CONTENTS

List of figures xv
List of tables xvii
Foreword xx
Acknowledgements xxi

Introduction 1

PART ONE Introduction to risk management 11

Learning outcomes for Part One 11
Part One further reading 11
Part One case studies 12
  Rank Group: How we manage risk 12
  ABIL: Risk management overview 12
  BIS: Approach to risk 13

01 Approaches to defining risk 15
Definitions of risk 15
Types of risks 17
Risk description 18
Inherent level of risk 20
Risk classification systems 20
Risk likelihood and magnitude 21

02 Impact of risk on organizations 24
Level of risk 24
Impact of hazard risks 25
Attachment of risks 26
Risk and reward 29
Attitudes to risk 30
Risk and triggers 32

03 Types of risks 35
Timescale of risk impact 35
Four types of risk 36
Embrace opportunity risks 39
12 Risk analysis and evaluation 143

Application of a risk matrix 143
Inherent and current level of risk 145
Control confidence 147
4Ts of hazard risk response 148
Risk significance 149
Risk capacity 150

13 Loss control 152

Risk likelihood 152
Risk magnitude 153
Hazard risks 154
Loss prevention 156
Damage limitation 157
Cost containment 157

14 Defining the upside of risk 159

Upside of risk 159
Opportunity assessment 162
Riskiness index 163
Upside in strategy 167
Upside in projects 168
Upside in operations 169

PART FOUR Risk response 171

Learning outcomes for Part Four 171
Part Four further reading 171
Part Four case studies:
  Intu Properties: Insurance renewal 172
  The Walt Disney Company: Disclosures about market risks 172
  Australian Mines Limited: Risk assessment and management 173

15 Tolerate, treat, transfer and terminate 175

The 4Ts of hazard response 175
Tolerate risk 177
Contents

16  Risk control techniques  186
    Types of controls  186
    Hazard risk zones  190
    Preventive controls  192
    Corrective controls  192
    Directive controls  193
    Detective controls  194

17  Insurance and risk transfer  196
    Importance of insurance  196
    History of insurance  197
    Types of insurance cover  198
    Evaluation of insurance needs  200
    Purchase of insurance  200
    Captive insurance companies  203

18  Business continuity  206
    Business continuity management  206
    Business continuity standards  208
    Successful business continuity  211
    Business impact analysis (BIA)  214
    Business continuity and ERM  214
    Civil emergencies  216

PART FIVE  Risk strategy  219

Learning outcomes for Part Five  219
Part Five further reading  219
Part Five case studies:  220
    AMEC Foster Wheeler: Principal risks and uncertainties  220
    BBC: Internal controls assurance  220
    Emperor Watch & Jewellery: Risk management  221

19  Core business processes  223
    Dynamic business models  223
    Types of business processes  226
Part Six case studies:  286
Network Rail: Our approach to risk management  286
Ekurhuleni Metropolitan Municipality (EMM): Risk management  286
Ericsson: Corporate governance report  287

24  Risk-aware culture  289
Styles of risk management  289
Steps to successful risk management  290
Defining risk culture  291
Measuring risk culture  295
Alignment of activities  297
Risk maturity models  299

25  Importance of risk appetite  302
Nature of risk appetite  302
Risk appetite and the risk matrix  304
Risk and uncertainty  306
Risk exposure and risk capacity  308
Risk appetite statements  310
Risk appetite and lifestyle decisions  313

26  Risk training and communication  316
Consistent approach to risk  316
Risk training and risk culture  317
Risk information and communication  319
Shared risk vocabulary  321
Risk information on an intranet  322
Risk management information system (RMIS)  323

27  Risk practitioner competencies  325
Competency frameworks  325
Range of skills  326
Communication skills  328
Relationship skills  331
Analytical skills  332
Management skills  333

PART SEVEN  Risk governance  335

Learning outcomes for Part Seven  335
Part Seven further reading  335
## Contents

Part Seven case studies: 336
- Severn Trent Water: Our approach to risk 336
- Tim Hortons: Sustainability and responsibility 336
- DCMS: Capacity to handle risk 337

### 28 Corporate governance model 339

Corporate governance 339
- OECD principles of corporate governance 340
- LSE corporate governance framework 342
- Corporate governance for a bank 343
- Corporate governance for a government agency 344
- Evaluation of board performance 347

### 29 Stakeholder expectations 351

Range of stakeholders 351
- Stakeholder dialogue 353
- Stakeholders and core processes 354
- Stakeholders and strategy 356
- Stakeholders and tactics 357
- Stakeholders and operations 358

### 30 Operational risk management 360

Operational risk 360
- Definition of operational risk 361
- Basel II and Basel III 363
- Measurement of operational risk 364
- Difficulties of measurement 366
- Developments in operational risk 367

### 31 Project risk management 370

Introduction to project risk management 370
- Development of project risk management 371
- Uncertainty in projects 372
- Project lifecycle 374
- Opportunity in projects 377
- Project risk analysis and management 378

### 32 Supply chain management 380

Importance of the supply chain 380
- Scope of the supply chain 381
- Strategic partnerships 382
- Joint ventures 384
Outsourcing of operations 384
Risk and contracts 387

**PART EIGHT** Risk assurance 389

Learning outcomes for Part Eight 389
Part Eight further reading 389
Part Eight case studies: 390
  - Unilever: Our risk appetite and approach to risk management 390
  - Colgate Palmolive: Damage to reputation 390
  - Sainsbury’s and Tesco: Principal risks and uncertainties 391

33 The control environment 393

Nature of control environment 393
Purpose of internal control 394
Control environment 395
Features of the control environment 397
CoCo framework of internal control 399
Good safety culture 401

34 Risk assurance techniques 402

Audit committees 402
Role of risk management 404
Risk assurance 405
Risk management outputs 407
Control risk self-assessment 408
Benefits of risk assurance 409

35 Internal audit activities 411

Scope of internal audit 411
Role of internal audit 412
Undertaking an internal audit 414
Risk management and internal audit 416
Management responsibilities 419
Five lines of assurance 420

36 Reporting on risk management 423

Risk reporting 423
Sarbanes–Oxley Act of 2002 425
Risk reports by US companies 426
Charities’ risk reporting 428
Public-sector risk reporting  429
Government report on national security  430

Appendix A: Abbreviations and acronyms  433
Appendix B: Glossary of terms  436
Appendix C: Implementation guide  446
Index  449