

Sixth Edition

Fundamentals of Risk Management

Understanding, evaluating and implementing
effective enterprise risk management

Paul Hopkin and Clive Thompson



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
	<i>Appendix A: Abbreviations and acronyms</i>	<i>426</i>
	<i>Appendix B: Glossary of terms</i>	<i>429</i>
	<i>Index</i>	<i>437</i>