

CONTENTS

Foreword by Steve Fowler vii

Foreword by Mrutyunjay Mahapatra x

Acknowledgements xii

01 Introduction 1

Outline 1

Business is about taking risk 2

The difference between taking managed and unmanaged risks 5

Benefits of well-managed enterprise risk management 7

The myths about risk 8

Capacity to take risk 12

Questions for senior management and the board to ask 13

Notes 14

02 About enterprise risk management 15

Outline 15

Risk management 16

Implementing the programme for ERM 20

ERM – the process 22

Essential attributes of ERM for delivering value and capacity 23

Top level leadership in ERM 24

Identifying risk: types of risk, risk lists and taxonomies 26

Evaluating and prioritizing risk 29

Governance, risk and compliance 36

Questions for senior management and the board to ask 37

Notes 38

03 Risk as an opportunity/threat to objectives and value drivers 39

Outline 39

Risk – opportunities and threats 39

Risk as uncertainty 43

Threat and opportunity management 45

Dealing with threat 45

Dealing with opportunity 47

Differentiating between objectives, strategic goals and value drivers 51

Questions for senior management and the board to ask 57

Notes 57

04 Implementing an ERM programme 59

Outline 59

Establish the foundation – the operating model for ERM 59

Documentation for ERM 62

Language, oversight and governance 63

Building capabilities: assess and develop responses and capabilities 66

Improving capabilities: monitoring and communication 68

Questions for senior management and the board to ask 70

05 Risk attitude, risk propensity and risk appetite 73

Outline 73

Risk aversion versus risk hungry 73

Applications of a risk appetite tool 76

Risk capacity versus tolerance 77

Developing risk appetite frameworks 78

The risk of not taking a risk 82

Risk appetite and value drivers 83

Organization behind the setting of risk appetite 88

Examples of risk appetite statements 90

Questions for senior management and the board to ask 93

Notes 95

06 ERM culture, blame, boundaries and elephants in the room 97

Outline 97

ERM cultures and the blame culture 98

Using risk appetite as a tool to destroy the blame culture 99

Managing risk 101

The link between managed risk taking, mice, Maslow and Herzberg 104

The elephant in the room and conduct risk 108

In the public interest 113

Questions for senior management and the board to ask 114

Notes 117

07 Embedding and integrating ERM 119

Outline 119

What does embedding mean? 119

Main aspects of embedding ERM 121

A 16-step plan for embedding ERM 128

The three lines of play 130

Questions for senior management and the board to ask 136

Notes 138

- 08 Maturity in enterprise risk management 139**
Outline 139
How risk maturity enables managed risk taking 139
Action plan for measuring and tracking performance 143
Questions for senior management and the board to ask 152
Notes 153
- 09 Resilience and sustainable habits 155**
Outline 155
Business continuity management 156
The role of senior management 161
Corporate social responsibility 166
Questions for senior management and the board to ask 172
Notes 174
- 10 Learning and communication 177**
Outline 177
The learning habit 179
ERM information systems 188
External communication 194
Questions for senior management and the board to ask 194
Notes 196
- 11 Conformance, performance, roles, responsibilities and regulations 199**
Outline 199
Managing conformance versus performance 200
The role of boards in ERM 200
Governance for ERM 203
The role of internal and external audit in ERM 208
Compliance requirements for risk management: various countries and industries 211
Questions for senior management and the board to ask 220
Notes 222
- 12 Deliverables from quantitative ERM approaches 223**
Outline 223
Measuring and valuing 223
Models for valuing risk and capital 229
Own risk and solvency assessments – a useful model 232
Stress testing and reverse stress testing 235
Risks that cannot be valued 239
Questions for senior management and the board to ask 240
Notes 242

13 Simple, elegant ERM tools for senior management 243

Outline 243

The triangle of risk – trigger, environment, strength or weakness 244

Using cause and consequence analysis to transform risk approach 249

Macro and micro risk management 252

Questions for senior management and the board to ask 253

Notes 254

14 ERM and performance management synergies 255

Outline 255

Risk management alignment within the organization 256

Performance management 256

Performance management methods 258

Questions for senior management and the board to ask 263

Notes 264

15 The key strategic questions for senior management and boards to ask themselves 265

Outline 265

Recognizing the risks *of* versus the risks *to* the strategic plan 266

The key strategic questions 268

Summary 281

Appendix 1. Examples of corporate governance and ERM regulations 283

Appendix 2. The main principles of the UK Code of Governance, October 2012 285

Appendix 3. Summary COSO guidance 287

Appendix 4. Case study: Applying a more granular mathematical model to a risk for a non-financial organization 291

Appendix 5. Capital and risk considerations for US insurers, from NAIC ORSA Guidance 294

Appendix 6. Sample terms of reference for a board risk committee 297

Appendix 7. Example of roles of CRO and ERM team 302

Further Reading 305

Index 307