and that is inbuilt into the activities, processes and controls that deliver the main activities of an organization. The main goal of good operational risk management is to build operational resiliency and process reliability. In many ways, operational risk is closely related to infrastructure risks described in the FIRM risk scorecard classification system.

The Basel Committee on Banking Supervision in their *Principles for the Sound Management of Operational Risk* states:

The Principles in this document for banks cover governance; the risk management environment; information and communication technology; business continuity planning; and the role of disclosure. These elements should not be viewed in isolation; rather, they are integrated components of the operational risk management framework (ORMF) and the overall risk management framework (including operational resilience) of the group.¹

Operational risks now have a specific definition, especially in financial institutions. Whilst addressing the same types of risks, operational risk in financial institutions is differentiated by the fact that there is a need to quantify these risks in terms of potential financial loss.

Financial institutions are required to have sufficient capital reserves available to meet the actual and potential financial losses and obligations faced by the organization in severe but plausible scenarios. This is a key requirement of the regulatory framework set out for banks in the Basel III Accord and under regulation for European insurance companies through the Solvency II European Directive. Under these regulations, financial institutions need to measure the level of operational risk that they face and could face under stressed conditions.

The capital adequacy regulations that are based on Basel II require that banks take their operational risk exposure into account in determining their capital requirements. This operational risk management framework should include identification, measurement and monitoring, reporting, control and mitigation frameworks for operational risk. This assessment of capital requirements is often called economic capital. Under Basel II the regulations require that banks must follow one of three specific quantitative methods to provide another measure of capital requirement.

Basel III is one part of the Basel Accords that set out recommendations on banking laws and regulations, as issued by the Basel Committee on Banking Supervision (BCBS). Its purpose is to build on previous regulations and build an international standard that banking regulators can use when creating regulations about how much capital banks need to put aside to guard against the types of financial and operational risks they face. The implementation of Basel III requirements has been repeatedly pushed back and it is expected that they will come fully into force in January 2023 (postponed from January 2022 due to the Covid-19 pandemic).

Basel III sets a revised Standardized Approach (SA) framework to calculate minimum operational risk capital requirements that will replace the three-calculation methods part of Basel II and, in doing so, is expected to improve comparability across banks.

Definition of operational risk

Operational risks faced by banks and other financial institutions represent essentially the same types of disruptive hazard risks that are faced by other organizations, although the definition may be broader and the terminology slightly different. The specific point in the case of operational risk for financial institutions is that the level of operational risk needs to be quantified, because the level of risk has to be covered by available capital within the institution. This leads to an imperative for the bank to reduce the level of operational risk to the lowest level that is cost-effective.

Banks have long been concerned with market risk and credit risk (and insurance companies with underwriting risk as well), but the advent of Basel II and Solvency II requires financial institutions to consider broader operational risk exposures. Operational risk was initially defined as being any form of risk that was not market

risk or credit risk. This imprecise definition was replaced by Basel II with a definition of operational risk as: ‘the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events’.

The Basel II definition includes legal risk, but excludes strategic and reputational risk. The types of risks associated with the Basel II definition include the following:

- internal fraud, including misappropriation of assets, tax evasion and bribery;
- external fraud, including theft, hacking and forgery;
- employment practices and workplace safety;
- clients, projects and business practices;
- damage to physical assets;
- business interruption and systems failures;
- execution, delivery and process management.

However, there is also recognition that operational risk is a term that has a variety of meanings and that certain financial institutions use a different term or a broader definition. The Basel II definition identifies four types of risk categories: people, process, system and external events. People risks include failure to comply with procedures and lack of segregation of duties. Process risks include process failures and inadequate controls. System risks include failure of applications systems to meet user requirements and the absence of built-in control measures.

Finally, external risks include action by regulators (change of regulation, but excluding enforcement or disciplinary action), unsatisfactory performance by service providers and external fraud. External risks also include legal action by customers of financial institutions in relation to negligence or fraud committed by staff as well as natural disaster, terrorism and other external events that could cause business interruption.

The definitions of market risk and credit risk are also worth considering in relation to financial institutions. Market risk is the risk that the value of investments may decline over a period, simply because of economic changes or other events that impact large portions of the market. Credit risk is the risk that there will be a failure by a customer/client to repay the principal and/or interest on a loan or other outstanding debt in a timely manner, or at all. Underwriting risk is also important for insurance companies; it is the exposure to the risks of the client through insurance policies.

The losses associated with the failure to manage operational risk can be very substantial. Losses suffered by so-called rogue traders are sometimes attributed to market risk. The argument is that the losses occurred because market conditions changed in an unexpected way and significant losses materialized. From an operational risk perspective, this analysis is incorrect. However, it is more correct to say that the losses occurred because of a failure to control the activities of traders. If the operations had been controlled by adequate operational risk controls, the traders would

not have been in a position to have put substantial assets of the bank at risk. Blaming the losses on the market risk when such substantial assets of the bank should not have been in the market at all, is incorrect.

Failure of operational risk management

Operational risk management is at a crucial point in its development. Numerous approaches have been developed across different industries, but many institutions are struggling to make these fully effective by really embedding them into the day-to-day management of their business. In order to overcome this challenge, it is essential to define clearly the relationship between operational risk processes and the overall control environment.

Indeed, the effectiveness of operational risk management has been impeded by a common failure to truly embed operational risk into the overall management of risk and control. Group risk functions must demonstrate to business-unit staff the full potential of using operational risk processes, developed under the group framework to manage the actual risks in the business.

As a consequence, the governance of operational risks involves more than just calculating the yearly operational risk capital. As economies and financial conditions change over time, so does the operational risk exposure. This implies that a number of specific operational risk events may become even more likely, which in times of crises require the attention of top management.

Table 31.1 ORM principles (Basel II)

The 12 principles on ‘Sound Practices’ of the Basel Committee on Banking Supervision are as follows:

Principle 1: Risk culture	Places the emphasis on senior management to implement a strong risk culture and recommends that the code of conduct should be reviewed and approved by the board, attested to by employees, its implementation overseen by a senior ethics committee, and be publicly available.
Principle 2: Operational risk management framework (ORMF)	Recommends the board of directors and management to understand the nature and complexity of risks inherent in their systems.

(continued)

Table 31.1 (Continued)

Principle 3:	The board of directors	Emphasizes the board responsibility to ensure ownership by senior management.
Principle 4:	Risk appetite	Recommends that the operational risk appetite should be easy to communicate and understand. It should clearly articulate the motivations for assuming or avoiding certain types of risk.
Principle 5:	Senior management	Emphasizes senior management's responsibility for risk.
Principle 6:	Identification and assessment in usual operations	Lists the tools used to identify and assess risk including detail on the qualitative and quantitative analysis involved in the RCSA process and the documentation required.
Principle 7:	Identification and assessment in change	Clarifies how the three lines of defence operates during change. It further recommends central records of products and services are maintained to facilitate the monitoring of changes.
Principle 8:	Monitoring and reporting	Makes clear senior management's duty to monitor and report on risk issues including emerging risks.
Principle 9:	Control and mitigation	Banks should have a strong control environment that utilizes policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.
Principle 10:	Information and communications technology	Banks should implement a robust ICT risk management programme in alignment with their operational risk management framework.
Principle 11:	Business continuity planning	Banks should have business continuity plans in place to ensure their ability to operate on an ongoing basis and limit losses in the event of a severe business disruption.
Principle 12:	Disclosure	A bank's public disclosures should allow stakeholders to assess its approach to operational risk management and its operational risk exposure.

In March 2021 the BCBS updated the *Principles for the Sound Management of Operational Risk*, reflecting the natural relationship between operational resilience, operational risk and Basel III reforms. The 12 principles of 'sound practices' on operational risk put forward by the Basel Committee are set out in Table 31.1.

The Basel Accords describe a comprehensive minimum standard for capital adequacy that national supervisory authorities are working to implement. They are intended to

promote a more forward-looking approach to capital supervision that encourages banks to identify the risks they face and improve their ability to manage those risks. As a result, it is intended to be more flexible and better able to evolve with advances in markets and risk management practices.

Measurement of operational risk

Operational risk has become a specific issue in financial institutions because of the requirement to measure/quantify the level of operational risk that they face. The measurement of operational risk can involve a number of methods, and these are normally based on historical information, simulated information or a combination of both. Table 31.2 sets out examples of operational risks faced by a bank or financial institution.

Table 31.2 Examples of operational risks faced by a bank or financial institution

Event category	Definition	Description	Examples
Internal fraud	Losses due to fraud, misappropriation or circumvention of regulations by internal party	Unauthorized activity, theft and fraud	Unreported transactions Unauthorized transactions Theft and fraud Tax non-compliance Insider trading
External fraud	Losses due to fraud, misappropriation or circumvention of the regulations by third party	Systems security, theft and fraud	Theft/robbery Forgery Hacking/theft of information
Employees	Losses arising from injury or non-compliance with the employment legislation	In a safe environment, damaged employee relations and discrimination	Compensation claim Discrimination allegation
Clients	Losses arising from failure to meet professional obligations to clients	Disclosure and fiduciary	Fiduciary breaches Disclosure violations Misuse of confidential information
Physical assets	Losses arising from loss or damage to physical assets	Disasters and other events	Natural disaster losses Terrorism/vandalism

(continued)

Table 31.2 (Continued)

Event category	Definition	Description	Examples
Systems	Losses arising from disruption of business or system failures	Systems	Hardware or software failure Telecommunications Utility disruption
Processes	Losses from failed transaction processing or process management	Transaction capture, execution, documentation and maintenance	Data entry or loading error Missed deadline or responsibility Failed reporting obligation Incorrect records

Basel III now provides a standardized approach to measuring operational risk for regulatory capital purposes, which is a function of a bank's income (captured through a Business Indicator) and historical losses (captured through the Internal Loss Multiplier).

In order to measure operational risk, the financial institution needs to adopt a structured approach. Even after the identification of the risks, quantification is only possible if the amount of damage and risk probabilities are determined. Operational risks are hard to quantify but attempts have been made using third-party databases maintained by consortium data, for example operational risk exchange.

Difficulties of measurement

The development of interest in operational risk has been based on the need to quantify operational risk in financial institutions. The challenges of quantifying operational risk have been considerable and this is recognized by the PRA, the UK regulator. Expected levels of loss can only be estimated even if the probability of loss is fairly accurately known, risk types under operational risk are varied and the loss distributions are difficult to create due to lack of data, especially for extreme events. Although statistical approaches have been adopted and developed, a universally accepted approach is still not available.

The expected losses can have a direct and indirect cost. Indirect costs are often larger, and include the loss of a customer. This loss can be represented by the present value of that customer and all future gains from that relationship. Actions that should be taken will include internal control measures as well as evaluation by internal audit. Internal audit within a financial institution has the familiar, but vitally important, responsibility of checking whether procedures are followed in practice and whether the procedures themselves are likely to be effective in reducing the level of operational risk.

Table 31.3 Operational risk in financial and industrial companies

Financial	Industrial
Errors mostly arise when people reach their mental limits.	Errors are mostly due to people reaching their physical limits.
Systems are highly complex and widely distributed and the environment is only partly manageable.	People are working in relatively simple relationships and the environment is highly manageable.
Loss prevention is concerned with security of value and assets.	Loss prevention is mainly concerned with physical safety, equipment protection and avoiding accidents.
Loss prevention is aimed at avoiding financial loss.	Loss prevention is aimed at avoiding physical harm to people or equipment and/or the manufacture of faulty goods (scrap).
The main incentive for committing mistakes is personal financial gain or self-interest.	The main incentive for making deliberate mistakes is reducing effort or (possibly) sabotage.
Risk management is a key skill in financial services and has central importance to the organization.	Risk management is not central to operations, although the aim is to avoid disruption to manufacturing processes.

Table 31.3 illustrates the different natures of operational risk faced by financial and industrial companies. The table provides a comparison of the nature and impact of human error in a financial institution, compared with an industrial undertaking. It is clear that the control of staff behaviour and actions is much more difficult in financial institutions than in manufacturing facilities.

It is worth noting that operational risk quantification is possible for non-financial institutions, and a transport company (for example) could investigate the operational risks associated with its activities. The risks associated with the operations include the price of fuel, tax obligations and the financial impact of delivery mistakes. Operational risks can arise from road traffic accidents or other delivery delays and changes by customers that have not been correctly incorporated into the delivery schedule.

It is likely that the most important operational risks faced by a transport company would be incorrect customer deliveries and road traffic accidents. The quantification of risk exposures associated with the various categories of operational risk will help a transport company focus on those risks with the greatest potential to cause disruption to normal efficient routine operations, and then take the appropriate control actions to reduce these operational risk exposures.

Developments in operational risk

Before considering developments in operational risk, it is worth noting that concerns about operational risks are universal in all organizations. Although the banks and other financial institutions may have a specific approach to operational risk, the issues that are being considered are the same issues that affect all other types of organizations in the public, private and third sectors. (The third sector refers to not-for-profit organizations, including charities, membership and voluntary bodies.)

Although the issues are the same, the approach in banks and other financial institutions can be different. In a non-financial institution, the questions related to operational risk may well be: 'What is the value of my assets, how do I protect them and to what extent and value (or limit of indemnity) do I need to purchase insurance?' In the financial sector, the questions are more likely to be: 'What are the capital requirements attached to my assets?' and 'Can I afford to keep that amount of (non-productive) capital in reserve or do I need to purchase insurance, and to what value or limit of indemnity?'

It is generally accepted that operational risk concerns need to be integral to the management of a financial institution. It is often the case that management trainees within financial institutions spend some time in the risk management function, as they progress with their career in the general management side of the business. It is the intention that this involvement with risk management will create greater awareness before the individual progresses into other roles.

The measurement of operational risk in financial institutions is still proving to be a challenge, and the global financial crisis showed that the extent of operational risk exposure was greater than most banks believed. Certain financial institutions are seeking to adopt risk management standards, such as ISO 31000, the IRM standard and the COSO ERM cube.

The responsibility for the management of risk and the implementation of controls usually rests with line managers. If this responsibility is not accepted, there is a danger that operational risk management will not be fully integrated into management of the financial institution with disastrous consequences, and this is emphasized by the Sound Principles guidance from the Basel Committee.

Calculation of operational risk exposure is a requirement of both Basel II and III, and financial institutions therefore have to undertake this work. Financial institutions are driven by increasing regulatory demands and other corporate governance pressures. Raising the level of operational risk awareness by quantifying the level of risk and explaining the full significance of risk management to relevant members of staff should be to the benefit of the organization. This increased awareness will enable the organization to identify the sources of operational risk and take appropriate cost-effective actions to optimize the level of operational risk exposure.

Project risk management

Projects will be undertaken by organizations for a number of reasons. When alterations to strategy are being planned, a project (programme of work) or series of projects will often be necessary in order to implement the revised strategy. Also, improvements to operational core processes will require changes that will be implemented by undertaking a project. Selection of projects and programmes of work defines the tactics of the organization for the implementation of strategy.

It is important to draw a distinction between project risk management, which is about delivering the project on time, within budget and to quality, and the reason why the project was undertaken. Project risk management is concerned about the risks embedded within delivery of the project. There are also the risks of the project and whether the project is the correct allocation of funds. The risks of the project can be identified by asking whether: 1) the full benefits of the project will actually be delivered; and 2) this particular project represents the best tactics for delivering strategy.

The London Olympics 2012 is an example of a major project that was delivered on time, within budget and to quality. Whether staging the Olympic Games in London in 2012 was a correct decision and whether the legacy of the Olympic buildings and other infrastructure has been delivered is a much broader issue.

Project risk management should be seen as an extension of conventional project planning. The main requirements for any project are that it is delivered on time, within budget and to specification or performance. Risk is often defined in terms of uncertainty or deviation from the expected/required outcomes. It is in relation to project risk management that the definition of risk being represented by uncertainty is most relevant. Within project management, variability of outcomes is very undesirable. Therefore, the focus of risk management in projects is often on the reduction in the variability of outcomes and the management of control risks.

There will be uncertainties within any project related to events, conditions and circumstances. The requirements of project risk management are to identify the events that could give rise to uncertainty and respond to these events appropriately. The style of risk management most relevant to project risk management is control management.

As well as managing the risks and uncertainties in a project, the project manager should also be looking for opportunities that may arise when certain developments within the project are more favourable than expected. Project risk management should take account of these positive developments and ensure that the structure for managing risks in projects is sufficiently flexible for the opportunities to be recognized and benefits obtained.

For example, consider a project of building a new road where one of the bridges can be completed well ahead of schedule because of favourable ground conditions. There may be an opportunity to build the benefit of this early completion into the future project plan, so that this gain is not lost in the overall timescale for delivery of the final completed project.

Development of project risk management

Project risk management is a type of control management. Projects may relate to the delivery of a finite, specific or tactical development or process enhancement, such as new:

- construction;
- products;
- IT systems;
- technology;
- markets.

Projects and enhancements are fundamentally important to organizations. Most projects are undertaken either to keep ahead of competitors or to catch up with them. Some projects will implement remediations and/or mitigate risk as well. In the context of risk management, the project itself may be considered to be a risk reduction exercise that is designed to achieve specific management objectives.

Project risk management is a well-developed discipline, with risk control and (especially) event management as the risk management activities that are most important. The requirement for all projects is that they are delivered within the defined cost, time and quality parameters. Delivering a project is often considered in terms of a project triangle bounded by time, cost and quality. If the project is delivered perfectly the triangle will remain in proportion, but if less time is allotted, then either the cost will go up or the quality reduce. Similarly, if the cost of the project reduces it will affect the time allowed and the quality of the output.

Quality is the relationship between specification and performance. Some projects require that the outcomes comply with a certain specification, such as a new floor in a restaurant that has to be constructed from specified materials. Other projects may require a desired level of performance, such as specifying the level of slip resistance of the floor. Sometimes, both a specification and a performance will be required.

Because of the nature of projects, historical loss data will not usually be available. Accordingly, project risk management needs to be forward-looking in order to anticipate problems before they arise.

Compliance hazard, control and opportunity risks need to be considered as part of the successful management of any project. There are risks associated with failure to obtain necessary permissions and approvals (compliance risks). There are risks to the project that can prevent it being delivered on time and within budget (hazard risks). There are risks to the project concerning the specification, performance and quality of the final outcome (control risks). Finally, there are risks that can enhance the delivery of the project, such as earlier than expected availability of materials (opportunity risks).

Uncertainty in projects

In order to manage uncertainty in projects, organizations have a range of possible actions they can take. An organization can decide to respond in one of the following ways:

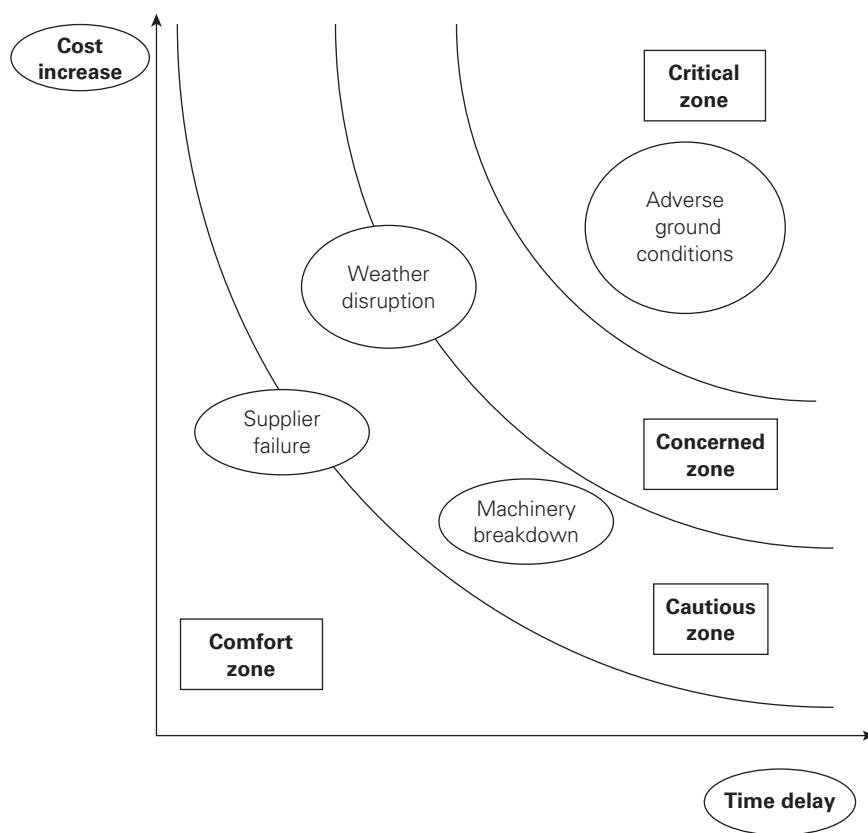
- accept the risk or uncertainty;
- adapt activities and procedures;
- adopt contingency plans and responses;
- avoid the risk or uncertainty.

For low-exposure/low-uncertainty risks, the organization (or project) will usually accept uncertainty attached to each risk. For high-exposure/low-uncertainty risks, the organization will adapt activities and procedures and introduce controls, including (when appropriate) insurance. For low-exposure/high-uncertainty risks, the organization will adopt appropriate contingency plans, and for high-exposure/high-uncertainty risks, the organization will wish to avoid the uncertainty attached to the risk.

Figure 31.1 illustrates the use of the risk matrix to plot the possible range of risks on the project. The matrix plots the possible time delay that could result against the potential for cost increases associated with that event. This diagram will help the project manager identify whether the risks fit into the comfort, cautious, concerned or critical zones. The other variable shown in the diagram equates to the likelihood of each event occurring, and this is indicated by the size of the bubble used to represent that risk.

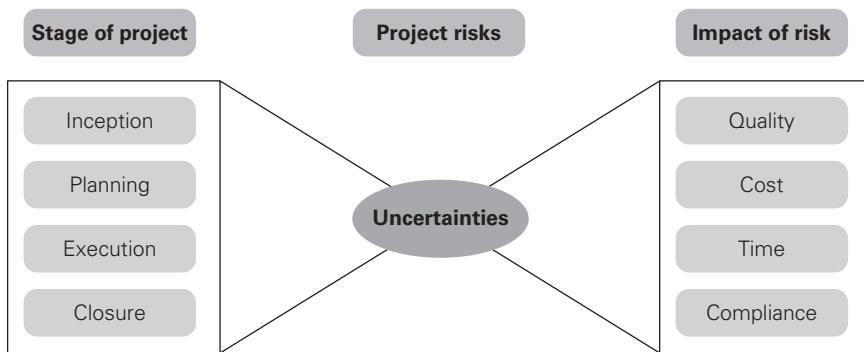
The delivery of the Olympic Games in London in 2012 required the biggest construction project undertaken in London during the second half of the first decade of the 2000s. During the course of construction, the global financial crisis arose and the financial structure for delivering the project had to be renegotiated. Although this was a major concern, it was successfully completed. Figure 31.1 identifies adverse ground conditions as a possible cause for concern in any construction project. In the

Figure 31.1 Risk matrix to represent project risks



case of the Olympic Games 2012, the construction of the Olympic village received a boost in terms of time and cost because the ground was found to be less contaminated than expected.

Figure 31.2 represents the risk management process in project management as a bow-tie. In this use of the bow-tie, the sources of risk are shown as inception, planning, execution and closure. At the centre of the bow-tie are the uncertainties associated with the project, because the management of uncertainties is the essence of project risk management. The purpose of this bow-tie representation is to illustrate that controls can be introduced to reduce the uncertainties in the centre of the bow-tie, manage the uncertainties as they arise, and introduce further controls to limit the impact of those uncertainties on quality, cost, time and compliance.

Figure 31.2 Bow-tie to represent project risks

NOTE Size of bubble represents likelihood.

Project risk register

A risk register or risk matrix should be populated and updated regularly throughout the duration of the project. A risk management software tool can often be a cost-effective way of maintaining your risk register as it can reduce the manual workload and help prioritize risk management activity.

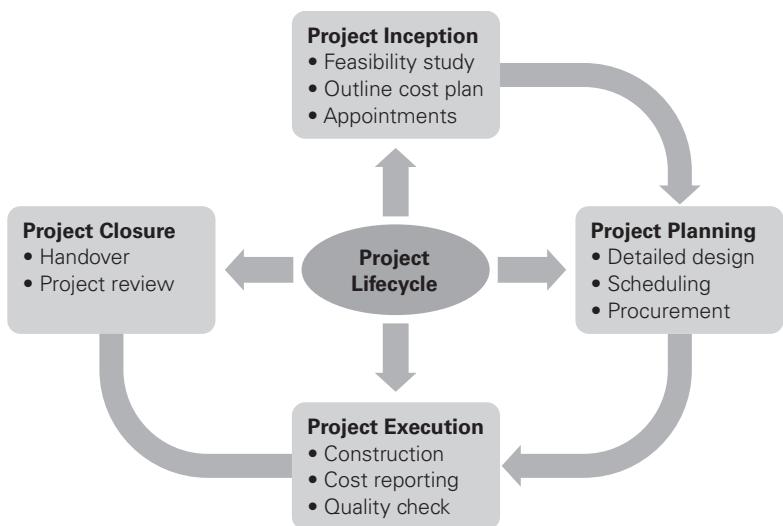
Once risks have been identified and plans to reduce them put in place, it is imperative that they are reviewed regularly. The internal and external project environment is continually changing. Some risks will fall away, others will arise that could never have been envisaged at the outset.

The risk register must therefore be continually updated and reports generated at regular and frequent intervals. Management reports should provide clear visibility on the risks faced, enable prioritization of the activity and facilitate decision making.

Project lifecycle

Project risk management has become one of the best-developed and respected branches of risk management. This is not surprising, given the dynamic and pressured environment in which many projects are undertaken. Projects can range in size, but however large or small the project, a number of specific stages will always be present. Figure 31.3 illustrates the key stages in the project lifecycle. An important additional feature of project risk assessment is that the requirements of the client should always be of the utmost importance. The client may be external to the organization, but is sometimes part of the same organization.

Figure 31.3 Project lifecycle



SOURCE Reproduced with permission from Feasible.

Figure 31.3 sets out the project lifecycle as having four stages. These are project inception, project planning, project execution and project closure. The activities within each of these four stages are listed in the figure. It is important to understand the stages in the project lifecycle, so that the risk management inputs into each stage can be planned and executed, and the required benefits obtained.

The risk management process as applied to project management is similar to the standard risk management process discussed in Chapter 6. However, the framework that supports the risk management process in each case may be quite different, because of the dynamic nature of the projects.

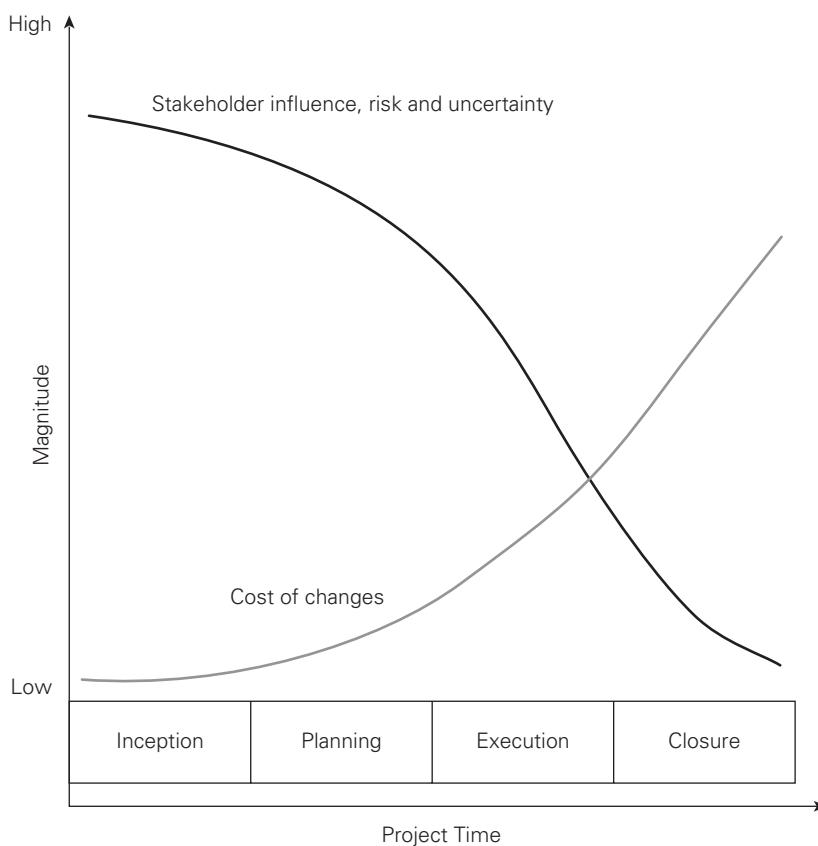
Each stage of the project lifecycle will have significant risk and uncertainty embedded within it. The uncertainty embedded in each stage of the project will include such issues as defining the project precisely, agreeing the timescale and budget, and confirming the performance/specification. There will also need to be arrangements for changes and developments within the project specification, as well as arrangements for any deviation from expected circumstances.

Figure 31.4 illustrates how uncertainty decreases during the various stages of a project. Many organizations include a fourth variable in the project triangle. This uncertainty may relate to the scope of the project, the effectiveness of the tactics that gave rise to the project or the ability of the project to comply with stakeholder expectations. The stakeholders will almost certainly include regulators, and so compliance is often added as the fourth output from a project that has to be successfully delivered. Sustainability is also used by some organizations as an alternative fourth

output from a project. The simple approach is to include compliance and sustainability as part of the third output of quality, specification or performance. Successful management of a project will require the following:

- making risk management part of the project;
- identifying risks early in the project;
- communicating about risks;
- considering both threats and opportunities;
- clarifying ownership issues;
- prioritizing risks;
- analysing risks;
- planning and implementing risk responses;
- registering project risks;
- tracking risks and associated actions.

Figure 31.4 Decreasing uncertainty during the project



Opportunity in projects

Projects are undertaken because they represent an opportunity to be embraced or a challenge that needs to be overcome. Often a number of projects will need to be undertaken at the same time. A collection of projects of this sort is referred to as a programme.

Good project planning requires arrangements to overcome unexpected events or circumstances. This is often referred to as contingency in the budget or timescale. Contingency may be for additional time to complete a task, or additional costs that may arise to ensure that the final project deliverable operates to the required specification. As the project develops, any perceived difficulties will need to be addressed and opportunities to reduce the impact of these difficulties explored.

Very frequently, the specification of a project will change during the course of the work. A well risk-managed project will take the opportunity of change to specifications to provide a greater level of customer satisfaction, as well as a greater level of income for the organization delivering the project.

The main opportunity offered by undertaking a project is that the project will prove to be the correct tactic for delivering the strategic objectives. In some organizations, projects are only authorized if they reduce the risks faced by the organization. This is particularly true in energy companies, where the justification for undertaking projects will be to improve output, efficiency or quality of operations. This in turn reduces the risk associated with reduced output, wasted resources and poor quality.

As well as achieving the opportunities offered by undertaking the project, organizations will also wish to take advantage of opportunities that are offered within the project. These opportunities may reduce costs, reduce time and/or increase quality. For example, as was the case with the 2012 Olympics, if a construction project assumes a certain level of ground contamination but this proves to be less than expected, there would be an opportunity for the project to be delivered ahead of schedule and at reduced cost. Some construction project contracts will include clauses to share the benefits should the circumstances arise.

Within many established cities, there are archaeological remains that may be of considerable historical interest, if uncovered during the excavation phase of the project. When undertaking construction work to replace buildings in old cities around the world, there is a chance that the construction company will come across such archaeological remains. Cautious construction companies will plan for this eventuality and build the consequences into the project plan. The possible time delays introduced by finding archaeological remains can be built into the project timeline, and the increased costs associated with these delays may be covered by archaeological insurance, if it is available at a cost-effective price.

Table 31.4 PRAM model for project RM

Project risk analysis and management is a process that enables the analysis and management of the risks associated with a project

Properly undertaken, it will increase the likelihood of successful completion of a project to cost, time and performance objectives.

Risks for which there is ample data can be assessed statistically.

However, no two projects are the same.

Often, things go wrong for reasons unique to a particular project, industry or working environment.

Dealing with risks in projects is therefore different from situations where there is sufficient data to adopt an actuarial approach.

Because projects involve a technical, engineering, innovative or strategic content, a systematic process is preferable to an intuitive approach.

Project risk analysis and management (PRAM) has been developed to meet this requirement.

Project risk analysis and management

The Association for Project Management (APM) developed the project risk analysis and management (PRAM) guide in the mid-1990s. The key considerations that underpin the PRAM approach are set out in Table 31.4. Perhaps one of the most important points made is that there is often no historical experience specific to the project that will enable accurate prediction of the impact of risk-based events. The PRAM guide provides steps to project risk management that are broadly consistent with the steps outlined above.

The PRAM approach represents a continuous set of activities that can be started at almost any stage in the lifecycle of a project. There are five points in a project where particular benefit can be achieved from using the PRAM model:

- 1 Feasibility:** At this stage the project is most flexible, enabling changes to be made that can reduce the risks at a relatively low cost.
- 2 Sanction:** The client can view the risk exposure associated with the project and check that all steps to reduce/manage the risks have been taken.
- 3 Tendering:** The contractor can ensure that all risks have been identified and that risk contingency or risk exposure limits have been set.
- 4 Post-tender:** The client can ensure that all risks have been identified by the contractor and assess the likelihood of programmes being achieved.
- 5 During implementation:** The likelihood of completing the project to cost and timescale will increase if all risks are identified and correctly managed.

Supply chain risk management

ISO 28000:2007 Specification for Security Management Systems for the Supply Chain provides the following definition of supply chain:

A supply chain is a set of interconnected processes and resources that starts with the sourcing of raw materials and ends with the delivery of products and services to end users. Supply chains may include producers, suppliers, manufacturers, distributors, wholesalers, vendors, and logistics providers. They include facilities, plants, offices, warehouses, and branches and can be both internal or external to an organization.

Many organizations outsource major parts of their operations and support services. This can range from the use of contract cleaners through to transport, communications and manufacturing outsourcing. Many leading suppliers of fashion goods design the products and supply the finished items through franchised retail stores. All manufacturing and distribution activities are frequently outsourced to third-party providers in different parts of the world.

Because of these developments, supply chain management has become vitally important. Managing the supply chain in an increasingly globalized and competitive world can be very challenging. Uncertainties in supply and demand, globalization of marketplaces, shorter product lifecycles and rapid changes in technology have led to a higher exposure to risks in the supply chain. For example, in early 2021 there was a global shortage of semiconductors used by car manufacturers. The majority of the supply of these components is from Taiwan and the Covid-19 health crisis caused a bottleneck in the supply, leading to the temporary closure of car plants in North America.

All kinds of uncertainties can cause problems in the supply chain, and this has increased the importance of risk management. It is impossible to eliminate risk entirely, but adequate attention to risk management matters can reduce the likelihood and magnitude of any disruption to supply. As the trend towards obtaining components and finished goods continues to lead to greater use of manufacturing facilities overseas, the corporate social responsibility issues also tend to increase.

Conflicting stakeholder requirements of value for money and profitability often mean goods are procured from a low-cost manufacturer, probably based in a country with lower employment costs. However, care needs to be exercised that the goods will be of appropriate quality, obtained at the lowest cost and supplied ethically.

There are many risks associated with this course of action. There may be quality and availability issues or questions of corporate social responsibility that need to be addressed. The essence of the supply chains for many organizations is that they have gone from 'lowest risk at any cost' to a situation of 'lowest cost at any risk'. In reality, both hazards and opportunities need to be managed. In other words, the potential

downside of outsourcing needs to be identified and mitigated with the same level of diligence as the upside or assumed benefit of outsourcing is embraced.

Scope of the supply chain

Because of the increased use of outsourcing, there is an increasing interest in the risks associated with reliance on third parties. Outsourcing of operations is normally undertaken because it is assumed that costs can be reduced and risks transferred. A careful evaluation of the balance between risk and reward should be undertaken before any supply chain outsourcing decisions are taken.

The organization should be aware of the fact that outsourcing means that the organization will not only have to focus on its own risks but should also look at the risks associated with other links in the supply chain. Supply chain management and risk management are interrelated. Supply chain considerations are becoming more common, as well as much more complex.

Outsourcing of the various components of the infrastructure of an organization is only part of supply chain management. Many organizations also outsource services as simple as cleaning or maintenance of offices, warehousing and delivery of goods to individual shops, and even complex 'back office' services in the financial services industry.

There is frequent reference to upstream and downstream supply chains. Generally speaking, upstream supplies are those items that are delivered to you and downstream supply chain refers to the goods that you deliver onwards. This can be explained as a timber grading company situated on the side of a river waiting for timber to be delivered from upstream. The company grades the timber and then delivers the graded timber downstream to customers. However, this terminology is not universally used and sometimes goods that are provided onwards to customers are considered as a delivery chain. Whatever terminology is used, it is the case that most organizations receive goods and services from component suppliers or outsourced services providers. Organizations will need to assess the risks associated with their various suppliers, as well as considering the risks arising from their position as suppliers of products and services that are delivered to their own customers and clients.

Strategic partnerships

When setting up arrangements to outsource part of its operations, an organization will need to consider very carefully the selection of each strategic partner. For example, the production of an in-house magazine will be outsourced by many organizations. Depending on the importance placed on this magazine, an organization may wish to set up a strategic partnership with the publisher.

Supply chain risk management becomes even more important when production activities are involved. When a supermarket sets up an arrangement for the supply of manufactured goods, there are many considerations. The ability of the supply chain partner to deliver the required goods on time and within the agreed cost on a sustainable basis will be a key consideration.

In order to secure exclusive supply, a supermarket may wish to enter into strategic partnerships with its suppliers. These strategic partnerships will result in the supermarket receiving priority treatment in the event of potential disruption to supply. The benefit to the supermarket of this arrangement is that continuity of supply is guaranteed and costs will be reduced. For the supplier, the benefits will be a secure market for its goods and a long-term contract. The disadvantage for the supplier is that the price may be fixed, even though the supplier could obtain a better price on the open market from time to time. There is a further disadvantage that the supplier may be dependent on orders from only one customer.

With increased focus on cost and use of 'just-in-time' delivery, single supplier arrangements may increase the risk of business interruption. Although organizations will wish to limit potential losses by purchasing insurance, it is unlikely that traditional insurance will adequately protect the reputation and market share of the organization in these circumstances. Therefore, organizations will need to look at business continuity strategies and developing strategic partnerships. These issues explain why greater emphasis is being placed on organizational 'resilience' and this topic is discussed further in Chapter 19.

Strategic partnerships are very useful alliances formed for the benefit of stakeholders. They can sometimes involve competitors working together such as the example of the energy companies combining to allow the availability of well-capping equipment at strategic parts of the globe to prevent the re-occurrence of a Deepwater Horizon-type event described in Chapter 13.

Joint ventures

Securing priority status from suppliers may be part of the arrangements for an organization to secure its supply chain. However, for very critical components or support operations, priority status may be insufficient. Many organizations, therefore, explore the possibility of setting up joint ventures with their suppliers in order to ensure priority supply status.

Setting up joint ventures also allows the organization to have some management control over the operation of a supplier and eliminate the possibility that the supplier will deliver goods to a competitor in difficult market conditions. Joint-venture arrangements may also be an appropriate way of responding to competitor activities by denying the competitor access to the products produced by the joint-venture

partner. Joint ventures may also be a successful way of responding to technology changes in the marketplace, because the organization will not need to find all of the funding required to embrace the new technology.

These sorts of competition and technology changes in the supply chain may be very significant. In fact, it may be beyond the resources of existing organizations operating in the marketplace to respond to these changes. Joint-venture operations can ensure continuity of supply chains and also, if correctly executed, deliver competitive advantage. All of this can be achieved while putting less capital at risk.

An organization may have a strategic objective of reducing its dependency on suppliers. Tactical options will be available, including taking over the supplier or setting up a new organization jointly with your supplier as a separate joint-venture organization. Setting up a joint-venture organization will put the organization into a situation where more of the risks are under their direct control. Setting up such a joint venture may be the appropriate tactical option, because it will require less capital and/or fewer resources to be allocated than would be the case if the supplier were purchased outright.

The advantage of joint ventures is that the risks are shared. These are usually shared by contractual agreements or by the establishment of a separate company with an agreed allocation of capital to fund that company. Because the capital is shared, the risks involved with the venture will be shared and, accordingly, the benefits and rewards will be shared. Joint ventures are a mechanism whereby an organization can exploit benefits but with a lower risk exposure. This will be a suitable way forward for organizations that do not have the appetite to fully fund the venture.

Outsourcing of operations

There are many benefits associated with outsourcing the manufacture of components to specialist sub-contractors. However, organizations that decide to outsource in this way need to be aware of the risks and introduce appropriate controls. Outsourcing (or transferring) the manufacture of components does not completely transfer the risks associated with the activity. As with any transfer of risk, a suitable contract needs to be developed and implemented and this contract should provide clarity on where risk is allocated within the contract. The contract is likely to include penalty clauses for failure to perform, but contracts that also include provisions for rewarding exceptional performance provide a greater sense of co-operation. Table 31.5 identifies examples of the risks associated with outsourcing for a car manufacturer.

Table 31.5 Risks associated with outsourcing**Risks for car manufacturer outsourcing supply of components:**

Late or delayed delivery from supplier as a result of loss of control and increased dependency on third-party supply.

Risk that the components may be outside technical specification or otherwise of poor/unacceptable quality.

Unethical or other inappropriate behaviour by the component supplier may damage the reputation of the car manufacturer.

Cost reduction may not be maintained after the car manufacturer has lost the ability to manufacture the components.

Outsourcing of non-core operations can also give rise to supply chain exposures. Table 31.6 sets out a list of considerations when setting up a contract for the supply of outsourced support. It is important that organizations consider the scope of the outsource arrangements and the range of services to be supplied. Various other features of the outsourced agreement will need to be addressed.

In many countries, there is legislation covering the protection of employees when an operation is outsourced. For example, if an organization decides to transfer the catering or the cleaning services to an outsourced company, the employment rights of staff previously employed by the organization may be protected. This can be a significant obstacle to the outsourcing of certain facilities management and other activities and thereby obtaining the cost reduction that would result.

Outsourcing of operations is usually considered to be a mechanism for having non-core activities undertaken by a contractor. For example, an office-based business may decide to outsource cleaning and catering, as well as other facilities management operations. The benefits will normally focus on reduced cost while at the same time receiving a greater level of expertise from the outsourced contract.

Table 31.6 Scope of outsourcing contracts**As a minimum, the agreement between the organization and the outsourced service provider must address the following issues:**

Scope and duration of the arrangement.

Services to be supplied and restrictions on sub-contracting.

Pricing, fee structure, service levels and performance requirements.

Audit and monitoring rights.

Confidentiality, privacy and security of information.

Default arrangements and termination provisions.

Dispute resolution arrangements.

Insurance requirements, liability and indemnity.

The next box considers some of the benefits of outsourcing. Outsourcing is often undertaken to save costs, but it may also be undertaken so that the work is fulfilled by a specialist company. For example, a mortgage lender may outsource property surveys to a company with greater resources and more expertise.

Benefits of outsourcing

Most businesses outsource certain functions, but this is a major decision and the benefits can be difficult to define. Outsourcing can cut costs by reducing overheads and having a professional perform the operation. Although this benefit is attainable, it should not be the only reason a company decides to outsource.

The benefits of outsourcing can be divided into two types. First, there are the direct benefits of having a specialist company undertaking the outsourced activities. Then, there are the indirect benefits of giving greater focus to the core activities that remain in-house. The direct benefits of outsourcing are reduced costs, decreased cycle times and improved customer perception and satisfaction, including:

- focus on core competency;
- reduction in the cost of manufacturing and logistics services;
- reduction in head count of hourly workers and management;
- improved accuracy;
- flexibility and wider range of services;
- access to global networks and superior technology;
- improved service and quality;
- reduced capital investment and increased cash flow.

Risk and contracts

Risk management is clearly an important component when setting up supply chain contracts or deciding to outsource certain activities. The need for a detailed contract between the organization and the suppliers of the outsourced service is clear from the factors considered in Table 31.6. The nature and complexity of the contract will depend on at least the following factors:

- level of the risk associated with the contracted service;
- value of the contract for supply of goods or services;
- duration and scope of the contract;

- level of skill required in the delivery of the contracted services;
- critical nature of the goods or services that are being contracted.

The desire to achieve greater value for money and reduce costs has resulted in complex supply chains that are far more fragmented than was previously the case. Many organizations will contract out key parts of their activities so that money can be saved and a greater level of specialist expertise is available from the outsourced company. Outsourcing also enables organizations to focus on their own core operations and competencies and scale their operations up or down as demand requires.

However, this has resulted in complex global supply chains that are more vulnerable to potential disruption through external sources such as terrorism, pandemics and natural disasters. Organizations need to undertake a thorough risk assessment of their supply chain and outsourcing arrangements to ensure that the risks associated with these contracted services are adequately managed. Remember that contracting out the supply of goods or services does not transfer all of the risks.

Outsourcing arrangements should be introduced only when they offer a cost-effective and efficient way of running the business. Outsourcing decisions based on a belief that risks are being completely transferred to a third party may prove to be incorrect. Damage to reputation may still be suffered if the outsourced manufacturing activity produces sub-standard goods or is exposed as operating unethical business practices.

It is possible that the cost of supply will be reduced, but the risks may actually be increased. When contracting out services and supply, the organization needs to be satisfied that the risks associated with this transfer are within the risk appetite and consistent with the risk attitude of the organization, as well as being within its risk capacity. Finally, evaluation should be undertaken to determine the actual risk exposures that are associated with increasingly complex supply chain arrangements.

Note

- 1 Basel Committee on Banking Supervision and Bank for International Settlements (2012) *Core Principles for Effective Banking Supervision*, www.bis.org/publ/bcbs230.pdf (archived at <https://perma.cc/TQ5M-C9N9>)

THIS PAGE IS INTENTIONALLY LEFT BLANK

PART EIGHT

Risk assurance and reporting

LEARNING OUTCOMES

Having studied this section readers will be able to:

- Describe the nature and purpose of internal control and the contribution that internal control makes to risk management.
- Summarize the importance of the control environment in an organization and provide a structure for evaluating the control environment (CoCo).
- Explain the importance of governance, risk and compliance (GRC) and the relationship to the three lines of defence model.
- Summarize the importance of risk assurance and identify the sources of risk assurance available to the board/audit committee (CRSA).
- Describe the activities of a typical internal audit function and the relationship between internal audit and risk management.
- Describe the activities involved in an ERM initiative and how these can be allocated to internal audit, risk management and line management.
- Discuss the importance of risk reporting and the range of risk reporting obligations placed on companies, including Sarbanes–Oxley.
- Produce examples of risk reporting approaches adopted by different types of organizations, including companies, charities and government agencies.

Further reading

- Canadian Institute of Chartered Accountants (1995) Criteria of Control, www.cica.ca
- Hillson, D (2016) *The Risk Management Handbook: A practical guide to managing the multiple dimensions of risk*, Kogan Page, London
- HM Government (2020) *National Risk Register: 2020 edition*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/952959/6.6920_CO_CCS_s_National_Risk_Register_2020_11-1-21-FINAL.pdf
- Institute of Internal Auditors (2004) The role of internal auditing in enterprise-wide risk management, www.iiajapan.com/pdf/data/erm/ERM.pdf
- McNally, J S (2013) *The 2013 COSO Framework and SOX Compliance*, www.coso.org/documents/COSO%20McNallyTransition%20Article-Final%20COSO%20Version%20Proof_5-31-13.pdf
- Woods, M (2011) *Risk Management in Organizations: An integrated case study approach*, Routledge, Abingdon

CASE STUDIES

The student can review the following examples to illustrate further the areas discussed in Part Eight and throughout this book.

Unilever: Opportunity assessment

Unilever states that its success as an organization depends on its ability to identify and exploit the opportunities generated by its business and the markets it operates in. They have 'embedded' risk management across all activities to achieve this. They say that they put 'risk and opportunity assessment at the core of the Board agenda... Unilever's appetite for risk is driven by the following:

- Our growth should be consistent, competitive, profitable and responsible.
- Our actions on issues such as plastic and climate change must reflect their urgency, and not be constrained by the uncertainty of potential impacts.
- Our behaviours must be in line with our Code of Business Principles and Code Policies.
- Our ambition to continuously improve our operational efficiency and effectiveness.'

Their approach to risk management is 'designed to provide reasonable, but not absolute, assurance that our assets are safeguarded', indicating their willingness to accept and exploit some risks.

Their annual report includes a separate section on climate change, which includes details on their 'strategy and risk management' approach, including providing detailed

plans around their 'climate strategy to reduce emissions within our operations, through our value chain, as well as describe how we are managing risks and meeting consumer needs connected with climate change'.

Edited extracts from: Unilever PLC (2020) Purpose-Led, Future-Fit: Unilever Annual Report and Accounts 2020, www.unilever.com/Images/annual-report-and-accounts-2020_tcm244-559824_en.pdf

Colgate Palmolive: Damage to reputation

Colgate Palmolive is a US-based and listed company offering personal care and pet products globally. They recognize that their reputation for producing safe and secure goods is critically important. Their form 10-k states that 'Maintaining our strong reputation with consumers and our trade partners globally is critical to selling our branded products.' As such they implement a series of actions to defend their reputation such as 'our Ethics and Compliance, Diversity, Equity and Inclusion, Sustainability and Social Impact, Brand Protection and Product Safety, Regulatory and Quality initiatives'.

They recognize that negative sentiment could arise through 'health concerns, threatened or pending litigation or regulatory proceedings, environmental impacts (including deforestation, packaging, plastic, energy and water use and waste management), our environmental, social and governance practices, or other sustainability or policy issues'.

They further itemize 'the widespread use of digital and social media by consumers' which 'has greatly increased the accessibility of information and the speed of its dissemination'.

Edited extracts from: Colgate Palmolive Company (2020) We Are Colgate: 2020 annual report, <https://investor.colgatepalmolive.com/static-files/1d8483af-a8b5-485f-9cff-992592a92b3b>

Sainsbury's Bank: Evidence of control

J Sainsbury is a major UK grocery, retail and financial services business operating physical and online distribution platforms. The Sainsbury's Bank operation is a regulated entity offering personal banking and credit card facilities.

They state in the annual report:

[We] adopt a process-centric approach to identifying, measuring and controlling our key risks, ensuring that attention is focused on what matters most. We undertake Process Risk and Control Assessments (PRCA) across all of our key activities to ensure that appropriate and effective controls are in place, and treatment plans are identified where strengthening is required.

They specifically refer to an enterprise-wide view of risk and state that this 'allows for greater ownership of top risks by subject matter experts'. They also refer to inherent and

residual risks along with aligning the control environment to ‘its target exposure if different from current residual levels’.

Interestingly, reference is made to their Risk Management Information System, which they term a ‘Business Enterprise Risk Tool (BERT)’, which ‘is used to record and manage our key processes, the controls we have in place, any treatment plans to improve our control environment and to record our management of risk events’.

Edited extracts from: Sainsbury's Bank plc (2020) Annual Report and Financial Statements for the Year Ended 29 February 2020, https://about.sainsburys.co.uk/~media/Files/S/Sainsburys/documents/reports-and-presentations/annual-reports/2020/Sainsburys_Bank_AR20.pdf

The control environment

32

Nature of internal control

The system of internal control within an organization is an important component in the successful management of its risks. Internal control is concerned with the methods, procedures and checks that are in place to ensure that a business or organization meets its objectives. There are alternative definitions of internal control and some of the key definitions are set out in Table 32.1. One possible definition of internal controls can be considered to be the actions taken by management to plan, organize and direct the performance of sufficient actions to provide reasonable assurance that objectives will be achieved.

Table 32.1 Definitions of internal control

Organization	Definition
Criteria of Control	Internal control is all the elements of an organization that, taken together, support people in the achievement of the organization's objectives. The elements include resources, systems, processes, culture, structure and tasks.
COSO	A process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: <ul style="list-style-type: none"> • effectiveness and efficiency of operations; • reliability of financial reporting; • compliance with applicable laws and regulations.
Institute of Internal Auditors	A set of processes, functions, activities, sub-systems and people who are grouped together or consciously segregated to ensure the effective achievement of objectives and goals.

The phrase ‘control environment’ is preferred by internal auditors. ISO 31000 refers to the ‘risk management context’. The COSO ERM cube refers to the ‘internal environment’. In all cases, the intention is to refer to the level of maturity of the organization with regard to internal control activities. When referring to internal control activities, it is important to have a single definition within the organization.

ISO Guide 73 defines control as a measure that is modifying risk. It also states that controls include process, policy, device, practice, or other actions that modify risk. Guide 73 also makes the important point that controls may not always exert the intended or assumed modifying effect. Internal control incorporates the organizational and hierarchical structure, as well as planning and objective setting. The scope of internal control extends to evaluation of controls designed to support the organization in achieving objectives and executing strategy, but it also applies to the control of actions to ensure that the organization does not miss business opportunities.

When designing effective internal controls, the organization should look at the arrangements in place to achieve the following:

- maintenance of reliable systems;
- timely preparation of reliable information;
- safeguarding of assets, both physical and cyber, including data;
- optimum use of resources;
- preventing and detecting fraud and error.

Resilience of the organization in the event of external shock

Effective financial controls, including maintenance of proper accounting records, are an important and well-established element of internal control. These financial controls help ensure that the company is not unnecessarily exposed to financial risks and that financial information used within the business and for public reporting is reliable.

Purpose of internal control

The primary purpose of internal control activities is to help the organization achieve its objectives. Typically, internal controls have the following purposes:

- safeguard and protect the assets of the organization;
- ensure the keeping of accurate records;
- promote operational effectiveness and efficiency;

- adhere to policies and procedures, including control procedures;
- enhance reliability of internal and external reporting;
- ensure compliance with laws and regulations;
- safeguard the interests of shareholders/stakeholders.

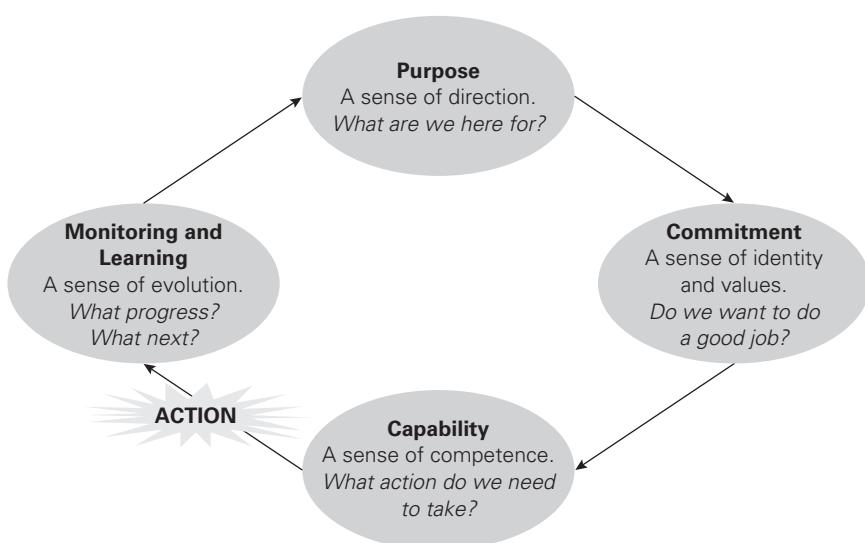
The internal control system includes internal control activities and the structure and responsibilities that relate to them. The purpose of this internal control system is to enable directors to drive the organization forward with confidence, in both good and bad times. A further purpose of the internal control system and internal control activities is to safeguard resources and ensure the adequacy of records and systems of accountability.

The purpose of the control environment is to ensure consistent responses to risks that materialize. A well-developed control environment will also ensure that pre-planned responses to a crisis situation are efficiently and effectively implemented. There are a number of approaches to the evaluation of the control environment, including LILAC, CoCo and risk maturity models such as FOIL and the 4Ns, as described in Chapter 25.

In many ways, the use of a maturity model will help evaluate the status of the control environment in terms of the implementation of the selected structure that will be used to drive improvements in the control environment and achieve a greater level of risk awareness in the organization. In summary, the LILAC or CoCo model will be selected as the means of driving and measuring improvements in the control environment. The level of success in implementing the selected framework will be reflected in the level of risk maturity, as measured by FOIL and the 4Ns, that has been achieved. An enhanced level of maturity will enable the organization to achieve more sophisticated outcomes from its risk management efforts, as illustrated in Figure 3.2. Risk maturity models can be used as a means of benchmarking the risk management status of an organization and targets can be set to increase risk maturity.

Control environment

The criteria of control framework, otherwise known as CoCo, produced by the Canadian Institute of Chartered Accountants, is a structured means of measuring the quality of the control environment within an organization. The control environment, which the COSO ERM cube labels as the ‘internal environment’, is a measure of the risk culture within the organization. The view taken by the CoCo framework is that if the control environment is satisfactory, risk management and internal control activities will be successfully and appropriately undertaken.

Figure 32.1 The CoCo framework

SOURCE Reproduced with permission from Guidance on Control, Canadian Institute of Chartered Accountants (1995, Toronto).

The structure of the CoCo framework is set out in Figure 32.1. The framework has four components, which are represented as a continuous cycle. The components are based on a sense of direction of the organization, a sense of identity and values, a sense of competence and a sense of evolution.

A number of organizations use the CoCo framework as a means of benchmarking compliance with the internal control component of the COSO ERM cube. This approach will, therefore, be based on a framework that is a combination of CoCo and the remaining seven components of the COSO ERM cube. Table 32.2 gives more information on the specific requirements of each of the four components of the CoCo framework.

The rationale behind CoCo is explained in the framework as follows:

A person performs a task guided by an understanding of its purpose and supported by capability. The person needs a sense of commitment to perform the task well. The person monitors his or her performance and the external environment to learn how to do the task better and any required changes. In any organization of people, the essence of control is the four components set out above.

There are similarities between the CoCo approach and the LILAC measure of risk awareness or risk culture that has been mentioned previously. The LILAC approach suggests that risk management activities will be embedded when the risk culture

Table 32.2 Components of the CoCo framework

Purpose	Objectives should be established and communicated. Significant internal and external risks should be identified and assessed. Policies should be established, communicated and practised. Plans should be established and communicated. Plans should include measurable performance targets and indicators.
Commitment	Shared ethical values should be established, communicated and practised. HR policies should be consistent with ethical values. Authority, responsibility and accountability should be clearly defined. Mutual trust should be fostered to support the flow of information.
Capability	People should have the necessary knowledge, skills and tools. Communication processes should support the values of the organization. Sufficient and relevant information should be identified and communicated. Decisions and actions within the organization should be co-ordinated. Control activities should be designed as an integral part of the organization.
Monitoring and learning	Environment should be monitored to re-evaluate controls. Performance should be monitored against the targets. Assumptions behind objectives should be periodically challenged. Information needs and related information systems should be re-assessed. Procedures should be established to ensure appropriate actions occur. Management should periodically assess the effectiveness of control.

displays leadership, involvement, learning, accountability and communication. Individual organizations should decide how they wish to measure the control environment/risk-aware culture within the organization. Whatever method is used to measure the risk culture, there is no doubt that it is critical to the successful implementation of risk management.

CoCo is an internal control framework, but it is described in this chapter because it is an established framework. There is a strong interface between risk management activities and internal control, and the CoCo framework therefore provides a useful means of evaluating the risk culture of an organization. CoCo defines three major objectives of controls:

- effectiveness and efficiency of operations;
- reliability of internal and external reporting;
- compliance with applicable laws and regulations and internal policies.

Features of the control environment

There are significant differences between COSO internal control and CoCo, as well as several key similarities. CoCo has a broader approach to the control environment than is set out in COSO. To give two examples of the broader approach in CoCo, it recognizes that controls are required in the setting of objectives, strategic planning and corrective actions; it also recognizes that the control environment of an organization is important when making decisions.

When undertaking an evaluation of the control environment using the structure of CoCo, a company may discover that good scores were obtained for the purpose, commitment and capability of the organization. However, the score for the monitoring and learning component may not be good enough. This information will enable the company to identify that it needs to pay more attention to the areas of challenging objectives and the assumptions that lie behind them. Better auditing of controls and a structured senior management review of risk management and internal control activities can then be introduced.

The main differences in approach between COSO internal control and CoCo are that CoCo is more explicit about the following issues:

- identification of a need to exploit opportunities;
- mitigation of weaknesses in business resilience;
- the importance of individual trust to the quality of the control environment;
- the need to periodically challenge assumptions.

There are two versions of the COSO cube, and it is the COSO ERM cube (2004) that is considered in detail in this book. COSO internal control was originally published in 1992, but was updated in 2013 and the first component of the COSO internal control cube is called the control environment. The features of the control environment that are considered to be important by COSO internal control can be summarized as:

- the organization is committed to integrity and ethical values;
- the board has oversight of development and performance of internal control;
- the management sets structures, reporting lines, authorities and responsibilities;
- the organization seeks to attract, develop, and retain competent individuals; and
- the organization holds individuals accountable for internal control responsibilities.

Expectations of internal control

A sound system of internal control reduces, but cannot eliminate, the possibility of poor judgement in decision making, human error, control processes being deliberately

circumvented by employees and others, management overriding controls, and the occurrence of unforeseeable circumstances.

A sound system of internal control therefore provides reasonable, but not absolute, assurance that a company will not be hindered in achieving its business objectives, or in the orderly and legitimate conduct of its business, by circumstances that may reasonably be foreseen. A system of internal control cannot, however, provide protection with certainty against a company failing to meet its business objectives or all material errors, losses, fraud, or breaches of laws or regulations. For these reasons, internal control systems are audited, as we discuss in Chapter 32.

CoCo framework of internal control

The first component of the CoCo framework is concerned with the establishment and communication of objectives, the significant internal and external risks faced by the organization, and the policies designed to support achievement of the organization's objectives. Plans to assist with the achievement of objectives and the inclusion of measurable performance targets and indicators are also important aspects of the purpose component of CoCo.

When establishing and analysing the purpose of the organization, CoCo makes it clear that the risks and opportunities facing the organization should be analysed in detail. The importance of risk assessment and organizational resilience is emphasized, together with the importance of recognizing the sources and origins of risk.

Components of a good risk culture

A good risk culture consistently supports appropriate risk-awareness, behaviours and judgements about risk taking within a strong risk governance framework. A good risk culture bolsters effective risk management, promotes appropriate risk taking, and ensures that emerging risks or risk-taking activities beyond risk appetite are recognized, assessed, escalated and addressed.

A good risk culture should emphasize the importance of ensuring that: 1) an appropriate risk-reward balance consistent with risk appetite is achieved when taking on risks; 2) an effective system of controls commensurate with the scale and complexity of the organization is in place; 3) the quality of risk models, data accuracy, capability of available tools to accurately measure risks, and justifications for risk taking can be challenged; and 4) all limit breaches, deviations from established policies, and operational incidents are investigated with proportionate disciplinary actions when necessary.

SOURCE Based on Financial Stability Board (2014) FSB releases a framework for assessing risk culture and progress report on enhanced supervision, www.fsb.org/2014/04/pr_140407/

The commitment component of CoCo is concerned with shared ethical values, including integrity. It is also concerned with human resource policies and practices and communication throughout the organization. Authority, responsibility and accountability are also included, together with the requirement to achieve an atmosphere of mutual trust.

The capabilities component of CoCo is concerned with the fact that people should have the necessary knowledge and skills to support the organization's objectives, as well as its values. Sufficient relevant information should be identified and communicated, together with decisions and actions of different parts of the organization. Activity should be co-ordinated and designed as an integral part of the organization.

The monitoring and learning component of the CoCo framework is concerned with external and internal environments and the fact that they should be monitored to obtain information. Performance should be monitored against targets and indicators and assumptions behind the objectives of the organization should be periodically challenged.

The information needs and related information systems should be assessed when objectives change, and a procedure should be established and performed to ensure that appropriate change actions occur in these circumstances. Finally, management should periodically assess the effectiveness of control in the organization and communicate results to appropriate stakeholders. An example of an organization evaluating its control environment is set out in the next box.

Evaluating the control environment

Many organizations have created their own formulas for educating employees about why controls are important and what adopting such measures means to them. The common element among these organizations is a commitment by senior management that embraces the internal control model.

Canada Post Corporation uses eight major groupings to evaluate the control environment, as follows:

- leadership;
- planning;
- customer focus;
- people focus;
- process management;
- partnership;
- business performance;
- continuous improvement.

During self-assessment workshops, executives receive the final results of all audit work performed throughout the year. The group then discusses business objectives for the coming year and the risks that could interfere with achieving them. The participants rate themselves on a scale of 1 to 10 for each of the criteria. Internal audit then compares the information it received directly from a business process to the information the group acquired about that process during other workshops.

Using the workshop results, internal audit develops an audit opinion on the effectiveness of controls and an audit plan for the coming year. Additionally, internal auditing provides a summary of the results to the board of directors to consider in its strategic planning session. The report includes a commentary on the company's five highest risks and five weakest controls.

Good safety culture

Ensuring a risk-aware culture in the organization is vitally important. A risk-aware culture will be achieved when all members of staff and management understand and accept the importance of adequate risk management. In addition, management and staff need to understand the role they will play in the successful management of risks and have a desire to fulfil that role enthusiastically.

There are many ways in which a risk-aware culture can be demonstrated. Clearly, one of the ways of demonstrating such a culture is to achieve high scores in a CoCo analysis. The COSO ERM cube also has an internal environment component, although this component is not as comprehensive as the CoCo framework. Nevertheless, evaluation of the internal environment and the level of risk awareness within the organization can be undertaken using the COSO ERM cube.

Many organizations regard the combination of COSO ERM and CoCo as an ideal way of combining the detailed approach to measuring culture within CoCo with the more exhaustive approach of COSO ERM. ISO 31000 refers to the context of risk management. Context has three components in ISO 31000, described as the internal context, the external context and the risk management context. Together, analysis of these three contexts will provide information on the status of the risk-aware culture in the organization.

A subset of a good risk-aware culture is a strong safety culture. Following a major rail crash at Ladbroke Grove near London Paddington railway station in 1999, the Ladbroke Grove Inquiry heard various definitions of the word 'culture'. Counsel to the Inquiry submitted that:

A good safety culture is the product of individual and group values, of attitudes and patterns of behaviour that lead to a commitment to an organization's health and

safety management. Organizations with a positive safety culture are characterized by communication founded on mutual trust, by shared perception of the importance of safety and by confidence in the efficiency of preventative measures.¹

It is highly likely that Part II of the Inquiry into the Grenfell Tower fire will also discuss the culture around risk management when it reports its findings.

Research by the Health and Safety Executive into the components of a safety culture produced a detailed report and the key components of the safety culture were identified as leadership, involvement, learning, accountability and communication. This gives rise to the acronym LILAC, which is described in more detail in Chapter 25. This represents an alternative approach to the purpose, commitment, capability, monitoring and learning components of the CoCo framework.

The future for control processes

Traditionally, the control processes discussed above are on the whole backwards looking, seeking to monitor control and determining whether something has happened. It has often been described as ‘driving a car looking in the rear-view mirror’. The growth of technology, analytical process, real-time and continuous monitoring of systems is starting to enable a form of pre-emptive control. Integrating different data sets with monitoring can form analysis which is capable of spotting the leading indicators for potential failure.

In so doing, control measures become preventative rather than reactive.

Note

- 1 Rt Hon Lord Cullen (2001) *The Ladbroke Grove Rail Inquiry: Part 2 report*, Health and Safety Commission, www.orr.gov.uk/media/10940 (archived at <https://perma.cc/3WFY-J83M>)

Internal audit activities

33

Scope of internal audit

There needs to be a close working relationship between the risk management function and internal audit. The responsibilities allocated to each of these functions will vary according to the nature, type and size of the organization. This is an important working relationship, because successful management of risk depends on four important risk-based outputs, which can be summarized as MADE2:

- mandatory as required by laws, customers/clients and standards;
- assurance for the management team and other stakeholders;
- decision making based on the best information available;
- effective and efficient core processes throughout the organization.

It is clear that if these outputs are to be successfully delivered, all stakeholders need to work together, and that includes co-operation between risk management and internal audit. The range of activities that are related to risk assurance are explored in Chapter 34. The important contribution made by internal audit and the range of activities that the internal audit department undertake are considered in more detail in this chapter.

Internal control is concerned with the methods, procedures and checks that are in place to ensure that a business organization meets its objectives. Because internal control is concerned with the fulfilment of objectives, there is a clear link with risk management activities. Internal control activities within a large organization are likely to be evaluated by the internal audit department. In some cases, the internal audit function may be outsourced to an external accountancy firm.

Although there is a distinction between the approach and activities of internal audit and of risk management, there are areas of common interest. Internal audit is primarily concerned with risk assurance and in validating the controls and procedures in place to manage risk. It is generally considered inappropriate for internal auditors to fulfil an executive function by assisting management with the identification, design and implementation of those risk control measures, as will be seen below. Managing risk, however, is critical to the success of the organization and therefore considered an executive function.

Internal financial control in a charity

Internal financial controls are just one part of a charity's overall control framework. The wider framework should cover all the charity's systems and activities.

Executive management, staff and volunteers are responsible for ensuring that the controls put in place by the trustees are implemented. There should be a culture of control embedded in the operations of the organization; this culture is created by the trustees and senior management, who should lead by example in adhering to internal financial controls and good practice.

The trustees should, at least annually, ensure a review is conducted of the effectiveness of the internal financial controls. This should include an assessment of whether the controls are relevant to, and appropriate for, the charity and not too onerous or disproportionate.

A key feature of internal financial controls is to ensure that no single individual has sole responsibility for any single transaction from authorization to completion and review. It is important where the trustees administer the charity personally, more likely in smaller charities, that there is sufficient segregation of duties amongst them, so that no one trustee is overburdened or exercises sole responsibility.

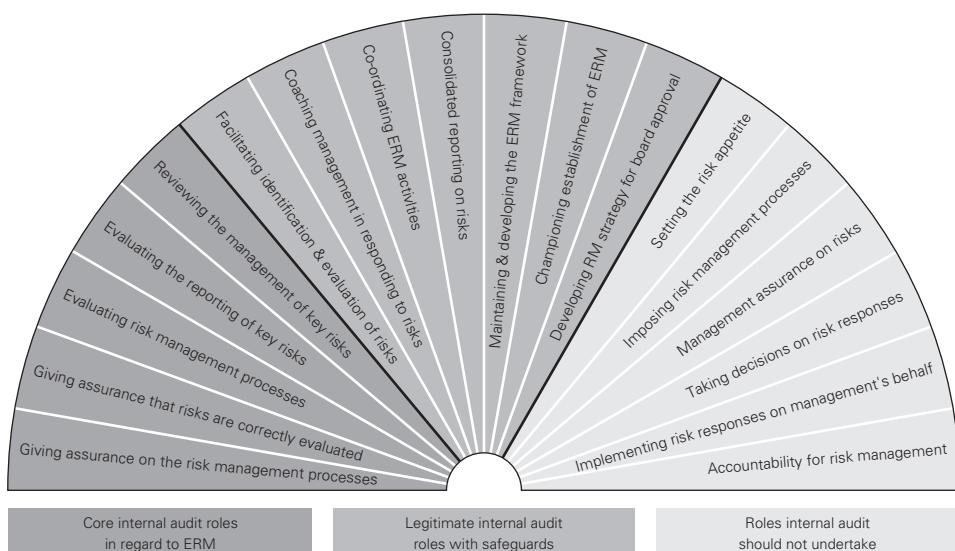
Role of internal audit

Figure 33.1 illustrates the range of activities that need to be undertaken in order to fulfil a successful ERM initiative. The diagram identifies those activities that are core to the work of the internal audit department. These activities include reviewing the management of key risks, evaluating the reporting of those risks and evaluating risk management processes.

The diagram identifies activities that internal audit should not undertake, generally taking decisions about and managing risk. The interface between the two sets of activities requires safeguards for internal audit to be involved but they have a legitimate reason to support them. The division of responsibilities set out in Figure 33.1 is not just compatible with the three lines of defence approach; it reinforces that approach and provides considerable detail on the allocation of responsibilities. Use of the information shown in Figure 33.1 will help an organization allocate responsibilities to management as the first line of defence, specialist risk management functions as the second line of defence, and internal audit as the third line of defence.

Establishing audit priorities is an important function of the audit department. In relation to risk management activities, internal auditors will need to establish their priorities for the testing of controls. There is an important interface between risk management and internal control. Risk management professionals are very good at

Figure 33.1 Role of internal audit in ERM



SOURCE Position Statement: *The role of internal audit in enterprise-wide risk management*, reproduced with the permission of the Chartered Institute of Internal Auditors – UK and Ireland. For the full statement visit www.iiainc.org.uk

assessing risks and identifying the appropriate type of control that should be in place. The risk register will often record current controls and make recommendations for the implementation of additional controls.

The core work of the internal auditor starts at this point. Having identified the critically important controls, the auditor will need to check that they are implemented in practice and that they are correct and effective. The outcome of testing of controls is to ensure that the intended level of risk is actually achieved in practice. In other words, the control actually moves the level of risk from the inherent level to the intended current level in the way that was planned and often assumed.

If the control is not effective and efficient, it will need to be modified. This is another area where risk management and internal audit share expertise. Although these discussions on controls can be facilitated by risk management and internal audit, the ultimate decisions on the controls and their anticipated effectiveness have to be made by the members of line management who are responsible for the controls.

Undertaking an internal audit

Undertaking an internal audit exercise involves a number of steps, as set out in Table 33.1. It can be seen that the steps involve planning, fieldwork, reporting and follow-up. As part of the audit exercise, the auditor should collect information relevant to

Table 33.1 Undertaking an internal audit**Planning**

- 1 Initial contact: Inform the client (audit target) or involved association about the auditing and its objectives.
- 2 Initial meeting: Conference meeting, so that the client can describe the areas for review and state the available resources and processes.
- 3 Preliminary survey: The auditors will gather all the needed data so they can have a good overview of the area or process to be audited.
- 4 Review internal control structure: The auditor will determine the priority areas for the audit to review.
- 5 Audit programme preparation: The audit programmes will outline the required fieldwork related to the audit topic/area.

Fieldwork

- 1 Testing for the critical internal controls: This process tests whether randomly selected records are accurate. Today, this may take the form of computer-assisted audit techniques (CAAT), which will review complete sets of data in order to identify patterns that can be indicative of fraud, error or omission.
- 2 Regular updates: The auditor will carry out financial reporting, mostly in oral communication, and the client may help in resolving any issues raised.
- 3 Drafting the audit summary: When fieldwork is done, the auditor will summarize findings, conclusions and recommendations.

Audit report

- 1 Audit report: The report will be reviewed by the audit team before presenting it to the client for further review.
- 2 Creating the report: Comments and suggestions on the first draft are taken into account in producing the final report.
- 3 Distribution of the final audit reports to people involved, senior management, audit committee, as agreed.

Follow-up

- 1 Audit follow-up: Response from the client will be reviewed, so that the findings may be tested and resolved.
- 2 Reporting the audit follow-up: The effects of resolved and unresolved findings will be included in the follow-up.

the audit that is to be undertaken. Analysis of the information that has been collected will enable the auditor to determine and agree the priorities and objectives of the review. For example, an audit of the supply chain will require the auditor to collect information on the contracts that are in place with suppliers.

Generally, there will be a long-term risk-based audit plan in place, which will identify which areas of an organization pose the key risks and should therefore be audited within specific times. Usually, an annual plan will sit within a larger three- or five-year plan that ensures all critical processes are reviewed. The annual plan should be approved by the board or audit committee, and ‘audit sponsors’ shall be identified who represent the client for the audit.

In many ways, the fieldwork is the most important part of the audit exercise. The auditor may need to visit locations, including supplier locations if the audit is concerned with the supply chain. The purpose of the fieldwork is to understand the risks and the controls that are in place to manage those risks. Testing of the controls will then be undertaken to ensure the efficiency and effectiveness of the controls that are in place. Testing of these controls will be based on discussions with the managers and staff, as well as observation of the activities as they are carried out.

Based on the fieldwork that has been undertaken, the auditor will produce the audit report. The audit report will contain comments on the efficiency and effectiveness of the controls that are in place and recommendations for further improvement, if considered necessary. The internal auditor will need to form an independent opinion of the level of control that has been achieved so that assurance can be provided to the audit committee, to the extent that this is justified. Also, if the audit report sets out recommendations, these should be agreed with the management of the unit. This should increase the likelihood of them being implemented. If the controls are inadequate and local management does not accept these conclusions, escalation of the issue will be required.

Risk management and internal audit

The working relationship between risk management and internal audit is one that needs to be managed carefully. The roles each perform are complementary, and striking a good working relationship will provide an opportunity to ensure more effective implementation of the risk management protocols and procedures. If they share a common focus there can be co-ordinated planning related to the management of risk, and the opportunities for sharing best practice regarding risk management tools and techniques will be enhanced.

The head of internal audit will usually have a reporting line to the most senior non-executive member of the board, perhaps even the chair. The risk manager will typically report to an executive member of the board. This is likely to be the company

secretary or finance director. Both parties need to find areas to co-operate without compromising the overall aims of their individual contributions.

The working relationship between risk management and internal audit will vary between organizations. The roles and responsibilities that are defined will be a reflection of the structure that seems most suitable for an organization. For example, both risk management and internal audit should attend risk assessment workshops. Risk managers may facilitate the risk assessment workshop, the responsibility for managing risk will always rest with the operational department, and the internal auditor will eventually be monitoring the controls.

Internal audit professionals require that control measures are identified in very precise terms that can be audited. The focus of internal audit activities is on the impact that the control measures actually have in practice. During an audit, internal auditors will request and be provided with information and data. The approach of the internal auditor is to test that information, so that the facts of the situation may be established.

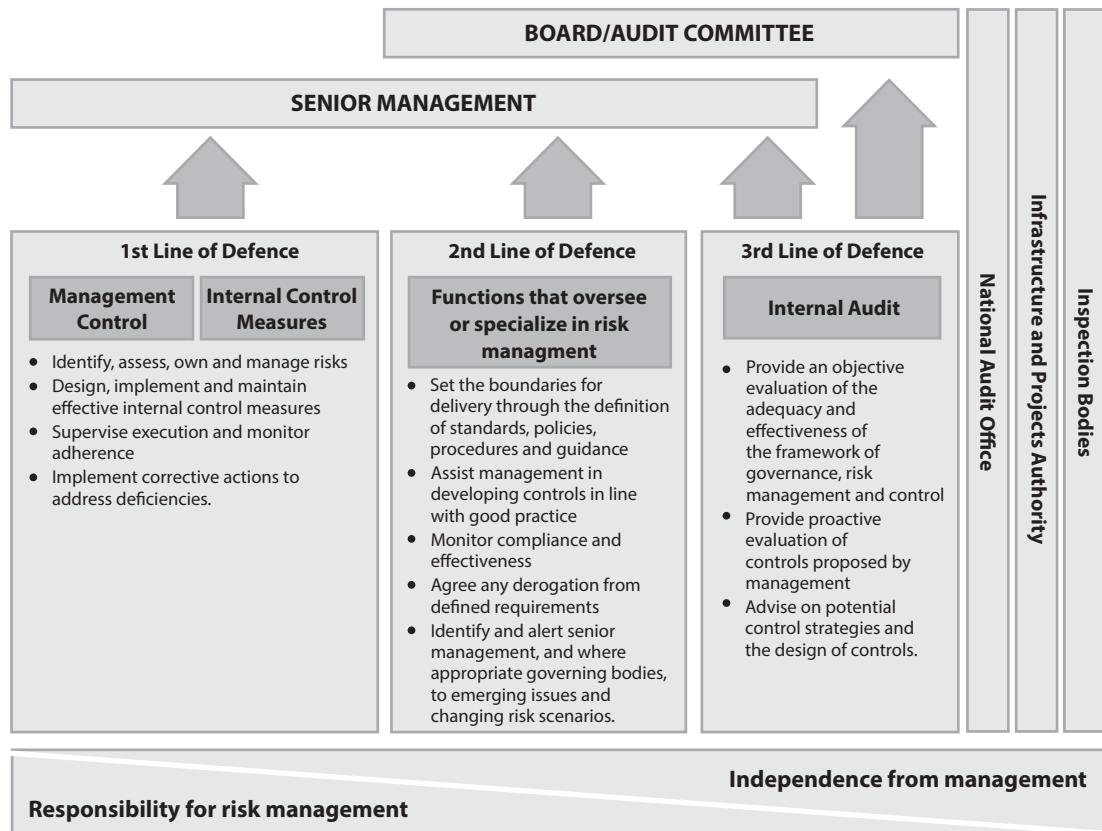
The three lines of defence approach is entirely consistent with the role of internal audit in enterprise risk management, as identified in Figure 33.1. In this respect: 1) management has primary responsibility for the management of risk; 2) specialist risk management functions can assist management in developing an approach to fulfilling their responsibilities; and 3) the internal audit function checks that the risk management process and the risk management framework are effective and efficient.

Any organization can be divided into three layers of senior management (directors), middle management (managers) and staff/employees. This division is compatible with the roles and responsibilities allocated to management in Table 24.1. Specialist risk management functions may operate at corporate or group level as an overall facilitator of the development, implementation, monitoring and improvement of the risk management framework. Risk management functions will also include business continuity, as well as health and safety. These specialist risk management functions fulfil the same role as the group risk management function, but in a more specific area of risk. Typical roles and responsibilities allocated to risk management functions are shown in Table 24.1.

The three lines of defence approach is also compatible with the concept of governance, risk and compliance (GRC), illustrated in Figure 33.2. The GRC approach is based on the overall view that the board is responsible for governance issues across the whole organization. In this role, the board will look to all three lines of defence to ensure adequate attention is paid to risk. The non-executive directors, in particular, will look to internal audit to provide assurance on the broad range of compliance issues within the organization.

The requirement for keeping accurate financial records applies to all organizations, and these will often be produced by an external accountancy firm, which will also act as external auditors. External auditors will be required to confirm, and in

Figure 33.2 Governance, risk and compliance



SOURCE HM Government (2020) *The Orange Book: Management of risk – principles and concepts*, p 30, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866117/6.6266_HMT_Orange_Book_Update_v6_WEB.PDF

some cases attest to, the accuracy of the financial records. In Figure 33.2 this is the National Audit Office for government authorities.

As with so many areas of risk management and internal control, the terminology used will vary from organization to organization. The next box describes the three lines of defence approach applied to tax and how it varies from the approach defined above. Nevertheless, the organization in this example is recognizing that responsibilities need to be divided and three lines of responsibilities is an appropriate and robust way of ensuring adequate governance and compliance and, in the case of the example, efficient and effective management of tax risks.

An area where risk management and internal control can work together is in establishing the risk management/internal control priorities for the coming year. When an organization sets up a risk-based audit programme, it will be seeking to ensure that internal audit activities are focused on the priority significant risks facing the organization. The board may well be looking for a joint risk management/internal audit contribution that will achieve better strategic decisions, more successful delivery of projects and more efficient core processes.

Three lines of defence applied to tax

Tax risk management is about having clearly defined and understood roles and responsibilities covering data management, transaction processing, information gathering, verification and escalation. Applied to tax, the three lines concept could broadly look like this:

First line:

- This means having a strategic understanding and the right people responsible for the basic business processes as they affect tax – the complete and accurate recording of transactions, for example the purchase-to-pay, record-to-report and fixed asset processes, and the gathering and processing of the related tax information.

Second line:

- This is the regular monitoring process. It requires frameworks and guidelines, developed by the tax and finance functions together, which are designed to facilitate effective monitoring of tax risks, pick up problems early and identify weaknesses in the process. People are only human and they do make mistakes.

Third line:

- This is independent assurance that the tax function is running properly, through both internal and external auditing. It requires both that internal auditors bring themselves up to speed on tax risk matters, and that tax functions welcome the additional assurance that a successful audit can bring. After all, it's better to have your internal auditor spot a mistake than to have to explain it to a tax authority.

Management responsibilities

The alternative way of allocating the responsibilities set out in Figure 33.1 is that internal audit is responsible for the activities that are identified as core internal audit roles. Risk management facilitates and supports the activities in the centre of the fan, and line management at the appropriate level has responsibility for the roles identified as activities that internal audit should not undertake. The allocation of roles and responsibilities should take account of the guidance produced by the Chartered Institute of Internal Auditors referenced under Figure 33.1.

A clear definition of the responsibilities of risk management, internal audit and line management is essential so that ownership of risk becomes clear. Risk management can assist with the risk assessment activities and the design of the controls. Internal audit can provide support by auditing the controls to ensure that they are effective and efficient and that they have been fully implemented. However, the primary responsibility for the management of risk remains with the executive management of the organization. It is important that the activities of risk management and internal audit do not in any way diminish or undermine the ownership of risk by the management of the organization. This approach is also consistent with the statement in most of the risk management standards that risks should not be managed outside the contexts that give rise to the risk.

Five lines of assurance

The three lines of defence model may not represent best practice in all circumstances. It is relevant to hazard (or operational) risks, including internal financial control, as well as being appropriate for governance of compliance risks, but has limited application to opportunity risks. The audit committee generally does not audit the upside of risk, or seek to identify circumstances where opportunities have been missed. Therefore, it is possible that there will be a disconnect between the scope of work of the risk management and internal audit departments compared with the full range and scope of enterprise risk management activities.

The weaknesses in the three lines of defence model relate to the role and status of the board of directors as well as certain internal functions. For example, the board provides assurance, but the board is not usually identified as a line of defence. In fact, the board both receives assurance as a stakeholder group and provides assurance to other stakeholders, including external stakeholders. Some head office functions will often undertake activities that are first- and/or second-line activities and, potentially, operate as third-line as well. The treasury function within the head office of a large company will manage the treasury requirements of the organization as first-line managers. It will also be an area of expertise that decides the strategy and tactics to be adopted by the organization. In some cases, audit of the treasury function is

specifically outside the scope of an internal audit department in a large company and it is the external auditors that review and audit the treasury function.

For these reasons it is sometimes considered there are five lines of defence where external audit is the fourth line and regulators are the fifth line. In order to enhance the effectiveness of the three (or five) lines of defence model, the alternative approach of the five lines of assurance has been put forward.

The five lines of assurance model suggests the following sources of assurance:

- 1 The board of directors with overall responsibility for ensuring that effective risk management processes are in place and the other lines are managing risk to within appetite.
- 2 Senior executives and senior managers with overall responsibility for building and maintaining a robust risk management process and delivering reliable information on the principal risks.
- 3 Business unit leaders with assigned ownership or responsibility for reporting on specific risks, and ensuring resources are protected and objectives are being achieved.
- 4 Specialist units providing expertise on specific types of risk, such as treasury, safety, environment, information security, legal and insurance, with responsibility for related risk management processes.
- 5 Internal audit activities, providing independent and timely information to the board on the reliability of the risk management processes in the organization and producing consolidated reports.

Inevitably, there are variations in the format described above and different organizations will develop a structure for the five lines of assurance that suits their specific needs. The main enhancement provided by the five lines of assurance model, is that the first line of defence is divided into the board, senior executives and business unit leaders, each of these identified groups being responsible for providing assurance in relation to their allocated responsibilities.

One of the benefits of the five lines of assurance model is that improved communication is required between the board of directors, members of the executive and the business unit leaders. Also, close liaison is required between the specialist expert risk units and the internal audit activities. The focus is on providing consolidated assurance across the organization, to enhance a risk-aware culture, rather than concentrating on the design and implementation of controls.

Therefore, the five lines of assurance model is more relevant to the management of strategic and tactical risks (including opportunities) than the three lines of defence model. This fact arises directly from the increased focus on assurance in the five lines of assurance model, rather than control in the three lines of defence model. It should be noted that, in both models, external auditors and regulators will continue to fulfil their specific responsibilities.

Risk assurance techniques

34

Audit committees

An increasing number of organizations have decided that it is appropriate to have an audit committee. Almost invariably, the audit committee consists of non-executive directors, with senior executive directors in attendance at audit committee meetings. It is chaired by a non-executive director, often referred to as the lead non-executive director, but usually not the non-executive chairman of the organization. The audit committee is generally not considered to be a sub-committee of the board, but has a status and a seniority that enables the audit committee to evaluate all activities in the organization, including the activities of the board itself.

Although the audit committee may be considered to be the guardian of compliance within the organization, the terms of reference are usually much broader than just compliance. The board of an organization will be responsible for governance throughout the organization, including co-ordinating the activities of specialist risk management functions. In this way, the board is responsible for the first and the second lines of defence. In other words, the board is responsible for the governance and risk components of governance, risk and compliance.

An area that is directly relevant to the achievement of strategic objectives and therefore of concern to the board is the environmental, social and governance (ESG) position of the organization. This area is also discussed in Chapter 21 on visions and values for the organization.

The audit committee is in a position to evaluate the governance standards within the organization, ensure that risk management receives appropriate attention, and seek assurance on the levels of compliance achieved within the organization. The role of the audit committee may be much broader than this, and includes evaluation of the arrangements for governance of the board itself. Many large organizations establish a separate committee for making senior appointments, including appointments to the board. This committee will normally be referred to as the nominations committee. Likewise, many large organizations will have a committee responsible for establishing remuneration and benefits structures that will apply throughout the whole organization.

The existence of a separate nominations or remuneration committee does not diminish the role and responsibilities of the audit committee. Nominations and remuneration, as well as some other committees, will be sub-committees of the board and are likely to have joint executive and non-executive membership. In reviewing the effectiveness of the board, the audit committee will also evaluate the effectiveness of the sub-committees. Given this role, the audit committee will retain its position as the ultimate monitor of governance, risk and compliance throughout the whole operation. The audit committee will seek assurance relating to all aspects of the strategy, tactics, operations and compliance of the organization.

The outcomes and impact of risk management activities are often reported to an audit committee in a large organization. Audit committees have a range of responsibilities, including the obligation to obtain adequate risk assurance in the organization. Table 34.1 provides a list of typical responsibilities of the audit committee. Audit committees should be non-executive bodies that do not have executive responsibility for risk management. Similarly, they should not have responsibility for the identification of significant risks or the identification and implementation of critical controls.

Table 34.1 Responsibilities of the audit committee

External audit	Recommend the appointment and re-appointment of external auditors. Review the performance and cost-effectiveness of the external auditors. Review the qualification, expertise and independence of external auditors. Review and discuss any reports from the external auditors.
Internal audit	Review internal audit and its relationship with external auditors. Review and assess the annual internal audit plan. Review promptly all reports from the internal auditors. Review management response to the findings of the internal auditors. Review activities, resources and effectiveness of internal audit.
Financial reporting	Review the annual and half-year financial results. Evaluate annual report against requirements of the governance code. Review disclosure by CEO and CFO during certification of annual report.
Regulatory reports	Review arrangements for producing the audited accounts. Monitor and review standards of risk management and internal control. Provide assurance that proposed regulatory and legislative changes are being adequately considered for all aspects of the organization, particularly in a global context. Develop a code of ethics for CEO and other senior management roles. Annually review the adequacy of the risk management processes. Receive reports on litigation, financial commitments and other liabilities. Receive reports of any issues raised by whistleblowing activities.

The function of the audit committee is to seek risk assurance and check that the procedure for the identification of significant risks is appropriate. The audit committee should validate that the significant risks have been correctly identified, as well as seeking assurance that critical controls have been correctly implemented.

The audit committee is concerned with internal control in the organization. Internal control is described in guidance to the UK Corporate Governance Code as the whole system of controls, financial and otherwise, established in order to provide reasonable assurance of effective and efficient internal control and compliance with laws and regulations.

It is worth considering the role of the audit committee in relation to the requirements of the UK Corporate Governance Code. The Code only applies to companies that are listed on the London Stock Exchange, although the principles set out in the Code appear to be gaining wider acceptance and application. One of the requirements is that companies without an internal audit function should review the need for such a department on a routine basis.

Even if these requirements do not apply to an organization, it is still appropriate for the audit committee to ensure that it can fully respond to these questions, by ensuring that necessary information is collected. An important component of governance requirements is the acknowledgement of the limitations of internal control.

Role of risk management

The risk management policy should set out the roles and responsibilities for risk management and internal control. The purpose of risk management is to fulfil mandatory obligations, provide assurance, support decision making and help ensure the effectiveness and efficiency of core processes (MADE2).

When allocating risk management responsibilities, consideration should be given in respect of each of the significant risks faced by the organization to the separate allocation of responsibilities for:

- determining strategy;
- designing controls;
- auditing compliance.

For example, a head office department may decide on the appropriate level of security for an organization. The design of the appropriate controls may be the responsibility of the production department. This is appropriate because security risk may be an integral part of production that needs to be under the ownership of the production department. In other organizations, it may be appropriate for the security arrangements to be designed by a specialist security adviser or the head of security

within the company. Auditing of compliance with the security arrangements is likely to be the responsibility of the internal audit department.

Even in a small organization, it may be important for responsibilities for the management of fraud risk to be separated between different employees or departments. In a small charity, for example, it may be appropriate for a non-executive board member to undertake the internal control audit and thereby provide an objective view of the efficiency and effectiveness of the internal financial controls in place in the organization.

The role of the risk manager in the allocation of these responsibilities should be a facilitation role. The risk manager may facilitate a workshop designed to identify the fraud risks within the organization and allocate responsibilities for controlling them.

However, the risk manager cannot be responsible for implementing controls or auditing compliance. Risk management and internal audit should restrict their roles to the evaluation of the effectiveness of the controls and assist with the identification of whether additional and/or different control measures should be introduced. Risk managers should be aware of the added value of internal audit, as outlined in the next box.

Added value of internal audit

Although what constitutes value-added activity will vary based on many factors, there are some general rules that apply across the board. Four factors that can help auditors determine what will add the most value to their organization are:

- knowledge of the organization, including its culture, key players, and competitive environment;
- courage to innovate in ways stakeholders don't expect and may not think they want;
- ability to adapt to the organization in ways that exceed stakeholder expectations;
- knowledge of those practices that the profession, in general, considers value-added.

Three of these factors (organizational knowledge, courage and ability to adapt) are competencies and personal qualities that, for the most part, are self-explanatory. However, knowledge of the practices that the profession considers value-added is a continuing professional challenge for internal auditors.

Risk assurance

Risk assurance is an important component of the overall risk management process. The audit committee will seek assurance that all of the significant risks are being adequately managed and that all of the critical controls are effective and that they have been efficiently implemented.

There are often discussions at audit committees about 'how seriously a particular department takes risk management and internal control'. The risk manager and the internal auditor will undoubtedly be able to offer an opinion. However, what the audit committee will require is an objective evaluation of the performance of that department. This objective evaluation of the risk culture within the department will form the main basis of assurance for the audit committee. There are other sources of assurance available to the audit committee and these are set out in Table 34.2. Subject to the nature of the organization, the audit committee may depend on some or all of these sources of assurance. Risk assurance is also available from the external auditors, although this may be limited to validation of the accounting processes and financial performance.

Assurance will also be required in relation to the risk management activities themselves. The review and monitoring stage of the risk management process is usually represented as an information and experience loop that provides feedback to the

Table 34.2 Sources of risk assurance

Culture measurement	By use of a recognized framework such as CoCo or COSO in order to gain a quantitative evaluation of the control environment.
Audit reports	Produced by internal audit and external auditors on a range of issues including risk assessment, implementation, compliance and training.
Unit reports	On such issues as risk performance indicators, control risk self-assessment, response to audit recommendations and reports on incidents that have occurred.
Performance of the unit	On risk-related issues, losses, significant weaknesses in control measures and details of any material losses suffered by the unit.
Unit documentation	On topics such as the risk management policy, health and safety policy, business continuity plans and disaster recovery plans.

beginning of the process. When considering the review and monitoring activities that need to be undertaken, the following stages should be borne in mind:

- review of the process as it operates in the organization;
- review of the standards of risk control in force;
- review of the level of success in reducing risk exposures;
- review of the level of success in achieving business objectives;
- review of why a high-risk strategy, project or operation was successful;
- delivery of risk assurance across this whole range of activities.

When a company plans to borrow more money from the bank, it may be asked to demonstrate how the board obtains assurance that the management of significant risks is satisfactory. The sources of assurance available might include:

- evaluation of the risk culture of the organization;
- quality of audit reports produced by internal audit;
- quality of reports produced by the various departments;
- overall business success of individual departments.

The company may decide that the reports from internal audit and the quality of reports from departments will be the basis of risk assurance. The company can also introduce a control risk self-assessment (CRSA) procedure that will be based on the components as set out in the risk guidance published by the Financial Reporting Council. Areas of weakness identified in the CRSA returns will be reported to the executive committee and remedial action will be required. All of these actions will provide the board with greater assurance and place the company in a better position to secure the additional funding from the bank.

When considering risk assurance, the organization will need to evaluate different issues, depending on whether the evaluation is related to strategy, tactics, operations or compliance. Assurance on adequate management of hazard risks can be achieved by evaluation of the hazard risk performance of the department.

Depending on the risk priorities of the organization, the board or audit committee may require annual reports on certain hazard risks. Because of the importance of health and safety at work, boards usually receive annual reports on safety performance. Likewise, the audit committee will wish to receive an annual report on the incidents of fraud that have been detected within the organization. This will be especially true of organizations that handle large amounts of cash.

Risks that are concerned with uncertainty, and in particular with the successful completion of projects, are often the subject of a review by the board or audit committee. Within large organizations, it is typical to have a post-implementation review of a project. For example, if the board of a retail company has authorized the opening of a new store, the audit committee will require a review of the completion of the

project for opening the store. This post-implementation review will evaluate whether the project was delivered on time, within budget and to specification. It is also common for the audit committee to require a further post-implementation review of the first 12 months, trading of the new store.

Risk assurance related to strategy/opportunities is more difficult and somewhat less well developed. Nevertheless, there is an increasing number of examples of organizations that undertake opportunity evaluations. This has become increasingly common in the professional consultancy firms. When a new business prospect arises, many professional consultancy firms have an opportunity review committee that decides on whether the organization wishes to offer its services to the client prospect. This type of opportunity evaluation may initially be achieved by attaching a risk assessment to a new business proposal.

Risk management outputs

When working together, risk management and internal audit should always concentrate on the outputs from the risk management process and the impact that is sought. The contribution of risk management is to ensure a greater chance of achieving the objectives of the organization, and this is also a stated intention of internal audit activities.

Overall, risk management/internal audit outputs are intended to achieve enhanced performance of the organization in the four important areas of effective and efficient strategy, tactics, operations and compliance (STOC). These outputs will be achieved by ensuring minimum disruption to routine operations from hazard risks, together with selection of effective processes that are appropriate for the organization. Selection of effective processes requires informed decision making and the successful design and delivery of projects. Risk management and internal audit should work together to achieve these outputs.

The most important decisions taken by an organization relate to strategy. Risk management and internal audit both have roles to play in helping the organization reach strategic decisions that result in the development of effective and efficient strategy. For example, risk management should ensure that risk assessment workshops address strategic decisions and internal audit should evaluate the quality of the strategic decision-making procedures.

The required outputs from risk management/internal audit can be summarized as fulfilling mandatory obligations, providing assurance, supporting decision making and ensuring the existence of effective and efficient core processes (MADE2). Risk management and internal audit should work together to achieve these outputs. Due regard should always be paid to the desire of internal audit to remain independent of executive management as they fulfil their activities. The need to retain this independence is another reason why internal audit should not become too closely involved in the executive role and responsibilities related to the management of risk.

Control risk self-assessment

As well as undertaking physical audits, internal audit departments will often facilitate a procedure of self-certification of controls. Self-certification of controls is an arrangement whereby local senior management complete a regular (often annual) return confirming details of the level of risk assurance that has been achieved in the department.

This type of self-certification is generally known as control risk self-assessment (CRSA) and it is frequently undertaken as an electronic return or recorded on the intranet of the organization. The questionnaire for the control risk self-assessment can be based on the criteria set out in COSO internal control, CoCo or any other relevant internal control framework, such as the risk guidance from the UK Financial Reporting Council.

As well as providing confirmation of adequate levels of internal control and risk assurance, the CRSA return can also provide details of situations where significant weaknesses in controls have been identified. This information will enable the internal auditors to identify areas where additional controls may be required. Also, in addition to identifying significant weaknesses, the CRSA return can require information on any material failures that have occurred.

A benchmark test for identifying a material failure should be supplied and will be much lower than the test for materiality applied by external auditors. For example, an organization that had set a test of materiality at £1 million might require reports on the CRSA return of any failure in controls that resulted in an incident/loss in excess of £100,000 at departmental level.

Approaches to CRSA

The executive has recommended the use of an annual CRSA exercise, to be conducted by internal audit, as part of the annual review of corporate governance. Each year a sample of the governance policies will be chosen by the governance panel for inclusion in the CRSA exercise. Policy custodians will be required to help formulate questionnaires and report back on the feedback received from services to internal audit.

The findings from the CRSA exercise, together with the assessment of compliance against each of the supporting principles and work carried out by internal audit in accordance with the annual audit plan will be drawn together into the annual governance statement, for review by the governance panel, the audit committee and the executive committee.

Benefits of risk assurance

Corporate governance is a major concern for all organizations and their stakeholders. Therefore, risk assurance should not be an administrative or box-ticking exercise. Organizations need to demonstrate that corporate governance is a priority for management. Many organizations recognize the need for openness of risk reporting. This requires effective communication activities to be in place at all times.

Having established good communication activities, the organization needs to ensure that there are positive messages to be communicated to stakeholders. Undertaking risk assurance activities will provide assurance to all stakeholders, including employees, suppliers, customers, government departments, external audit and internal audit, as described in the next box.

Obtaining risk assurance is an important part of the corporate governance arrangements for all organizations, as well as being of benefit to the STOC core processes, activities and decisions of the organization. The benefits of adequate risk assurance are that it:

- builds confidence with stakeholders;
- provides reassurance to sponsors and financiers;
- demonstrates good practice to regulators;
- prevents financial and other surprises;
- reduces the chances of damage to reputation;
- encourages the risk culture within the organization;
- allows more secure delegation of authority.

Reporting on risk management 35

Risk reporting

There is a wide range of risk management documentation that is relevant to risk management activities. Table 23.1 lists the types of risk management documentation that may be required as follows:

- risk management administration;
- risk response and improvement plans;
- event reports and recommendations;
- risk performance and certification reports.

The risk management manual should describe the control environment or risk culture. Typically, it will include a range of information, as set out in Table 23.2. The four categories of reports mentioned above can be characterized as established procedures, action plans, incident reports and performance reports. Chapter 23 discussed the established procedures in some detail, when describing the contents of the risk management manual. Action plans, especially those embedded within the risk register, together with the recommendations that come from incident reports, will help maintain risk management as a dynamic set of activities within the organization.

The subject of risk management documentation is mentioned again here because of the importance of risk performance and certification reports. In fact, the importance of these documents has increased considerably in recent times, because of the introduction of the Sarbanes–Oxley Act of 2002. Enhanced reporting requirements have been applied to all types of organizations in most parts of the world. It is important for an organization to ensure that the reports it submits achieve the highest standards that apply, whilst being compatible with other requirements.

For example, there may be specific requirements that apply, such as the Sarbanes–Oxley Act when an organization is listed on the New York Stock Exchange. However, that organization may also be listed on another stock exchange with different requirements. Additionally, the organization may have subsidiaries that are registered as a charity, or operate as (for example) an insurance company, perhaps a captive insurance company.

Risk performance and certification reports include operational management reports as well as more formal declarations and certified reports to stakeholders. In certain cases, certification of the financial results of operations of the organization will be undertaken as a formal attestation by a third party. Typically, this third-party attestation will be undertaken by an external auditor. Such a written attestation will also include an evaluation of the effectiveness of the control activities related to financial reporting.

The risk guidance from the Financial Reporting Council published in 2016 provides a comprehensive set of responsibilities for the board of an organization.¹ Table 35.1 provides a summary of the risk management obligations allocated to the board and it is item 6 on risk communication and reporting that is the most relevant to this chapter. It is important to note that the risk management reporting and communication obligations refer to both internal and external communications and the obligations also refer to the importance of risk management information being communicated both to and from the board.

Table 35.1 Risk management responsibilities of the board

The FRC risk guidance identifies the risk management responsibilities of the board and these can be summarized as follows:

1	Risk management processes	<ul style="list-style-type: none"> • Ensure that RM is incorporated within normal processes. • Identify the principal risks facing the company.
2	Principal risks and risk appetite	<ul style="list-style-type: none"> • Assessment of risks to the business model and strategy. • Risks the organization is willing to take or 'risk appetite'.
3	Risk culture and risk assurance	<ul style="list-style-type: none"> • Risk culture is embedded throughout the organization. • Adequate RM and assurance discussions take place at the board.
4	Risk profile and risk mitigation	<ul style="list-style-type: none"> • Risk profile of the company is kept under review. • Measures to manage or mitigate the principal risks are taken.
5	Monitoring and review activities	<ul style="list-style-type: none"> • Monitoring and review of risk management is undertaken. • Monitoring and review is ongoing and not just annual.
6	Risk communication and reporting	<ul style="list-style-type: none"> • Internal and external risk management communication takes place. • Necessary risk information is communicated to and from the board.

In summary, the FRC risk guidance requires that board attention should be paid to the risk management process, profile, principal risks and mitigation; the business model, strategy, risk appetite, risk culture and risk reporting; as well as the longer-term viability of the organization.

Reporting requirements have become increasingly detailed and it is sometimes necessary for organizations to produce separate reports for different regulatory authorities. Also, some organizations may decide to issue specific reports to achieve a high profile for certain aspects of their organization. In particular, several organizations issue separate corporate social responsibility reports to highlight their achievements in this important area. The case studies presented at the beginning of each part of this book are all extracts from reports of companies listed on the London Stock Exchange. These case studies indicate the wide range of topics that are reported by listed companies in relation to the broad range of risk management and internal control issues that are covered in this book.

Sarbanes–Oxley Act of 2002

The Sarbanes–Oxley Act (SOX) was passed in response to a range of corporate scandals in the United States. These scandals involved misrepresentation of the financial status of various organizations, leading to misleading financial statements. The primary purpose of SOX is to ensure that information disclosed by companies listed on the stock exchanges in the United States is accurate.

SOX requires that controls are in place to ensure the accuracy of all information reported by the organization. Section 302 of SOX requires that all data produced by the organization must be validated. In relation to financial statements, detailed analysis of risks that could result in misrepresentation of the financial results of the organization has to be undertaken. The procedures for compiling financial information and attestation of the financial disclosures by external auditors (as required by section 404) are very detailed and are considered by many to be extremely onerous and costly to undertake.

When complying with section 404 of SOX, the risk assessment is designed to identify weaknesses in the financial reporting structure. This is a very detailed procedure that requires considerable work by the internal audit department. The financial results of the organization and the evaluation of the financial reporting structure have to be reviewed by external auditors, who have to provide an attestation that they consider the results to be accurate.

SOX requirements state that an approved risk management framework should be used to evaluate risks to accurate financial reporting. The framework recommended for ensuring the accuracy of financial disclosures is the COSO internal

control cube (2013). Note that the COSO ERM cube (2004) includes all of the requirements of the earlier internal control version of the COSO cube. The SOX requirements apply to subsidiaries of US companies operating in other countries. They will also apply to organizations based in other countries if the company has a listing on a US stock exchange. Therefore, the internal control version of COSO is used by companies in many countries in the world.

In order to comply with the requirements of Sarbanes–Oxley, many organizations have decided to set up a disclosures committee to validate all information disclosed by the organization. Because of the extensive application of SOX, many companies based in countries other than the United States have also been obliged to set up disclosures committees. The risk architecture shown in Figure 24.1 for a large corporation includes a disclosures committee.

Compliance with the requirements of the Sarbanes–Oxley Act of 2002 is a costly and time-consuming exercise. Questions have been asked about whether the Act has been effective in improving the accuracy of reports from companies that are listed on US stock exchanges. These criticisms are relevant, given that the SOX requirements relate primarily to accuracy of reporting, rather than the achievement of enhanced risk management standards. A summary of some of the views of the CEOs of some US companies is presented in the box below.

Is Sarbanes–Oxley effective?

Chief executives across the United States view the Sarbanes–Oxley law as reactionary and over-burdensome. Yet they still cite ‘improper accounting practices’ as the number one ethical issue facing business today. A survey of CEOs on business ethics by Georgia State University polled nearly 300 chief executives at both private and public companies. Among its findings, most executives agreed that the Sarbanes–Oxley Act strengthened public and investor trust in corporate America, although it had done nothing to improve ethical standards at their businesses. Many suggested that the Act was an over-reaction to the ethical failures of a handful of executives and has proven burdensome and unnecessary.

However, examples remain of inaccurate, misleading and potentially fraudulent activity of senior management, which Sarbanes–Oxley was designed to rout. Amongst these examples are when General Electric, one of the founding companies of the Dow Jones Index, agreed to pay US\$200 million to the SEC for misleading investors about the source of profit in its power and insurance businesses in 2020.

Risk reports by US companies

Companies that are listed on a US stock exchange are required to make extensive disclosures about risk factors. These risk management reports are intended to be forward-looking, rather than a commentary on the risks that have materialized in the past. The reports are contained in the periodic Form 10-K or Form 20-F filings. It is not unusual to find several pages dedicated to risk factors. Typically, this section of the filing will be between three and ten pages long.

Table 35.2 provides a partial list of the industry, economic and environmental risks reported in Form 20-F for a US-listed company.

It is normal for the list to be introduced by a comment, such as ‘important factors that may cause future financial difficulties include, but are not limited to’, and then followed by a long list with detailed explanations. Items listed typically include:

- regulatory developments and changes;
- competition in our businesses;
- decisions of competition authorities regarding proposed joint ventures;
- compliance with governmental regulations;
- general economic conditions;
- loss of a strategic customer;
- higher costs of insurance for terrorism, sabotage or hijacking;
- our ability to achieve cost savings;
- fluctuations in fuel costs;
- changes in currency and interest rates;
- disruptions at key sites and facilities;
- incidents resulting from the transport of hazardous materials;
- strikes, work stoppages and work slowdowns;
- disruptions due to employee illness as a result of an influenza pandemic;
- market acceptance of our new service and growth initiatives;
- changes in customer demand patterns;
- the impact of technology developments on our operations;
- disruptions to technology infrastructure, including cyber attack such as malware, ransomware, distributed denial of service;
- adverse weather conditions;
- if our sub-contractors’ employees were considered our employees;
- changes in tax laws or their interpretation by authorities;
- higher costs related to implementation of the Sarbanes–Oxley Act;
- changes in environmental laws.

Table 35.2 Risk report in a Form 20-F**In relation to industry, economic and environment risks, the following have been identified for further detailed comment:**

- Risk of expiration of patents or marketing exclusivity.
- Risk of patent litigation and early loss of patents, marketing exclusivity or trademark.
- Risk of expiration or earlier loss of patents covering competing products.
- Failure to obtain patent protection.
- Impact of fluctuations in exchange rates.
- Debt-funding arrangements.
- Risks of owning and operating a biologics and vaccines business.
- Competition, price controls and price reductions.
- Taxation.
- Risk of substantial product liability claims.
- Performance of new products.
- Environmental/occupational health and safety liabilities.
- Developing the business in emerging markets.

Table 35.2 is an example of a list of risk factors, but it does not include all of the items contained in the full list filed as part of Form 20-F. Each of the listed risks would usually be described in more detail, by way of a detailed explanation of up to half a page. Additionally, the Securities and Exchange Commission (SEC) is considering whether to require more detailed reports on the risk committee reporting structure in companies listed on US stock exchanges. The SEC is the federal regulator of US stock exchanges and has the mission to protect investors, maintain fair, orderly and efficient markets, and facilitate capital formation.

Charities' risk reporting

Risk reporting by charities is compulsory in most countries in the world. In general, there is an expectation that charities should have detailed risk management procedures broadly equivalent to those required of government departments or of companies listed on a stock exchange. A shortened version of the advice on risk reporting set out in the UK Charity Commission guidance is as follows:

The form and content of risk reporting should reflect the size and complexity of an individual charity. The Charity Commission is not seeking to standardize risk reporting. A narrative style report that addresses the key aspects will be an acceptable approach to reporting, provided that the report provides:

- an acknowledgement of trustees' responsibility;
- an overview of the risk identification process;

- an indication that major risks have been reviewed or assessed;
- confirmation that control systems have been established.²

It is recognized that some charities, particularly larger charities or those with more complex operations, will wish as a matter of best practice to expand on this basic approach in their reporting. Where this more detailed approach to reporting is adopted it will be desirable to address the following broad principles, describing how they have been incorporated into the risk management procedures of the charity:

- linkage between the identification of major risk and the operational and strategic objectives of the charity;
- procedures that extend beyond financial risk to encompass operational, compliance and other categories of identifiable risk;
- linkage of risk assessment and evaluation to the likelihood of its occurrence and impact should the event occur;
- ensuring risk assessment activities and monitoring are ongoing and embedded in management and operational procedures;
- trustees' review and consideration of the principal results of risk identification, evaluation and monitoring.

Most charities are already likely to consider risk in their day-to-day activities. In fact, it has been reported that many charities now see risk management and other governance requirements as the most significant challenges facing the organization. This appears to imply that charities are becoming more risk-averse and spend more effort on compliance issues than on fundraising.

Even where a formal risk management process has not been completed, it will often be possible for aspects of the approach to risk to be drawn out for comment. A typical report on risk management for a small charity may be as follows:

- Risk assessment processes are in place to identify priority significant risks facing the charity.
- Risk management policies, protocols and procedures are embedded into routine operations.
- Analysis of strategy is undertaken to identify significant risks that could impact the delivery of the strategy.
- Procedures are in place to ensure legal compliance, including routine reports on legal matters, to the board of trustees.
- Trustees receive training on those risk management and corporate governance issues relevant to the charity.

Table 35.3 Government risk-reporting principles

Openness and transparency	Government will be open and transparent about its understanding of the nature of risks to the public and about the process it is following in handling them.
Involvement	Government will seek wide involvement of those concerned in the decision process.
Proportionality	Government will act proportionately and consistently in dealing with risks to the public.
Evidence	Government will seek to base decisions on all relevant evidence.
Responsibility	Government will seek to allocate responsibility for managing risks to those best placed to control them.

Public sector risk reporting

Attention to risk management in government departments and other areas of the public sector is mandatory in most countries. Much of the information on risk management in government bodies is freely available on websites and this information forms very useful reference material. However, because the information is publicly available, there is often no specific mention of the risk reporting to external stakeholders. The government in the UK has produced a set of principles on risk reporting. Table 35.3 sets out those risk reporting principles as openness and transparency, involvement, proportionality, evidence and responsibility.

There is usually extensive information on how the risk-reporting structure will work within a government body.

Government report on national security

One of the biggest steps forward in risk communication in recent times has been the willingness of governments to be more open about security threats. Many governments undertake a national security threat analysis and publish the results. For example, the UK government published in 2011 a document entitled the *National Security Strategy of the United Kingdom*. This publication gives details of the threats to national security faced by the UK. More recently, the UK Cabinet Office published the *National Risk Register*.³ The main threat categories identified in the document are as follows:

- environmental hazards events, including weather, coastal and river flooding and human or animal disease;
- human and animal health, with specific reference to Covid-19;

- major accidents, including industrial and transport;
- societal risks, including public disorder and organized crime;
- malicious attacks on crowded places, infrastructure, transport and electronic infrastructure (including nuclear or non-conventional attack).

The document provides detailed analysis of the various threats and the measures that are in place to minimize these threats. The report also discusses the drivers that are changing the risk profile of nations. These drivers include:

- political;
- climate;
- competition for energy;
- poverty/inequality/poor governance;
- globalization – economic, technological and demographic.

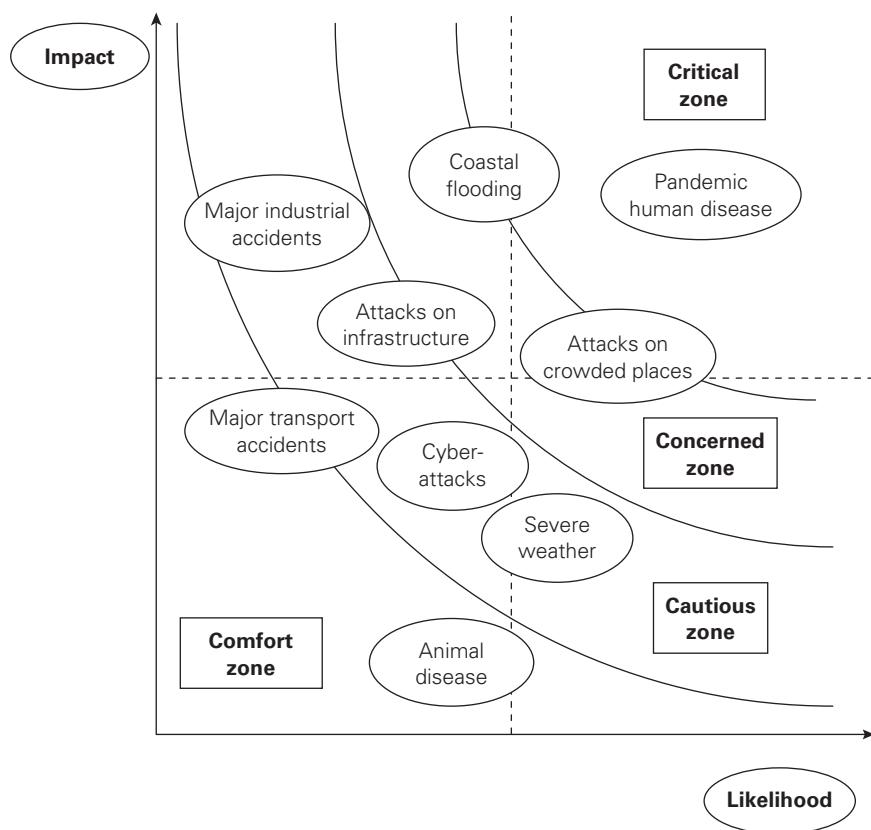
In March 2021, the UK Government published its report on *Global Britain in a Competitive Age: The integrated review of security, defence, development and foreign policy*. Within this analysis, there was review of key objectives or dependencies of the UK.⁴

These reviews by the UK government are interesting examples of the detailed risk assessment being undertaken at national level. It demonstrates that risk management is now embedded into the heart of national government. The fact that risk management has been embraced by national governments indicates that the importance of risk management is recognized at the highest level. Figure 35.1 shows some of the significant risks to UK national security identified by the government in 2011.

The UK government has not classified risks in this way, but if the risk attitude structure described in Figure 10.1 is used, then it is possible to identify the major threats where a government is comfortable that it can respond, such as transport accident, cyber attack and animal disease. If the government were to use this structure, it would appear that the government is cautious about major industrial accidents, attacks on infrastructure and severe weather. The government is concerned about coastal flooding and attacks on crowded places.

Finally, the risk attitude analysis suggests that the government identified the critical issue facing national security as pandemic human disease. In 2016 the government conducted Exercise Cygnus, to test its preparedness for the outbreak of a pandemic (using a flu virus). Reports suggest many of the 57 recommendations were not acted upon, including a need to increase critical care capacity and a review of how the social care and health service interface. Despite being recognized as a critical risk, the political will did not seem to exist to take any action on this. This is further evidence perhaps that the culture of an organization is critically important in applying risk management lessons. Doubtless many of the ‘lessons to be learned’ as a result of the Covid-19 pandemic will come to light in the public inquiry to be conducted from 2022.

Figure 35.1 Selected UK security threats



Notes

- 1 Financial Reporting Council (2016) *The UK Corporate Governance Code*, www.frc.org.uk/getattachment/ca7e94c4-b9a9-49e2-a824-ad76a322873c/UK-Corporate-Governance-Code-April-2016.pdf (archived at <https://perma.cc/TQ5M-C9N9>)
- 2 The Charity Commission (2010) Charities and risk management, www.gov.uk/government/publications/charities-and-risk-management-cc26 (archived at <https://perma.cc/TQ5M-C9N9>)
- 3 HM Government (2020) *National Risk Register: 2020 edition*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/952959/6.6920_CO_CCS_s_National_Risk_Register_2020_11-1-21-FINAL.pdf (archived at <https://perma.cc/TQ5M-C9N9>)
- 4 HM Government (2021) *Global Britain in a Competitive Age: The integrated review of security, defence, development and foreign policy*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age_-the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf (archived at <https://perma.cc/TQ5M-C9N9>)

APPENDIX A

Abbreviations and acronyms

The table below lists the 50 most important abbreviations and/or acronyms that are used in the book. This appendix should also be cross-referenced with the definitions set out in Appendix B. However, not all of the abbreviations and acronyms have corresponding entries in Appendix B, because some of the entries in this appendix relate to concepts and ideas, rather than a topic that can be summarized by way of a short definition.

The reference provided in the right-hand is column is to a specific figure or table, where one is provided. If there is no specific figure or table, a general reference to the chapter that discusses the abbreviation or acronym is provided.

Abbreviation	Term in full	Reference
4Cs	comfort, cautious, concerned and critical	Figure 10.1
4Es	explore, expand, exploit and exist	Figure 15.2
4Ns	naïve, novice, normalized and natural	Figure 25.1
4Ps	people, premises, processes and products	Table 2.2
4Ts	tolerate, treat, transfer and terminate	Chapter 12
5Cs	clear, concise, coherent, credible and complete	Chapter 28
5Es	explore, exit or expand, exploit and exist	Figure 15.3
6Cs	cost, coverage, capacity, capabilities, claims and compliance	Chapter 18
BCP	business continuity plan/planning	Chapter 19
BIA	business impact analysis	Chapter 19
BPR	business process re-engineering	Chapter 30
CEO	chief executive officer	Chapter 24
CoCo	criteria of control	Figure 32.1
CORR	customer, offering, resources and resilience	Chapter 21

(Continued)

Abbreviation	Term in full	Reference
COSO	Committee of Sponsoring Organizations of the Treadway Commission	Figure 4.3
CRAM	communication, relationship, analytical and management	Table 28.2
CRO	chief risk officer	Chapter 24
CRSA	control risk self-assessment	Chapter 34
CSFSRS	customers, staff, financiers, suppliers, regulators and society	Chapter 30
CSR	corporate social responsibility	Table 21.1
DRP	disaster recovery plan/planning	Chapter 19
EM3	embrace, manage, mitigate and minimize	Chapter 11
ERM	enterprise risk management	Chapter 6
FIRM	finance, infrastructure, reputation and marketplace	Table 11.2
FOIL	fragmented, organized, influential and leading	Table 25.5
FMEA	failure modes effects analysis	Chapter 10
GRC	governance, risk and compliance	Figure 33.2
HAZOP	hazard and operability	Chapter 10
IIA	Institute of Internal Auditors	Chapter 32
IRM	Institute of Risk Management	Table 1.1
LILAC	leadership, involvement, learning, accountability and communication	Table 25.4
LSE	London Stock Exchange	Chapter 29
MADE2	mandatory, assurance, decision-making, effective and efficient core processes	Table 3.4
OECD	Organisation for Economic Co-operation and Development	Table 29.1
ORM	operational risk management	Chapter 31
PACED	proportionate, aligned, comprehensive, embedded and dynamic	Table 3.3
PCDD	preventive, corrective, directive and detective	Table 16.1
PDCA	plan–do–check–act	Chapter 7
PESTLE	political, economic, social, technological, legal and environmental/ethical	Table 11.3

(continued)

(Continued)

Abbreviation	Term in full	Reference
PIML	plan, implement, measure and learn	Chapter 7
PRAM	project risk analysis and management	Table 31.4
RASP	risk architecture, strategy and protocols	Chapter 23
RMIS	risk management information system	Table 27.3
SEC	Securities and Exchange Commission	Chapter 35
SEE	social, ethical and environmental	Chapter 21
SOX	Sarbanes–Oxley Act of 2002	Chapter 35
STOC	strategy, tactics, operations and compliance	Chapter 1
SWOT	strengths, weaknesses, opportunities and threats	Chapter 1

APPENDIX B

Glossary of terms

The table below sets definitions and (as necessary) cross references for a total of 101 risk management terms used in this book. Appendix A provides a list of the abbreviations and acronyms that are used in the book.

The reference column provides information on the location within the book where further information is provided, including reference to a relevant figure or table when appropriate.

There is an international standard related to risk management vocabulary and definitions. This is *ISO Guide 73:2009 Risk Management – Vocabulary*. Where appropriate and to the extent that is possible, the definitions used in Guide 73 are referenced in this book.

However, it is not possible to use a unified terminology because risk managers in different disciplines and business sectors use their own words and definitions. Indeed, the various risk management standards produced around the world use different terminology and definitions. ISO Guide 73 attempts to provide a unified language of risk, but it may take some time for these definitions to be universally adopted.

Term	Definition	Reference
accept	See 'tolerate'	Chapter 15
avoid	See 'terminate'	Chapter 15
benchmark test	Established criteria to determine whether a risk is significant to the organization	Table 12.2
business continuity plan (BCP)	Plan to ensure continuity of business operations in the event of a serious incident that impacts the organization	Chapter 19
business impact analysis (BIA)	Analysis to assess the potential damage, loss or disruption that would be caused by the failure of critical business processes	Chapter 19
business model	Customer offering that utilizes resources, underpinned by resilience (CORR)	Chapter 20

(continued)

(Continued)

Term	Definition	Reference
captive insurance company	Subsidiary owned by an organization that provides insurance for the organization and sometimes for customers of the organization	Figure 18.1
chief risk officer (CRO)	Job title for senior risk manager appointed to board or executive of an organization	Chapter 24
communication, relationship, analytical and management (CRAM)	Set of people skills that are required by risk management professionals, in addition to their risk management and business technical skills	Chapter 28
compliance risk	Category of risk that is associated with the management of mandatory obligations	Chapter 2
consequences	Effect on the strategic, tactical, operational and compliance (STOC) core processes resulting from a risk materializing	Chapter 20
control	Actions to reduce the likelihood and/or magnitude of a risk. Hazard controls can be preventive, corrective, directive or detective (PCDD)	Chapter 16
control environment	Attitude, awareness and culture of the organization regarding risk management and/or internal control, referred to in COSO ERM as the 'internal environment'	Chapter 32
control risk	Category of risk that is associated with the management of uncertainty	Chapter 2
control risk self-assessment (CRSA)	Self-audit exercise completed by a manager or director to report on current status of controls and control activities	Chapter 34
core process	Set of co-ordinated business activities to deliver a stakeholder expectation that may be strategic, tactical, operational or compliance (STOC)	Figure 30.1
corporate governance	Set of activities and policies that control the way in which an organization is directed, administered and/or controlled	Figure 29.1
corporate social responsibility (CSR)	Actions to take account of the impact of activities on stakeholders (CSFSRS), as well as the environment	Table 21.1
corrective control	Type of control designed to limit the scope for loss and reduce any undesirable outcomes that have been realized	Table 16.1

(continued)

cost containment	See 'loss control'	Chapter 13
current risk	Existing level of risk taking into account the controls in place, sometimes referred to as 'net risk' or 'managed risk', but most frequently as 'residual risk'	Figure 16.3
customer offering that utilizes resources underpinned by resilience (CORR)	Description of the business model defined by operational and compliance core processes that can be modified by strategic and tactical core processes	Chapter 21
damage limitation	See 'loss control'	Chapter 13
detective control	Type of control designed to identify that a hazard risk has materialized, so that actions can be taken to avoid further or greater losses	Table 16.1
directive control	Type of control based on giving directions to people to behave in a certain way and/or follow established procedures	Table 16.1
disaster recovery plan (DRP)	Plan for use in the event of a serious loss, such as IT failure, fire or earthquake to assist the recovery of the organization and support crisis management	Chapter 19
eliminate	See 'terminate'	Chapter 15
embedded risk management	See 'leadership, involvement, learning, accountability and communication' (LILAC)	Table 25.4
enterprise risk management (ERM)	Integrated and co-ordinated approach to all the risks faced by the organization – see range of definitions in Table 6.2	Table 6.2
frequency	See 'likelihood'	Chapter 1
governance, risk and compliance (GRC)	Integrated approach to risk management and risk assurance based on the three lines of defence	Chapter 29
gross risk	See 'impact'	Figure 1.1
hazard risk	Category of risk that is associated with the management of pure risks or perils – the effects of hazard risks need to be mitigated	Chapter 2
impact	Effect on the finances, infrastructure, reputation and marketplace (FIRM) when a risk materializes	Chapter 12

(continued)

(Continued)

Term	Definition	Reference
inherent risk	Level of a risk before any control activities are applied, sometimes referred to as the 'gross level' or 'absolute level' of the risk	Figure 12.1
insurance	See 'transfer'	Chapter 18
internal audit	Internal or outsourced, yet independent group of people, or set of activities, monitoring the effectiveness and efficiency of control activities	Chapter 33
internal control	See Table 32.1 for a range of definitions	Table 32.1
leadership, involvement, learning, accountability and communication (LILAC)	Set of attributes that should be present in order to achieve successful embedding of (enterprise) risk management in the organization	Table 25.4
level of risk	Combination of the likelihood and impact of the risk, as established during the risk rating stage of risk assessment and can be determined at either gross (inherent) or net (residual) level	Chapter 10
likelihood	Evaluation or judgement regarding the chances of a risk materializing, sometimes established as a 'probability' or 'frequency'	Chapter 12
loss control	Range of activities to reduce the potential impact of hazard risks on the organization, including loss prevention, damage limitation and cost containment	Chapter 13
loss prevention	See 'loss control'	Chapter 13
magnitude	Size of the event when a risk materializes, sometimes referred to as 'severity' of the event and representing the gross (or inherent) level of the risk. We use 'impact' in this book	Figure 1.1
mandatory, assurance, decision making, effective and efficient core processes (MADE2)	Summary of the main reasons for undertaking a risk management initiative	Chapter 3
material failure	Failure of controls in an organization, resulting in loss of a magnitude that is considered important by auditors	Chapter 33

net risk	See 'impact'	Chapter 12
operational risk	Defined in Basel II as 'risk of loss or gain, resulting from inadequate or failed internal processes, people and systems or from external events' and capable of impacting the operations of the organization	Chapter 31
operational risk management (ORM)	Approach to risk management associated, in particular, with banks, insurance companies and other financial institutions, where the measurement of the level of 'operational risk' is required by Basel II, Solvency II or similar requirement	Chapter 31
operations	Activities of the organization designed to deliver products and services to customers or clients	Chapter 20
opportunity risk	Category of risk that is associated with the benefits of speculative opportunities	Chapter 2
preventive control	Type of control that is designed to eliminate the possibility of an undesirable risk materializing	Table 16.1
principles of risk management	Set of attributes defining the features of successful (enterprise) risk management, summarized as proportionate, aligned, comprehensive, embedded and dynamic (PACED)	Table 3.3
project risk	Risk that could cause doubt about the ability to deliver a project on time, within budget and to quality	Chapter 31
project risk assessment and management	Process developed by the Association for Project Management that enables the successful analysis and management of the risks associated with a project	Table 31.4
proportionate, aligned, comprehensive, embedded and dynamic (PACED)	See 'principles of risk management'	Table 3.3
reduce	See 'treat'	Table 15.1
residual risk	See 'current risk'	Figure 16.3
retain	See 'tolerate'	Table 15.1
risk	Defined in Guide 73 as 'effect of uncertainty on objectives' – see Table 1.1 for a range of definitions	Table 1.1
risk appetite	Defined in Guide 73 as 'amount and type of risk that an organization is willing to pursue or retain' but definitions of risk appetite can vary considerably	Table 26.1

(continued)

(Continued)

Term	Definition	Reference
risk architecture, strategy and protocols (RASP)	See 'risk management framework'	Chapter 23
risk assessment	Means by which significant risks are evaluated and prioritized by undertaking the three stages of 'risk recognition', 'risk rating' and 'risk ranking'	Chapter 10
risk assurance	Means by which an organization receives reasonable assurance that the significant risks are being adequately controlled	Table 34.2
risk attitude	Long-term view of the organization to risk defined by the 4Cs of comfort, cautious, concerned and critical	Chapter 10
risk capacity	Maximum level of risk to which the organization should be exposed, having regard to financial and other resources	Figure 26.1
risk criteria	Basis for ranking or evaluation of the significance of a risk – will define the risk appetite of an organization	Chapter 26
risk exposure	Level of risk to which the organization is actually exposed, either with regard to an individual risk or the cumulative exposure to the risks faced by the organization	Figure 26.1
risk management	Management activities to deliver the most favourable outcome and reduce the volatility or variability of that outcome – see Table 3.1 for range of definitions	Table 3.1
risk management framework	Set of activities that support the risk management process, referred to as the risk architecture, strategy and protocols (RASP) and defined in Guide 73 as arrangements for designing, implementing, monitoring, reviewing and continually improving risk management	Figure 23.1
risk management information system (RMIS)	Computer software system or part of the intranet of the organization that records and communicates risk information	Table 27.3
risk management manual	Documentation that includes all risk management policies, procedures, protocols and guidelines	Chapter 23
risk management policy	Statement of the overall intentions and direction of the organization related to risk management – often a one-page document	Chapter 23

risk management process	Activities that deliver management and control of risks	Figure 3.1
risk management standard	Guidance that provides a description of the risk management process, together with advice on establishing a suitable risk management framework	Chapter 4
risk map	See 'risk matrix'	Figure 1.1
risk matrix	Presentation of risk information on a grid or graph, also referred to as a risk map or heat map and often used to illustrate information from the risk register	Figure 1.1
risk maturity model	Structure for determining the level to which risk management is embedded within an organization (4Ns)	Table 25.4
risk profile	See 'risk register'	Chapter 5
risk ranking	Stage in the risk assessment process that evaluates the risk with reference to the risk appetite or the established risk criteria, to help select the appropriate risk response	Chapter 10
risk rating	Early stage in the risk management process, which involves the identification of all of the risks faced by the organization	Chapter 10
risk recognition	Stage in the risk assessment process that analyses the likelihood and impact of a risk – referred to in Guide 73 as the level of risk	Chapter 10
risk register	Record of the significant risks faced by an organization, the controls currently in place, additional controls that are required and responsibility for control activities	Chapter 5
risk response	Implementation of actions to respond to risks, including (for hazard risks) decisions whether to tolerate, treat, transfer or terminate (4Ts)	Table 15.1
risk tolerance	Deviation from the expected level of risk leading to implementation of risk escalation procedures – definitions of risk tolerance can vary considerably	Chapter 26
Sarbanes–Oxley Act of 2002	US legislation that encourages use of the COSO internal control cube (2013) to ensure that the information disclosed by companies listed by the SEC is accurate	Chapter 35
severity	See 'magnitude'	Chapter 12
significant risk	Risk with the ability to impact above the established benchmark for that type of risk	Table 12.2
significant weakness	Weakness in controls in an organization with the potential to cause a significant or material loss	Chapter 34

(continued)

(Continued)

Term	Definition	Reference
stakeholder	Persons or groups of persons with an interest in the activities of the organization, summarized by CSFSRS	Chapter 30
strategic risk	Long-term or opportunity risk concerned with where the organization wants to go, how it plans to get there and how it can ensure survival	Chapter 20
strategic, tactical, operational and compliance (STOC)	Types of core processes that define the mission of the organization and its business model	Chapter 20
strategy	Statement of where the organization wants to be in three or five years time, often defined by strategic objectives	Chapter 20
tactical risk	Medium-term control or uncertainty risk associated with change and projects designed to ensure that the organization delivers the planned strategy	Chapter 20
tactics	Developments, projects and programmes of work to implement strategy and move the organization from where it is now to where it wants to be in three or five years' time	Chapter 20
target risk	The ultimate level of risk that is desired by the organization when planned additional controls have been implemented	Figure 12.2
terminate	Risk response that is appropriate when the level of risk is not acceptable to the organization or outside risk appetite, also referred to as 'avoid' or 'eliminate'	Table 15.1
tolerate	Risk response that is appropriate when the level of risk is within risk appetite, also referred to as 'accept' or 'retain'	Table 15.1
transfer	Risk response for risks outside risk appetite that the organization wishes to transfer or share, by means of insurance, contract or (perhaps) joint venture	Table 15.1
treat	Risk response for risks that can be (further) treated by introduction of cost-effective (corrective) controls, also referred to as 'control' or 'reduce'	Table 15.1
upside of risk	Additional benefits available to the organization by taking risk – see Table 14.1 for a range of interpretations	Table 14.1

INDEX

Index for *Fundamentals of Risk Management*

Note: Figures have page numbers in **bold** and Tables have page numbers in *italic*.

- 4Cs (comfort, cautious, concerned and critical) of risk
 - attitude 123–24
- 4Es (explore, exit, exploit, exist) of opportunity risk response 142–43, 178, 179–81
- 4Ns (naïve, novice, normalized, natural) of risk maturity 295–98, 389
- 4Ps (people, premises, processes, products) of sources of disruption 130, 214
- 4Ts (tolerate, treat, transfer, terminate) of hazard risk response 54, 142–43, 146, 156, 171–78, 179, 185, 212–13
- 5Cs (clear, concise, coherent, credible, complete) of communication 326
- 5Es (explore, exit, exploit, exist, expand) of opportunity risk response 57–58, 143, 146, 180, 181
- 5Ts (tolerate, treat, transfer, terminate, take the risk) of risk management 156
- 6Cs (cost, coverage, capacity, capabilities, claims, compliance) of insurance buying 203–04
- Aboriginal heritage site, destruction by Rio Tinto 349
- absolute risk 20
- accountability in a risk-aware culture 292
- ALARP (as low as reasonably practicable) level of risk 140
- alternative risk transfer (ART) 200
- Amazon 37–38, 244
- appetite for risk *see* risk appetite
- Arcadia 24
- Arthur Anderson (former accounting firm) 336
- AS/NZS 4360:1995 43
- ASIS standard 103
- Astra Zeneca 355
- attachment of risks 24–26
- attitude to risk *see* risk attitude
- audit committees 292, 336, 340, 407–09
- audits for risk assessment 118, 119
- balanced scorecard tool 293–94
- banks *see* financial organizations
- Barclays 314–15
- Basel Committee on Banking Supervision 340, 357–59, 360–62
- Basel II and III Accords 48, 137, 358–59, 360–61, 361, 363, 365
- benchmarking 148
- Black Lives Matter movement 238–39
 - death of George Floyd 350
- Blackrock 239
- board of an organization
 - Capita case study 332–33
- board of an organization
 - corporate governance obligations 335–36
 - evaluation of board performance 344–47
- risk management responsibilities 417–18
- Boohoo 239
- Booz Allen Hamilton case study 221–22
- bow tie tool
 - loss control 151, 152
 - method of analysing risk 28–30
 - representation of risk management 129–31
 - representation of project risks 369, 370
- bp case study 80–81
- brainstorming, role in risk assessment 118, 119, 119–20
- British Land case study 112–13
- British Standards Institute 59
- BS 13500:2013 337–38
- BS 25999-1:2006 103
- BS 31100 3, 115, 127, 171, 177, 207, 259, 351–52
- business continuity management 47
 - ERM and 87–88
 - increasing importance of resilience 103–04
- business continuity planning (BCP) 47, 87–88
 - BCP lifecycle 210
 - business impact analysis (BIA) 214
 - civil emergencies 216–17
 - components of 208–10
 - corrective versus directive approach 208
 - crisis management plan 208–10
 - definition of 207
 - disaster recovery timeline and costs 209–10
 - implications of the VUCA environment 207–08
 - insurance cover for costs associated with a major incident 213–14
 - key activities 212
 - model for BCP 210–12
 - principles for successful BCP 210–12
 - resilience and 208, 215–216
 - successful business continuity 212–14
 - testing of procedures 211–12
- business continuity standards, ISO 22301:2012 210–12
- business delivery model 223–24, 225
- business development model, features of 223–26
- business impact analysis (BIA) 214, 215
- business models
 - components of 233–34
 - business models, CORR (customer, offering, resources, resilience) 233–34
 - dynamic business models 223–26
 - effective and efficient operations 229–30
 - ensuring compliance 230–31
 - Nokia plc case study 257
 - reporting performance 231–32
 - risk assessment 235–36
 - risks associated with 223–32
 - strategy and tactics 227–29
 - types of business processes 226–27

- business process re-engineering (BPR) 163, 353
 business processes, types of 226–27
 business risks 40
- calculated risks 45–46
 Canada Post Corporation, evaluating the control environment 394–95
 Canadian Institute of Chartered Accountants *see* criteria of control (CoCo) framework
 Capita case study 332–33
 captive insurance companies 43, 200, 204–06, 301
 car ownership, risks associated with 32
 CASE (capabilities, activities, standards, ethics)
 components of reputation 242–43
- case studies
 Booz Allen Hamilton 221–22
 bp 80–81
 British Land 112–13
 Capita 332–33
 Colgate Palmolive 385
 Dangote Cement plc 168–69
 Darktrace 113–14
 DP World 81–82
 East African Breweries Limited 221
 Financial Conduct Authority (FCA) 257–58
 HBOS 100
 Lenovo Group 11–12
 Lincolnshire County Council 81
 NHS Resolution 169
 Nokia plc 257
 Ocado 10–11
 Pioneer Food Group 333–34
 Sainsbury's Bank 385–86
 Singapore Airlines 256–57
 Softcat plc 113
 Thomas Miller Holdings Ltd 169–70
 UK Cabinet Office 12–13
 UK Department for Work and Pensions (DWP) 334
 Unilever 384–85
 Whitbread plc 220–21
- charities
 financial controls 189
 internal financial controls 398
 reporting on risk management 421–22
 risk architecture 282, 283
- Chartered Institute of Internal Auditors 405
 checklists for risk assessment 118, 118, 119
 chief executive officer (CEO) 116
 chief risk officer (CRO) 44, 48, 86, 90, 279–80
 UK DWP case study 334
 civil emergencies, business continuity planning 216–17
 classification of risks 127–37
 climate change
 as a key risk 251–52
 types of risk associated with 252
 climate-related activities, proposed reporting requirements for firms 350
 clinical risk management 47–48, 271
 COBIT standard 48
 CoCo *see* criteria of control (CoCo) framework
 codes of conduct 322
 Colgate Palmolive case study 385
 commercial risks 40
 Committee of Sponsoring Organizations of the Treadway Commission (COSO) 59
 communication
 risk information 292, 313–15
 skills for 322, 323–26
 shared risk vocabulary 315–17
 technology to support risk management 316–19
 Companies Act 2006 (UK) 232, 276–77
 competencies *see* risk practitioner competencies
 competency frameworks 320–21
 compliance
 importance of 55
 mandatory requirements 230–31
 compliance risks 17–19, 31–33, 136, 145
 management of 286, 287
 minimizing 35–36
 upside of 165
 context for ERM 99–104
 changing face of risk management 99
 increasing importance of resilience 103–04
 lessons from the financial and health crises 99–101
 managing emerging risks 101–03
 power of taking risks 101
 context of risk management 61–63, 69–78, 395
 external context 69, 70, 71–72
 internal context 69, 70, 72–73
 risk management context 69, 74–75, 395
 scope of the context 69–71
 contracts, risks associated with 380–81
 control, definitions of 388
 control acceptance 145, 286, 287, 303
 control environment 387–96
 CoCo framework approach 389–91,
 393–94, 395
 definitions of internal control 387–88
 designing effective internal controls 388
 evaluation approaches 389
 evaluation of 393–95
 expectations of internal control 392–93
 features of 392
 future for control processes 396
 nature of internal control 387–88
 organizational resilience and 388
 purpose of internal control 388–89
 relationship to the risk culture 389–91
 risk response and 389–91
 risk-aware culture 395–96
 safety culture 395–96
 Sainsbury's Bank case study 385–86
 see also context of ERM; context of risk management
 control measures, impact on risk 148–49
 control of risks 172, 175–76
 control risk self-assessment (CRSA) 412, 414
 control risks 17–19, 31–33, 136, 145
 cost of controls 303
 management of 39–40, 294
 projects 28
 uncertainty and 303
 controls
 influence on level of risk 139–40
 level of confidence in 141–42
 controls for hazard risks
 cost of controls 189–92
 types of controls 182–85
 core processes 163–64, 226–27,
 228, 229
 effective and efficient operations 54–55
 importance for stakeholders 351–53
 STOC 26

- corporate governance 331–32
 - approaches to 335
 - collapse of companies and 336
 - definition of 335
 - ethical business and 236–37
 - evaluation of board performance 344–47
 - financial organizations 340–41
 - future directions 338
 - government agencies 341–44
 - London Stock Exchange framework 338–40
 - OECD principles 336–38
 - reporting by committees 336
 - requirements in different countries 335
 - risk appetite and risk tolerance 146–47
 - role of non-executive directors 340
 - role of the board of an organization 335–36
 - what happens if it is weak 336
- Corporate Governance Code (UK) 60, 162, 335, 409
- corporate scandals, impact of the Sarbanes–Oxley Act of 2002 418–19
- corporate social responsibility (CSR) 236–37
 - European Commission definition 237
 - reporting on 240–42
 - risk management and 237–39
 - scope of issues covered by 237–39
 - stakeholder issues 238–39
 - supply chain and ethical trading 239–42
- CORR (customer, offering, resources, resilience) 230, 233–34
- corrective controls 182–85, 187
- COSO 2017, definition of ERM 85
- COSO classification of risk 127
- COSO ERM cube/COSO framework 3, 48, 59, 60, 64, 66, 66–67, 68, 88–89, 105–06, 293, 313, 390, 419
 - internal control/internal environment 387, 388
 - internal environment component 395
 - risk classification system 129, 130
 - risk tolerance 306
- COSO ERM rainbow double helix 64, 67
- COSO frameworks 61
- COSO internal control cube 59, 60, 61, 88, 293, 392, 418–19
- COSO standard of 2013 59
- cost containment 150, 151–52, 153–54
- cost-effective controls 191–92
- cost of controls 303
- cost of risk concept 42–43
 - total cost of risk calculations 301–02
- cost of risk controls 189–92
- Covid-19 pandemic
 - business responses to 220–21, 221–22
 - business responses to (Singapore Airlines case study) 256–57
 - criticism of UK government corporate governance 343
 - impacts of 6–7, 8, 24, 207, 375
 - lessons to be learned 99–101
 - stakeholders of pharmaceutical companies 355
 - supply chain impacts 375
- CRAM (communication, relationship, analytical and management) skills 322
- credit risks 137, 359
- criteria of control (CoCo) framework 61, 68, 292, 293, 298, 393–94, 395
- approach to internal control 392
- definition of internal control 387
- evaluation of the control environment 389–91
- risk culture evaluation 389–91
- Crosby, James 44
- crowdsourcing technology 116, 118, 119
 - role in risk assessment 118, 119
- culture of an organization, defining risk culture 289–92
- current level of risk 19–20, 139, 139–41
- damage limitation 149–52, 153
- damage limitation controls, disaster recovery plans 208
- Dangote Cement plc case study 168–69
- Darktrace case study 113–14
- Deepwater Horizon oil spill 2010 153
- delivering objectives, UK Cabinet Office case study 12–13
- Deming cycle 92
- dependencies-driven approach to risk 25–26
- dependency analysis 118, 119
- detective controls 182–85, 188–89
- directive controls 182–85, 187–88
- directors of organizations, responsibilities of 276–78
- disaster recovery, timeline and costs 209–10
- disaster recovery planning (DRP) 47
 - business impact analysis (BIA) 214
 - successful business continuity 212–14
- disaster recovery plans 151, 207–08, 311–12
- Disney 238
- diversity initiatives 238–39
- documentation
 - risk registers 75–78
 - types of risk management documentation 264–72
 - see also* reporting on risk management
- downtime risk, controlling 148–54
 - cost containment 150, 151–52, 153–54
 - damage limitation 149–52, 153
 - disaster recovery plans 151
 - hazard risks 149–51, 152
 - loss control 151–52
 - loss prevention 151–52
 - reducing the severity of the event 149–51, 152
 - risk likelihood 148–49
 - risk magnitude 149–50
- DP World case study 81–82
- DuPont 48
- East African Breweries Limited case study 221
- education programmes in risk management 43
- EM3 (embrace, manage, mitigate, minimize)
 - approach 129, 310
- emerging risks, managing 101–03
- energy risk management 48
- Enron scandal 252, 336
- enterprise approach to risk management, DP World case study 81–82
- enterprise risk management (ERM) 44, 48–50, 79–80, 83–89
 - aligning with core business processes 294–96
 - barriers to implementation 288–89
 - benefits of an ERM approach 87, 248–51
 - business continuity management and 87–88
 - context for 99–104
 - definitions of 48, 85–86
 - enterprise-wide approach 83–85
 - evidence for value added 246–47

- enterprise risk management (ERM) (*Continued*)
 implementation 90–98
 in practice 86
 integrating strategy and performance 88–89
 maximizing enterprise value 252–53
 Nokia plc case study 257
 ongoing monitoring and review 193–97
 relationship to BCP and resilience 215–16
 risk attitude 125
 role of internal audit 398–99
 setting objectives for 105–09
 steps to successful risk management 286–89
 strategic use of 252–53
 environmental, social and governance (ESG)
 position 407
 ethical business
 Booz Allen Hamilton case study 221–22
 corporate governance and 236–37
 impact of the Sarbanes–Oxley Act of 2002 418–19
 Whitbread plc case study 220–21
 ethical trading 239–42
 ethics codes 322
 European Commission, definition of CSR 237
 European Foundation for Quality Management, risk
 maturity model 298
 external context 69, 70, 71–72, 395
 external risks 359
 external stakeholders 71, 72
- Facebook 238
 Factory Acts 42
 Financial Conduct Authority (FCA) case study 257–58
 financial controls for charities 189
 financial crisis (2008/09) 99–101
 HBOS case study 44, 100
 impact of reward systems on risk culture 109
 Walker review of bank governance and
 regulation 341
 financial institutions
 corporate governance 340–41
 operational resilience 215
 operational risk management 357–65
 Walker review of bank governance and
 regulation 341
 financial reporting 272
 Financial Reporting Council (FRC) UK 60, 61, 346–47,
 417–18, 338,
 financial reporting procedures 231
 financial risk management 48
 financial risks *see* FIRM risk scorecard
 financial scandals 252
 Enron 336
 impact of the Sarbanes–Oxley Act of 2002 418–19
 financial sector, risk classification 137
 fire risk, use of sprinkler systems 150
 FIRM (finance, infrastructure, reputation, marketplace)
 risk scorecard 23, 71–72, 73, 126, 127, 129,
 130, 131–33, 144–45, 149, 150, 151, 159–62,
 173, 174, 308
 five lines of assurance model 405–06
 Flint, Michigan, water supply scandal 349
 flow charts, use in risk assessment 118, 119
 FMEA (failure modes effects analysis) 120
 FOIL (fragmented, organized, influential, leading)
 characteristics 295–96, 297
 evaluation of the control environment 389
 future for risk management 7–8
- gambling industry 241
 General Electric 419
 geopolitical risk 40
 global crises, risk identification 100–01
 governance of risk management, Darktrace case
 study 113–14
 governance, risk and compliance (GRC) 288
 government
 reporting on risk management
 423–24, 425
 risk assessments 123
 government agencies, corporate governance
 341–44
 Grantham Institute of Climate Change
 (Imperial College) 252
 GRC (governance, risk and compliance) approach 7
 Grenfell Tower fire 2017 35, 261, 396
 gross risk 20, 139
- hazard risk zones 185, 186
 hazard risks 17–19, 31–33, 136, 137, 145
 4Ts of hazard risk management 54, 142–43, 171–78,
 179
 cost of risk controls 189–92
 impact of 23–24
 mitigation 36–39
 reducing the magnitude of the event 149–51, 152
 types of controls 182–85
 hazard tolerance 145, 286, 287
 HAZOP (hazard and operability)
 studies 120
 HBOS case study 44, 100, 348
 health and safety at work 47, 48
 Health and Safety at Work Act 1974 (UK) 42
 heat map 21–22
 honesty boxes 157
 hotels, control of fires in 150
 HSBC, compliance issues 55
- IEC 31010:2019 68, 117–18
 implementing ERM 90–98
 ERM mix 92
 implementing stage 93, 95–96
 integrating processes, reviewing and improving 91–92
 investment in change 90–91
 learning stage 93, 97–98
 measuring stage 93, 96–97
 organizational culture and 91
 PIML approach 92–98
 planning stage 93, 94–95
 implementing risk management 56
 information security risk management 47, 48
 infrastructure resilience, reasonable worst-case
 scenarios 216
 infrastructure risks *see* FIRM risk scorecard
 inherent level of risk 19–20, 115, 139, 139–41
 inspections for risk assessment 118, 119
 Institute of Internal Auditors (IIA) 16, 17, 85, 387
 Institute of Operational Risk 109
 Institute of Risk Management (IRM) 1, 7, 45, 146, 252
 definition of risk 16
 Professional Standards 320
 risk management standard 3, 129, 130
 insurance
 6Cs of insurance buying 203–04
 captive insurance companies 43, 200, 204–06, 301

- cover for costs associated with a major incident 213–14
 evaluation of insurance needs 201–02
 financial risk management 48
 history of 198
 purchase of insurance 203–04
 risk financing 42–43
 risk transfer 38, 172, 176–77, 198–206
 total cost of risk calculations 301–02
 types of insurance cover 200–01
 underwriting risk 359
- insurance risk manager role 278–79
 integrated approach to risk management, bp case study 80–81
 internal audit 229, 294, 397–406
 five lines of assurance model 405–06
 outputs from risk management/internal audit 413
 relationship to risk management 397
 relationship with organizational management 405
 role in ERM 398–99
 scope of 397–98
 three lines of defence model 398–99, 402, 403, 404, 405
 undertaking an internal audit 399–401
 value added by 410
 working relationship with risk management 401–04
- internal context 69, 70, 72–73, 395
- internal control
 CoCo framework 389–91
 COSO and CoCo approaches
 compared 392
 definitions of 387–88
 expectations of 392–393
 organizational resilience and 388
 purpose of 388–89
- internal control frameworks 68
- internal financial controls, charities 398
- internal stakeholders 72–73
- International Certificate in Risk Management 1
- International Consortium for Organizational Resilience 215
- International Organization for Standardization (ISO) 59
- International Risk Governance Council 102
- investment appetite 145
- ISO 14001 103
- ISO 22301 103, 210
- ISO 22316:2017 103, 215
- ISO 27001 103
- ISO 28000 103, 375
- ISO 31000 3, 17, 52, 59, 60, 61–65, 68, 69, 71, 103, 122, 125, 171, 176, 177, 193, 293, 388, 395
- ISO 31022 68
- ISO 31050 68
- ISO 37000 338
- ISO 9000 47
- ISO 9001 103
- ISO framework 105
- ISO Guide 73 3, 4, 16, 23, 45, 68, 75, 122, 171, 174, 259, 276, 315, 348, 388
- ISO Guide 83 348
- ISO/IEC Guide 51:2014 3–4, 68
- IT risk management 47, 48
- joint ventures, supply chains 377–78
- JP Morgan Chase 239
- Kamani, Mahmud 239
 key dependencies for an organization 118
 significant risk and 173, 174
 key performance indicators (KPIs) 247
 key risk indicators (KRIs) 247–48
 key risks, climate change 251–52
 Kloman, Felix 42–43
- Ladbroke Grove Rail Inquiry 395–96
 leadership skills 328–29
 leadership versus management 328–29
 learning culture 291
 Lego 239
 Lenovo Group case study 11–12
 levels of risk 19–20, 23
 levels of risk management sophistication 50–52
 lifestyle decisions, personal risk appetite and 309–10
 LILAC (leadership, involvement, learning, accountability, communication) components of risk culture 74, 290–91, 293, 312, 389, 390, 391, 396
- Lincolnshire County Council case study 81
- listed companies, use of risk management standards 60–61
- local authorities, civil emergencies and business continuity 216–17
- London School of Economics 45
- London Stock Exchange corporate governance framework 338–40
- long-term risks 128–29
- loss control 151–52
 disaster recovery plans 208
 loss prevention 151–52
- MADE2 (risk management objectives) 4, 53–54, 156, 230, 294, 397, 409
- managed level of risk 20
- management responsibilities, relationship with risk management and internal audit 405–06
- management versus leadership 328–29
- mandatory risks 17
- market risks 137, 359–60
- marketplace risks 145–46 *see also* FIRM risk scorecard
- Massey Ferguson 42–43
- medical risk management 47–48
- medium-term risks 128–29
- mergers and acquisitions 302
 Pioneer Food Group case study 333–34
- modern-day slavery 239
- monitoring and review 193–97
 frequency of 195
 importance of monitoring 194–95
 NHS Resolution case study 169
 process 195–96
 reporting 196–97
 responsibility for 197
- Moore, Paul 44
- nanotechnology, emerging risk of 102–03
- national security, UK government reporting 423–24, 425
- net risk 20, 139
- New York Stock Exchange, risk management standards used by listed companies 60–61
- NHS Resolution case study 169
- Nokia plc case study 257
- Nolan principles of public life 343
- non-executive directors, corporate governance role 340

- objectives-driven approach to risk 24–25
- objectives for ERM 105–09
 - aligning with risk management principles 108–09
 - alignment with strategy 106–07
 - alignment with the organization's objectives 105
 - implementing objectives 107–08
 - levels of objective setting 107–08
 - risk management standards and 105–07
 - SMART objectives 108
- objectives of risk management 53–54
- Ocado case study 10–11
- OECD principles of corporate governance 336–38
- Offshore Pollution Liability Association (OPOL) 200
- Olympic Games, London 2012 366, 368–69, 373
- OPDCA (observation-plan-do-check-act) approach 92
- operational reporting 231–32
- operational risk management (ORM) 99, 119, 275–76, 357–65
 - Basel II principles 360–61, 365
 - definition of operational risks 358–62
 - developments in operational risk 365
 - failure of 360
 - measurement of operational risks 362–64
- operational risks 137
- operations
 - effective and efficient operations 229–30
 - stakeholder involvement in 355–56
 - upside of risk 164–65
- opportunity assessment 157–59
 - Unilever case study 384–85
- opportunity evaluation and response 181
- opportunity in projects 373
- opportunity investment 286, 287, 299–300, 302, 303
- opportunity management
 - 4Es of 178, 179–81
 - 5Es of 57–58, 180, 181
- opportunity risk response
 - 4Es of 142–43
 - 5Es of 143
- opportunity risks 17–19, 27, 31–33, 136, 145
 - importance for organizations 40–41
 - power of taking risks 101
- organizational environment 219–20
- organizations
 - categories of operational disruption 38–39
 - minimizing compliance risks 35–36
 - mitigation of hazard risks 36–39
 - risk of operational disruption 38–39
- outputs from risk management/internal
 - audit 413
- outsourcing of operations, risks and benefits 378–80
- PACED principles of risk management 5, 52, 63, 86, 92
- pandemics, risk identification 100–01 *see also* Covid-19
 - pandemic
- PCDD (preventive, corrective, directive, detective)
 - controls for hazard risks 182–85
- PDCA (plan-do-check-act) format 61, 92, 96, 210
- PDSA (plan-do-study-act) approach 92
- people risks 359
- PepsiCo Group 333
- performance improvement, measurement using key risk indicators (KRIs) 247–48
- PESTLE analysis/risk classification 71, 119, 120, 129, 133–34
- Pfizer 355
- pharmaceutical companies, range of stakeholders 355
- PIML (plan, implement, measure, learn) approach 61, 63, 210
 - implementing ERM 92–98
- Pioneer Food Group case study 333–34
- pooling risk 200
- PRAM (project risk analysis and management) model 374
- preventive controls 182–85, 186–87
- principles of risk management 52
- process risks 359
- product recall risk management 154
- project life cycle 370–72
- project risk management 47, 228–29, 294, 366–74
 - development of 367–68
 - opportunity in projects 373
 - PRAM model 374
 - project lifecycle 370–72
 - uncertainty in projects 366, 368–70, 371–72
- project risk register 370
- project risks 136
- projects
 - control risks 28
 - cost of necessary controls 303
 - upside of risk 163–64
- public life, Nolan principles of 343
- public perception of risk 122–23
- public sector organizations
 - corporate governance 341–44
 - reporting on risk management 423–24, 425
 - risk architecture 282
- pure risks 17
- quality management 47
- questionnaires for risk assessment 118, 118, 119
- racism in society 350
- Rainbow Double-Helix framework (2017) 59, 64, 67
- RASP (risk architecture, strategy and protocols) 62–63, 74, 259–61
 - responsibility for 276, 279
- RBS, ABN Amro takeover 300
- record keeping, importance of 270–71
- regulation of mergers and acquisitions, Pioneer Food Group case study 333–34
- relationship skills 326–37
- reporting
 - corporate social responsibility (CSR) 240–42
 - financial reporting 272
 - management reports 272
 - performance 231–32
- reporting on risk management 193, 196–97, 383–84, 416–25
 - charities 421–22
 - companies listed on a US stock exchange 420–21
 - government 423–24, 425
 - impact of the Sarbanes–Oxley Act of 2002 416, 418–19
 - public sector 423–24, 425
 - range of requirements 416–18
 - responsibilities of the board 417–18
- reputation
 - CASE components of 242–43
 - importance of 242–44
 - perceptions of Amazon 244
- reputation risks

- Colgate Palmolive case study 385
 damage limitation 149
 unethical business behaviour 239–40
see also FIRM risk scorecard
- residual risk 19–20, 139, 139
 resilience
 business continuity planning (BCP) 208
 importance of effective internal control 388
 increasing importance of 103–04
 reasonable worst-case scenarios 216
 relationship to business continuity and ERM 215–16
 scenario planning and 215–16
 surviving shocks and disruption 207–17
- responsibilities for risk management
 allocation of 273–74
 directors of organizations 276–78
 range of 274–76
 risk manager 278–80
 risk ownership 273–74
 statutory responsibilities of
 management 276–78
- review *see* monitoring and review
- reward, risk and 26–27
- reward systems, impact on risk culture 109
- Rio Tinto 349
- risk
 definitions of 15–17
 impact of hazard risks 23–24
 levels of 19–20, 23
 nature of 1–2
 reward and 26–27
 triggers and 28–30
 types of 17–19, 31–33
 uncertainty and 15
 why understanding risk is important 22–23
- risk analysis 111–12, 122, 138–47
 ALARP level of risk 140
 current level of risk 139, 139–41
 defining the risk appetite 146–47
 gross risk 139
 impact 138–39, 141
 influence of controls on level of risk 139–40
 inherent level of risk 139, 139–41
 level of confidence in controls 141–42
 levels of risk 138–41
 likelihood 141
 magnitude 138–39
 potential consequences of a risk 138
 risk capacity of an organization 145–46
 tests for risk significance 143–45
- Risk and Insurance Managers Society (US)
 48, 85
- risk appetite 28, 70, 74, 101, 146–47, 286, 299–310
 definitions of 299–300
 distinction from risk attitude 125
 lifestyle decisions and 309–10
 nature of 299–300
 power of taking risks 101
 risk capacity of an organization 145–46
 risk exposure and risk capacity 303–05
 risk matrix for 300–02
 Softcat plc case study 113
 uncertainty and 303
 risk appetite matrix 124, 300–02
 risk appetite statements 306–08, 309
 risk architecture 62, 69, 70, 259–61, 263, 267, 280–82,
 283
- risk assessment 111–12, 115–26
 approaches 116, 117
 attitude to risk 123–26
 bottom-up approach 116, 117
 British Land case study 112–13
 BS 31100 115
 business impact analysis (BIA) 214
 business model 235–36
 government risk assessments 123
 identification of priority significant risks 120–22
 identifying significant risks 115
 importance of 115
 inherent risk 115
 nature of the risk matrix 120–22
 perception of risk 122–23, 125
 risk likelihood and risk impact 120–22
 risk rating 120–22
 role in strategy formulation 115
 STOC (strategy, tactics, operations and compliance)
 approach 116
 top-down approach 116, 117
- risk assessment techniques 117–20
 brainstorming 118, 119, 119–20
 checklists/questionnaires 118, 118, 119
 crowdsourcing technology 118, 119
 dependency analysis 118, 119
 flow charts 118, 119
 inspections and audits 118, 119
 key dependencies for an organization 118
 quantification of risk exposure 119
 risk workshops 118, 119, 119, 291, 158–59, 324–26
- risk assurance 383–84, 407–15
 audit committees 407–09
 benefits of 415
 control risk self-assessment (CRSA) 412, 414
 risk management outputs 413
 role in the risk management process 411–13
 role of risk management 409–10
 sources of 411–13
- risk attitude 27–28, 74, 123–26
 4Cs of 123–24
 distinction from risk appetite 125
 universe of risk 124
- risk attitude matrix 123–26
- risk-aware culture 61, 68, 74, 289–92, 395–96
 embedding risk management 291, 292
- risk awareness campaign 292
- risk calculations 301–02
- risk capacity of an organization 145–46, 286, 299,
 300–01
- risk exposure and 303–05
 ways to increase 101
- risk classification systems 20–21, 127–37
 advantages of 127–28
 compliance risks 136
 control risks 136
 examples 129–31
 finance sector 137
 hazard risks 136, 137
 opportunity risks 136
 project risks 136
 short-, medium- and long-term risks 128–29
 strategic risks 136
 time to impact 128–29
- risk committees, Thomas Miller Holdings Ltd case
 study 160–70

- risk criteria for an organization 70, 125–26
 risk culture 255–56
 components of a good risk culture 393
 defining 289–92
 evaluation using the CoCo framework 389–91
 FCA case study 257–58
 impact of reward systems 109
 measuring 292–94
 relationship to the control environment 389–91
 training in risk management and 312, 313
 ways to improve 293–94
 risk description 19
 risk elimination 172, 177–78
 risk evaluation 122, 146–47
 risk exposure 70, 145, 300–02
 quantification of 119
 risk capacity and 303–05
 total acceptable risk exposure 286
 total (actual) risk exposure 286
 risk financing 42–43, 177
 risk frequency 148
 risk impact (magnitude) 21–22, 23, 120–22, 141
 timescale 34–35
 risk improvement, use of a risk matrix 121
 risk information and communication 313–15
 use of technology 316–19
 risk likelihood 21–22, 23, 120–22, 141
 controlling downside risk 148–49
 risk magnitude, controlling downside risk 149–50
 risk management
 5Es of opportunity management 57–58
 achieving benefits 57
 activities 54
 barriers to implementation 288–89
 benefits 4–5
 calculated risks 45–46
 changing face of 99
 context of 1
 CSR and 237–39
 definitions of 45
 different approaches to 357–81
 driving and enabling activities 57–58
 effective and efficient core processes 54–55
 features of 5
 financial approach to 44
 five lines of assurance model 405–06
 future for 7–8
 impact on operations 229
 implementation 56
 importance for organizations 45–46
 in practice 6–7
 introduction to 9–10
 levels of sophistication 50–52
 objectives 53–54
 origins of 42–45
 outputs 413
 overview 2–3
 principles of 52
 relationship with organizational management 405
 specialist areas 47–48
 steps to successful risk management 286–89
 strategy 263–64
 styles of 286, 287
 terminology 3–4
 three lines of defence approach 398–99, 402, 403,
 404, 405
 uniting into a single function 44
 widening the scope of risk 43–44
 working relationship with internal audit 401–04
 see also enterprise risk management (ERM)
 risk management activities, aligning with core business processes 294–96
 risk management committees (RMC) 283–85
 risk management context *see* context for ERM; context of risk management; control environment
 risk management framework 62–63, 69, 259–62
 risk management information system (RMIS) 289, 317–19
 risk management manual 63, 259, 263, 265–68
 risk management policy 74, 259, 261–62, 263
 risk management process 49–50, 61, 62–63
 bow-tie tool 28–30
 context 69–78
 ISO 31000 63–64, 65, 68
 Ocado case study 10–11
 RASP approach 62–63
 risk management protocols 264–65, 267
 risk management roles 274–76
 risk management standards 3, 59–68
 approaches followed by 61
 context 61–63
 COSO ERM cube 64, 66, 66–67, 68
 ISO 31000 63–64, 65, 68
 risk management process 61, 62–63
 routine review of standards 68
 setting objectives for ERM 105–07
 updating of risk terminology 67–68
 use by listed companies 60–61
 risk manager role 278–80
 risk map 21–22
 risk matrix 20
 output from risk assessment workshops 158–59
 prioritizing risks 101
 project risks 368–69
 risk appetite 124, 300–02
 risk attitude 123–26
 risk likelihood and risk impact 21–22, 23, 120–22
 use in risk analysis 138, 139
 risk maturity 292, 293
 four levels of (4Ns) 295–98
 risk maturity models 296–98, 389
 risk ownership 273–74, 276
 risk perception 122–23, 125
 risk practitioner competencies 320–29
 analytical skills 327–28
 business skills 321
 codes of conduct 322
 communication skills 322, 323–26
 competency frameworks 320–21
 conflict resolution 326
 CRAM skills 322
 cultural awareness 326
 decision-making skills 328
 ethics codes 322
 facilitating risk assessment workshops 327
 influencing 326
 leadership skills 328–29
 listening skills 326
 management skills 328–29
 motivational skills 328
 negotiation skills 326
 people skills 322–23
 political skills 326–27

- preparing a training course or presentation 327
problem-solving skills 327–28
range of skills 321–23
relationship skills 326–27
running training courses and workshops 324–26
self-development 322
self-management 322
soft skills 322–23
technical skills 320–21, 322
- risk protocols 62, 69, 70, 259–61
- risk radar of an organization 74
- risk ranking 122
- risk rating 120–22
- risk registers 75–78, 270–71, 399
- risk reporting *see* reporting on risk management
- risk response 20, 146–47, 167–68, 171–81
- 4Es of opportunity risk response 142–43
 - 4Ts of hazard response 142–43, 171–78
 - 5Es of opportunity risk response 143
 - consistent response to risk 311–12
 - risk transfer 198–206
 - role of the control environment 389–91
 - strategic risk response 178, 178–81
- risk retention 200
- risk severity 122
- risk sharing 177, 199
- risk strategy 62, 69, 70, 255–56, 259–61
- risk termination 172, 177–78
- risk tolerance 172, 174–75
- risk appetite statements 306–08, 309
 - risk transfer 172, 176–77
 - alternative risk transfer (ART) 200
 - captive insurance companies 200, 204–06, 301
 - insurance 38, 198–206
 - options available to organizations 200
 - pooling risk 200
- risk treatment 172, 175–76
- risk treatment controls for hazard risks 182–92
- risk versus reward in strategy 178, 179–81
- risk workshops 118, 119, 119, 291, 158–59, 324–26
- riskiness index 71–72, 159–62
- Royal Borough of Kensington and Chelsea, risk management policy 261–62
- safety culture 395–96
- Sainsbury's Bank case study 385–86
- Sarbanes-Oxley Act 2002 (US) (SOX) 44, 53, 60, 129, 231–32, 252, 272, 280–81, 336, 416, 418–19
- scenario planning
- reasonable worst-case scenarios 216
 - resilience and 215–16
- Securities and Exchange Commission (SEC), US 421
- SEE (social, ethical and environmental) concerns 236
- shareholders 72
- provision of data for 350–51
 - reporting to 231
- shop security standards 37–38
- short-term risks 128–29
- significant risks
- identification of 24–26, 115, 120–22, 171
 - key dependencies and 173, 174
 - Lenovo Group case study 11–12
 - tests for 143–45
- Singapore Airlines case study 256–57
- skills *see* risk practitioner competencies
- SMART objectives 108
- Softcat plc case study 113
- Solvency II European Directive 48, 358
- specialist areas of risk management 47–48
- speculative risks 17, 40
- stakeholder management, Capital case study 332–33
- stakeholder needs, reporting on 232
- stakeholders 348–56
- building relationships with 326–27
 - communication of risk information to 313–15
 - CSR and 238–39
 - definitions of 348
 - dialogue with 350–51
 - ethical dilemma of companies 348–49
 - examples of harms caused by companies 348–49
 - expectations of organizations 24, 226–27, 348–50, 351–53
 - external stakeholders 71, 72
 - identifying and mapping 353–54
 - importance of core processes for 351–53
 - internal stakeholders 72–73
 - involvement in operational activities 355–56
 - questioning racism in society 350
 - range of (CSFRS) 327, 348
 - reporting to 231
 - strategy and 353–54
 - tactical stakeholders 354–55
- Staley, Jes 314–15
- Standards Australia 59
- standards development in risk management 43
- standards for risk management 58–68
- statutory responsibilities of management 276–78
- STOC (strategy, tactics, operations and compliance) core processes 4, 22–23, 26, 116, 126, 129, 149, 159, 308, 310
- strategic approach to risk management, Lincolnshire County Council case study 81
- strategic decision-making, role of risk management 55
- strategic partnerships, supply chains 376–77
- strategic risk response 178, 178–81
- strategic risks 136
- strategic use of ERM 252–53
- strategy
- importance of stakeholder analysis 353–54
 - risk versus reward 178, 179–81
 - setting objectives for ERM 106–07
 - upside of risk 162–63
- see also* risk strategy
- strategy formulation, role of risk assessment 115, 227–29
- styles of risk management 286, 287
- supply chain risk management 375–81
- definition of supply chain 375
 - ethical trading 239–42
 - joint ventures 377–78
 - outsourcing of operations 378–80
 - risks associated with contracts 380–81
 - scope of the supply chain 376
 - strategic partnerships 376–77
 - uncertainties in supply chains 375–76
- sustainability
- Dangote Cement plc case study 168–69
 - energy production 48
- SWOT analysis 25, 73, 119–20, 133, 228, 233
- system risks 359
- tactical stakeholders 354–55
- tactics 228–29
- target level of risk 19–20, 139, 139–40

- Task Force on Climate-related Financial Disclosures (TCFD) UK 251–52
 tax risk management, three lines of defence approach 404
 technology
 shop security systems 37–38
 to support risk management 316–19
 terminology 3–4
 shared risk vocabulary 315–17
 updating of risk terminology 67–68
The Orange Book (HM Government) 17, 45, 61, 334
 definition of ERM 85
 governance and leadership 344
 risk classification system 130, 134–36
 risk management framework 262
 risk monitoring 193–94
 risk reporting 193
 risk response 171
 types of hazard controls 182–85
 Thomas Miller Holdings Ltd case study 169–70
 three lines of defence model 194, 275–76, 340, 398–99, 402, 403, 404, 405
 timescale of risk impact 34–35
 total cost of risk 42–43
 total cost of risk calculations 301–02
 total risk exposure 145
 training in risk management 43, 324–26
 certificate in Sustainability and Climate Change 252
 consistent response to risk 311–12
 risk culture and 312, 313
 triggers for major crises 35
 triggers for risks 146
 UK Cabinet Office case study 12–13
 UK Charity Commission guidance on risk reporting 421–22
 UK Corporate Governance Code 60, 162, 335, 409
 UK Department for Work and Pensions (DWP) case study 334
 UK Financial Conduct Authority 19
 UK government, reporting on national security 423–25, 425
 uncertainty
 in projects 366, 368–70, 371–72
 in supply chains 375–76
 risk and 15, 303
 uncertainty risks 17
 management of 39–40
 see also control risks
 underwriting risk 359
 Unilever case study 384–85
 universe of risk 124
 upside of risk, maximizing 155–65
 defining the upside 155–57
 honesty boxes 157
 opportunity assessment 157–59
 riskiness index 159–62
 upside in operations 164–65
 upside in projects/programmes 163–64
 upside in strategy 162–63
 upside of compliance risks 165
 US stock exchange listed companies, reporting on risk management 420–21
 value added by internal audit 410
 value added by risk management 246–53
 benefits of an ERM approach 248–51
 evidence for 246–47
 performance improvement 247–48
 strategic use of ERM 252–53
 VUCA (volatile, uncertain, complex and ambiguous) environment 207–08
 Walker review of bank governance and regulation 341
 Walmart 238
 Wates principles (UK) 99
 whistleblowing 334, 336
 Barclays fine for non-compliance 314–15
 East African Breweries Limited case study 221
 Whitbread plc case study 220–21
 Windsor Castle fire 1992 153
 Zuckerberg, Mark 15