Fundamentals of Risk Management
Understanding, evaluating and implementing effective risk management

Paul Hopkin
# CONTENTS

List of figures  xiv  
List of tables  xvi  
Preface  xviii  
Acknowledgements  xix  

**Introduction**  1  

**PART ONE** Introduction to risk management  11  
Learning outcomes for Part One  11  
Part One Further reading  12  

**01 Approaches to defining risk**  13  
Definitions of risk  13  
Types of risks  15  
Risk description  16  
Inherent level of risk  17  
Risk classification systems  18  
Risk likelihood and magnitude  19  

**02 Impact of risk on organizations**  21  
Level of risk  21  
Impact of hazard risks  22  
Attachment of risks  22  
Risk and reward  25  
Risk and uncertainty  27  
Attitudes to risk  27  

**03 Types of risks**  29  
Timescale of risk impact  29  
Hazard, control and opportunity risks  30  
Hazard tolerance  33  
Mitigation of hazard risks  34  
Management of uncertainties  35  
Embracing opportunities  35
## Contents

### 04 Development of risk management  37
- Origins of risk management  37
- Changes in the marketplace  39
- Insurance origins of risk management  42
- Specialist areas of risk management  42
- Enterprise risk management  44
- Levels of risk management sophistication  45
- Bow-tie representation of risk management  47

### 05 Principles and aims of risk management  49
- Principles of risk management  49
- Importance of risk management  50
- Risk management activities  52
- Efficient, effective and efficacious  53
- Implementing risk management  54
- Achieving benefits  55

### 06 Risk management standards  57
- Scope of risk management standards  57
- Risk management process  60
- Risk management framework  60
- COSO ERM cube  62
- Features of RM standards  62
- Alternative approaches  65
- Case studies:
  - Generali Group: Risk factors  68
  - Rio Tinto: Managing risk effectively  69

**PART TWO**  Risk strategy  71

- Learning outcomes for Part Two  71
- Part Two Further reading  71

### 07 Risk management framework  73
- Risk architecture, strategy and protocols  73
- Risk management manual  76
- Risk management architecture  78
- Risk management strategy  79
- Risk management protocols  80
- Establishing the context  81
08  Risk management documentation  84
    Risk management documentation  84
    Risk response and improvement plans  86
    Event reports and recommendations  87
    Risk performance and certification reports  88
    Designing a risk register  88
    Using a risk register  89

09  Risk management responsibilities  96
    Allocation of responsibilities  96
    Range of responsibilities  97
    Statutory responsibilities of management  99
    Role of the risk manager  101
    Risk architecture  103
    Risk committees  106

10  Risk-aware culture  109
    Styles of risk management  109
    Defining risk culture  110
    Measuring risk culture  112
    Risk culture and risk strategy  113
    Alignment of activities  114
    Risk maturity  114

11  Risk training and communication  118
    Consistent response to risk  118
    Risk training and risk culture  119
    Risk information and communication  120
    Shared risk vocabulary  122
    Risk information on an intranet  122
    Risk management information systems (RMIS)  123

12  Risk practitioner competencies  126
    Competency frameworks  126
    Range of skills  128
    Communication skills  128
    Relationship skills  132
    Analytical skills  133
    Management skills  134
PART THREE Risk assessment 137

Learning outcomes for Part Three 137
Part Three Further reading 138

13 Risk assessment considerations 139

Importance of risk assessment 139
Approaches to risk assessment 140
Risk assessment techniques 141
Risk matrix 143
Risk perception 145
Risk appetite 147

14 Risk classification systems 151

Short, medium and long-term risks 151
Nature of risk classification systems 152
Examples of risk classification systems 154
FIRM risk scorecard 155
PESTLE risk classification system 156
Hazard, control and opportunity risks 158

15 Risk likelihood and impact 161

Application of a risk matrix 161
Inherent and current level of risk 162
Control confidence 164
4Ts of risk response 165
Risk significance 166
Risk capacity 167

16 Loss control 170

Risk likelihood 170
Risk magnitude 171
Hazard risks 172
Loss prevention 174
Damage limitation 175
Cost containment 175
17 Defining the upside of risk  177
Upside of risk  177
Opportunity assessment  180
Riskiness index  180
Upside in strategy  184
Upside in projects  185
Upside in operations  186

18 Business continuity planning  187
Importance of business continuity planning and disaster recovery planning  187
Business continuity standards  189
Successful business continuity planning and disaster recovery planning  192
Business impact analysis (BIA)  194
Business continuity planning and enterprise risk management  195
Civil emergencies  195
Case studies:
BG Group: Principal risks and uncertainties  196
IHG: Managing risk in hotels  197

PART FOUR  Risk response  199

Learning outcomes for Part Four  199
Part Four Further reading  199

19 Enterprise risk management  201
Enterprise-wide approach  201
Definitions of ERM  203
ERM in practice  204
ERM and business continuity  205
ERM in energy and finance  206
Future development of ERM  207

20 Importance of risk appetite  209
Risk capacity  209
Risk exposure  210
Nature of risk appetite  213
Risk appetite statements  217
Risk management and uncertainty  220
Risk appetite and lifestyle decisions  222
21 **Tolerate, treat, transfer and terminate** 224

The 4Ts of hazard response 224
Tolerate risk 226
Treat risk 228
Transfer risk 229
Terminate risk 230
Project and strategic risk response 231

22 **Risk control techniques** 235

Hazard risk zones 235
Types of controls 236
Preventive controls 240
Corrective controls 241
Directive controls 241
Detective controls 242

23 **Control of selected hazard risks** 244

Cost of risk controls 244
Control of financial risks 247
Control of infrastructure risks 249
Control of reputational risks 253
Control of marketplace risks 255
Learning from controls 256

24 **Insurance and risk transfer** 260

Importance of insurance 260
History of insurance 261
Types of insurance cover 262
Evaluation of insurance needs 264
Purchase of insurance 264
Captive insurance companies 267
Case studies:
Nationwide: Risk management and control 269
Rank Group: Governance framework 270
PART FIVE  Risk and organizations  271

Learning outcomes for Part Five  271
Part Five Further reading  272

25  Corporate governance model  273

Corporate governance  273
OECD principles of corporate governance  274
LSE corporate governance framework  275
Corporate governance for a bank  277
Corporate governance for a government agency  278
Evaluation of board performance  281

26  Stakeholder expectations  284

Range of stakeholders  284
Stakeholder dialogue  286
Stakeholders and core processes  287
Stakeholders and strategy  288
Stakeholders and tactics  290
Stakeholders and operations  290

27  Analysis of the business model  292

Simplified business models  292
Core business processes  295
Efficacious strategy  296
Effective processes  296
Efficient operations  297
Reporting performance  298

28  Project risk management  300

Introduction to project risk management  300
Development of project risk management  301
Uncertainty in projects  302
Project lifecycle  304
Opportunity in projects  307
Project risk analysis and management  308
29 Operational risk management 310
Operational risk 310
Definition of operational risk 311
Basel II 313
Measurement of operational risk 314
Difficulties of measurement 316
Developments in operational risk 317

30 Supply chain management 320
Importance of the supply chain 320
Scope of the supply chain 321
Strategic partnerships 323
Joint ventures 323
Outsourcing of operations 324
Risk and contracts 326
Case studies:
BBC: Corporate governance framework 328
Sainsbury: RM and internal controls 329

PART SIX Risk assurance and reporting 331
Learning outcomes for Part Six 331
Part Six Further reading 332

31 Evaluation of the control environment 333
Nature of internal control 333
Purpose of internal control 334
Control environment 335
Features of the control environment 337
CoCo framework of internal control 339
Risk-aware culture 341

32 Activities of the internal audit function 342
Scope of internal audit 342
Financial assertions 344
Risk management and internal audit 344
Risk management outputs 348
Role of internal audit 348
Management responsibilities 350
33 Risk assurance techniques 352
Audit committees 352
Role of risk management 355
Risk assurance 355
Undertaking an internal audit 357
Control risk self-assessment 359
Benefits of risk assurance 360

34 Reporting on risk management 361
Risk documentation 361
Sarbanes–Oxley Act of 2002 362
Risk reports by US companies 363
Charities’ risk reporting 365
Public sector risk reporting 366
Government report on national security 367

35 Importance of corporate reputation 370
Reputation and corporate governance 370
CSR and risk management 371
CSR and reputational risk 372
Supply chain and ethical trading 373
CSR reporting 375
Importance of reputation 376

36 Future of risk management 379
Review of benefits of risk management 379
Steps to successful risk management 380
Changing face of risk management 383
Emerging risks 384
Emerging trends in risk management 386
Future developments 387
Case studies:
John Lewis: Corporate social responsibility (CSR) 389
Man Group: Risk and control reporting 390

Appendix A: Abbreviations and acronyms 391
Appendix B: Glossary of terms 394
Appendix C: Implementation guide 404
Index 407