

# The Risk Management Universe

*A guided tour*

Edited by

*David Hillson*

First published in the UK in 2006  
Second edition 2007 by BSI  
389 Chiswick High Road  
London W4 4AL

© British Standards Institution 2006, 2007

All rights reserved. Except as permitted under the *Copyright, Designs and Patents Act 1988*, no part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior permission in writing from the publisher.

Whilst every care has been taken in developing and compiling this publication, BSI accepts no liability for any loss or damage caused, arising directly or indirectly in connection with reliance on its contents except to the extent that such liability may not be excluded in law.

The right of the contributors to be identified as the authors of this Work has been asserted by them in accordance with sections 77 and 78 of the *Copyright, Designs and Patents Act 1988*.

The authors have made every effort to seek permissions for all material used. Any omissions that are drawn to the attention of the publisher will be included in any future editions of the book.

Typeset in Sabon by  
Florence Production Ltd, Stoodleigh, Devon  
Index compiled by Indexing Specialists (UK) Ltd  
Printed in Great Britain by  
MPG Books, Bodmin, Cornwall

*British Library Cataloguing in Publication Data*  
A catalogue record for this book is available from  
the British Library

ISBN 978-0-580-50346-7 2nd edition

(ISBN 0-580-43777-9 1st edition)

# Contents

List of Figures	vii
List of Tables	x
Notes on the Contributors	xi
Foreword	xix
<i>Steve Fowler, CEO, Institute of Risk Management</i>	
1. Surveying the Risk Management Universe – Where Are We Now? <i>David Hillson</i>	1
2. Strategic Risk Management <i>Richard Anderson</i>	10
3. Corporate Governance <i>David Smith and Rob Politowski</i>	42
4. Financial Risk Management <i>David Bobker</i>	68
5. Business Continuity Management <i>John Sharp</i>	98
6. Reputational Risk <i>Arif Zaman</i>	128

vi *Contents*

7. Risk-assessed Marketing Planning <i>Terry Kendrick</i>	157
8. Operational Risk Management <i>Keith Blacker</i>	185
9. Project Risk Management <i>Stephen Ward</i>	212
10. Environmental Risk Management <i>Simon Pollard and Peter Young</i>	241
11. Legal and Contractual Risk Management <i>Anthony Cherry</i>	266
12. Technical Risk Management <i>Tyson Browning</i>	294
13. Managing Fraud Risk <i>Jon Finch</i>	323
14. Counter-terrorism Risk Management <i>Richard Flynn</i>	352
15. Understanding The Risk Management Universe – Consensus and Controversy <i>David Hillson</i>	377
Index	387

## *Figures*

2.1	Relationship of attribute to long-term performance	28
2.2	Balanced risk: mapping all four attributes	29
2.3	Enron risk culture	29
2.4	UK plc risk culture?	30
2.5	Target risk culture?	31
2.6	COSO: elements of control	32
2.7	COSO: the enterprise control framework	33
2.8	A new approach to controlling risk	34
3.1	Components of successful corporate governance	44
3.2	Corporate governance organigram	52
3.3	Relationship between threat and opportunity	53
3.4	Process for managing threats and opportunities	56
3.5	Risk matrix	58
3.6	IMS model	65
4.1	BP Ordinary share price 4 Jan 1993 – 31 Dec 2004	71
4.2	US\$/GB£ Rate Oct 1993 – Apr 2005	72
4.3	Three-month US Treasury Bill rate 1954–2005	73
4.4	Four simulated Brownian sample paths	73
4.5	The normal distribution assumed for market risk	75
4.6	One-sided loss curve – credit risk/operational risk	76
4.7	Simulated total corporate profit	83
5.1	External drivers for introduction of BCM	101
5.2	BCM as a unifying process	105
5.3	The BCM life cycle	106
5.4	Possible BCM structure	107
5.5	High-level process mapping example	110
5.6	Detailed process mapping example	110
5.7	Mapping resources to critical activities	111
5.8	Example of a risk matrix	112

5.9	Frequency of BCP rehearsals	122
5.10	Results of BCM rehearsals	122
5.11	Business continuity plan exercise process	124
6.1	Stakeholder expectations	129
6.2	Business challenges	130
6.3	Trust in leaders	131
6.4	A model of business relationships	132
6.5	Two ways to think about a business	134
6.6	Reputational risk and value creation	135
6.7	Customer loyalty across BTC and BTB markets	137
6.8	Customer, corporate and brand values	139
6.9	The six components of stakeholder sensitivity	153
7.1	The marketing planning process and risk	161
7.2	Addressing risks to the customer portfolio	171
7.3	A probability and consequences matrix for marketing planning	175
8.1	The jigsaw of operational risk responsibility	189
8.2	Core operational risk management model	191
8.3	Information flow for an incident database	193
8.4	Approaches to measuring operational risk	196
9.1	The SHAMPU process: flow chart portrayal	228
10.1	Fundamental concept of risk management showing regions of high (H), medium (M) and low (L) risk and objective of risk management	242
10.2	Framework for environmental risk assessment and management	246
10.3	Example conceptual model showing potential environmental exposures at a petrol retail forecourt	256
10.4	Example event tree for the release of flammable liquid from a process facility	257
10.5	The risk hierarchy from strategic to operational risk, applied here to the water utility sector	261
11.1	Illustration of crisis handling costs	271
11.2	Typical process flow	278
12.1	Example of a traditional process for managing technical risk	296
12.2	Standard risk model	297
12.3	Expected loss formula	298
12.4	Risk exposure in terms of probability and impact	299
12.5	Example risk reduction profile	300
12.6	Risk decreases with availability of useful information	302

12.7	Example TPM tracking chart for UCAV mission range	305
12.8	Conversion of week zero's three-point estimate to triangle distribution	307
12.9	Triangle distribution function showing relative probability of various range TPM outcomes at project start	307
12.10	CDF for UCAV range TPM	308
12.11	Utility curve for aircraft range	309
12.12	Reduction in unacceptable outcomes from week 0 to week 14	314
12.13	TPM profiles and risks during the UCAV preliminary design project	316
12.14	Overall risk profile for the UCAV preliminary design project	317
13.1	A schematic overview of the cyclic Fraud Risk Management Plan	341
14.1	Legal definition of terrorism	359
14.2	Terrorist attacks worldwide – by sector	360
14.3	Sources of information about terrorism	363
14.4	The components of a resilient business	367
14.5	The risk matrix	370

# *Tables*

1.1	Risk management professional bodies	3
1.2	Risk management standards and guidelines	4–5
3.1	Cascade of risk management system	55
5.1	Drivers for introduction of BCM, by sector	102
5.2	Drivers for introduction of BCM, by company size	103
6.1	Organizational memory and corporate amnesia	141
6.2	Reputational risk and employee branding	143
6.3	Reputational risk and intangible assets	155
7.1	Responses to risk	177
8.1	Comparison of people risk in industrial and financial settings	205
9.1	Typical uncertainty management issues in each stage of the project life cycle	215
9.2	Levels of objectives for project risk management	221
9.3	A nine-phase portrayal of the SHAMPU process	227
11.1	Example of expansion of subcategories of risk within each of the major categories	276
12.1	TPM data and risk levels at the beginning of the UCAV project	315
13.1	Sample FRMP content	345
14.1	Top 10 threats and disruptions to business	362
14.2	Some examples of threat, vulnerability and business impact	371

## *Notes on the Contributors*

**Richard Anderson** is a Director of Corporate Risk Group (<http://www.co-risk.com>) which he founded in conjunction with Professor Robert Baldwin of the London School of Economics in 2001. Corporate Risk Group advises organizations on how to develop their risk management programmes so that they are focused on generating performance gains rather than simply being compliance exercises. Richard worked with Professor Baldwin to develop a suite of diagnostic tools to help in this process and to assist companies in becoming Risk Intelligent Organizations. Richard has a particular interest in developing understanding around Balanced Risk and Risk Maturity. Richard advises organizations that include some of the world's largest companies headquartered in the UK and public sector equivalents.

Richard is a Chartered Accountant and a graduate of the London School of Economics. He regularly speaks at conferences and contributes articles to journals.

**Dr Keith Blacker BSc FCA MBA FIIA DBA** is a Director of Risk DNA Limited (<http://www.riskdna.co.uk>), a specialist risk management consultancy business. His expertise in risk management and business analysis has developed over many years both as an operational manager and as an adviser to businesses. Most of his 30-year career has been spent in the financial services industry both in the UK and abroad and he has been actively involved in implementing risk management frameworks in a number of organizations. Keith has a doctorate in Operational Risk Management from Henley Management College and has published a number of papers on the subject.

Keith is also a Director of the Henley Centre for Value Improvement, a research centre at Henley Management College, and Protection & Investment Ltd, a firm of Independent Financial Advisers regulated by

the UK Financial Services Authority, where he has responsibility for all corporate governance matters.

**Dr David Bobker MA DPhil ACA** is founder and Director of Real Assurance Risk Management (<http://www.realassurance.com>) which specializes in risk management, regulatory compliance, corporate governance and internal audit, delivering both consulting and training. He holds a First Class BA, MSc and DPhil in Mathematics all from Oxford University and is a Chartered Accountant.

David has spent a long and varied career in the financial services industry where he worked as an external auditor and an internal auditor (having been Head of Group Audit both for Alliance & Leicester plc and Norwich Union plc). He has authored a number of articles on internal audit and spoken widely at conferences in the UK and abroad. His interests also include corporate governance, having taken a keen interest in the original Turnbull consultation, and compliance, having been a group compliance officer and a supervisor at the Building Societies Commission (now part of the FSA) with responsibility for capital adequacy rules.

As well as supplying outsourced internal audit services, his recent consulting work has included quantified risk analysis and systems for clients. Always taking a keen interest in IT, he has now developed specialist Monte Carlo modelling software for the assessment and management of operational risk, as well as carrying out credit and market risk assignments. The other active area of work is training where over a three-year period he has delivered specialist courses on quantified risk methods to over 200 senior internal auditors and operational risk managers.

**Dr Tyson R. Browning** is Assistant Professor of Enterprise Operations at the M J Neeley School of Business at Texas Christian University in Fort Worth, Texas, USA. He teaches Operations Management (MBA Core) and Project Management (MBA elective) and conducts research on enterprise operations, process modelling, product development, project management, engineering management and systems engineering. He previously worked for Lockheed Martin Aeronautics Company, where he was the technical lead and chief integrator of the enterprise process architecture and author of company policies and processes driving the transition to a process-based company. Before joining Lockheed Martin, he worked with the Lean Aerospace Initiative at the Massachusetts Institute of Technology, conducting on-site research

at Boeing, Texas Instruments, General Electric, Daimler Chrysler and several other companies. Browning has also worked for Honeywell Space Systems and Los Alamos National Laboratory. He received a Bachelor's degree from Abilene Christian University and two Master's degrees and a PhD (in Technology Management and Policy) from MIT. He has authored over 20 papers on engineering management, risk management, the design structure matrix, organization design, process modelling and value measurement – publishing in *IEEE Transactions in Engineering Management*, *Systems Engineering*, *Project Management Journal*, *Technology Management Handbook* and others. He is a member of the International Council on Systems Engineering (INCOSE) and the Institute for Operations Research and the Management Sciences (INFORMS), and he also serves on the Editorial Board for *Systems Engineering*.

**Anthony Cherry** is a Partner in the national law firm, Beachcroft Wansbroughs. After graduating in Law from Manchester University in 1976 and serving Articles in the City he worked for three years in the legal department of ICI. Since 1983 he has been with his present firm and its predecessors. He is responsible for developing and delivering services, including Risk Counsel, which bring legal skills and experience to bear on business risk and opportunity in new and flexible ways. He also chairs the firm's Risk Management Directorate and contributes to its policy on Corporate Social Responsibility. He lives in Clevedon, North Somerset with his wife and three children.

**Jon Finch** retired in 2002 after 31 years in risk management, most recently as ICL/Fujitsu Services Group Business Risk Manager where he carried corporate responsibility for business risk management policy and processes. Based in corporate Internal Audit he worked to achieve protection against business risk. Jon Finch is well regarded within the UK risk management community as a specialist in business risk and practical business problem resolution. He was employed in commerce from 1961, in the UK Electricity and Gas Industries before ICL, initially as an accountant and later in IT system design and development. After joining ICL in 1971 he performed a significant number of internal and customer related troubleshooting assignments on behalf of the Board of ICL, of STC, and on secondment to major clients. Over the years Jon has succeeded in resolving crises in over 40 mainly litigious situations on behalf of ICL in 18 countries including Hong Kong, South Africa, New Zealand, Malaya, France, Germany, Hungary and Portugal.

Jon is semi-retired, writing and speaking on business risk management topics. He has the reputation of being an entertaining speaker in his field. He is married to an actress, has three children and lives in the Fens near Cambridge.

**Richard Flynn BSc (Hons) MSc RGN FRSA** is a serving Police Officer and is currently seconded to a national police unit providing protective security advice to the business community. He is the author of national guidances 'Expecting the unexpected' and 'Secure in the knowledge', both written to aid the business community in the development of security and business continuity plans. He has a wealth of experience working with the business community and his research interests include how organizations perceive and manage risk, and how crime prevention strategies can assist in the prevention of terrorism.

**Dr David Hillson PMP FIRM FAPM MCMI** is an international risk management consultant, and Director of Risk Doctor & Partners (<http://www.risk-doctor.com>). He is a frequent conference speaker and author on risk. David is recognized internationally as a leading thinker and practitioner in the risk field, and has made several innovative contributions to improving risk management. He is well known for promoting the inclusion of proactive opportunity management within the risk process, and has recently been working on applying emotional literacy to understand and manage individual and corporate risk attitudes.

David is active in the Project Management Institute (PMI) and was a founder member of its Risk Management Specific Interest Group. He received the 2002 *PMI Distinguished Contribution Award* for his work in developing risk management. He is an elected Fellow of both the Institute of Risk Management (IRM) and the Association for Project Management (APM), as well as being a member of the Chartered Management Institute.

**Terry Kendrick** is Director of the Centre for Marketing and Risk at the University of East Anglia (UEA). He has been a strategic marketing planning consultant for the past 18 years and has undertaken marketing planning projects in 17 countries for over 50 large organizations. He is particularly interested in the risks to effective marketing planning and has written both academic papers and managerial briefings on this topic. Terry is a member of the Chartered Institute of Marketing and contributes sessions to the MBA programme at UEA.

**Robert J Politowski** ACIB Dip Mgt Stud. MCMI LCIPD is a Director of IMS Risk Solutions. Rob has accomplished managerial and advisory skills at senior level with particular interest in Operations, Risk Management, Customer Service and Human Resources. Rob has over 20 years' experience in the retail financial sector in the UK. During this time he worked in various departments of a major UK Clearing Bank. He has substantial experience in the management and delivery of operations support through centralized operating centres including back office processing, customer service delivery and call centre operations. Additionally, he has significant experience in the management of operational risk issues within a wide range of banking operations encompassing credit risk, compliance and a range of special investigations having been an Auditor in the Group Audit function.

**Professor Simon Pollard** was appointed to the Chair in Waste and Environmental Risk Management at Cranfield University in September 2002. He obtained his PhD in Environmental Engineering from Imperial College in 1990. Simon has formerly held appointments at the Universities of Alberta and Edinburgh, with consultants Aspinwall & Company, with the Scottish Environment Protection Agency, and as the Environment Agency's Head of Risk Analysis. Simon's research and teaching interests are in sustainable technology systems, the management of wastes, contaminated land and environmental risk. He is the author of over 100 publications, Associate Editor of *Science of the Total Environment* and Director of Cranfield University's Integrated Waste Management Centre, coordinating activity on waste and resource management across the University. Simon has held professional appointments on the Government's Interdepartmental Liaison Group on Risk Assessment (ILGRA), the Executive Committee of the engineering institutions' Hazards Forum and has recently been elected to the Scientific and Technical Committee of the Chartered Institution of Wastes Management.

**John Sharp** FBCI (Hon) FCMI MCIM is recognized worldwide for the contributions he has made to Business Continuity Management. In 2004 he was made an Honorary Fellow of the Business Continuity Institute and received a special award for his outstanding contribution to the industry. Currently John is Policy and Development Director with Continuity Forum, an educational and development body. From 1997 until 2004 he was the Chief Executive Officer of the Business Continuity Institute where he was responsible for delivering services

to members throughout the world and working with all facets of industry, commerce and government to enhance the understanding and commitment to business continuity as a key management discipline.

John Sharp was chair of the committee that produced BSI's *Guide to Business Continuity Management* (PAS 56), and was also a member of the team producing BCM guidance for the UK Civil Contingencies Act. He works closely with government, regulators, police, security organizations and is a member of the London Resilience Business Team. John is a regular conference speaker and author on Business Continuity Management and has provided input to newspaper articles, radio, television and educational films.

**David A Smith BSc MSc Chartered Chemist** is Managing Director of IMS Risk Solutions with many years' experience of Health and Safety and Environmental Management Systems. He chairs a variety of important BSI Committees and represents the UK on ISO and CEN Committees on management systems standards and has substantial international experience in training, consultancy and auditing for a wide variety of clients in industry, government and the academic sector throughout the world. He has authored and edited a variety of books on management systems, most recently including a series of nine books on Integrated Management Systems published by British Standards Institution (BSI). He is co-author of the BSI publication *Managing Risk for Corporate Governance* – PD 6668:2000. Further publications include *Managing the Environment the 14001 Way* (1999, 2nd edn. 2005) – published by British Standards Institution – which is an award winning publication and provides comprehensive guidance on appropriate methodologies for effective environmental risk management systems. *Managing Safety the Systems Way* (1998) is a comprehensive guide to the implementation of Occupational Health and Safety Management systems to meet ILO and UK standards including the internationally recognized specification OHSAS 18001:1999 and BS 8800:2004.

**Stephen Ward** is Professor of Risk Management at the School of Management, University of Southampton, UK. He holds a BSc in Mathematics and Physics (Nottingham), an MSc in Management Science (Imperial College, London), and a PhD in developing effective models in the practice of operational research (Southampton). He is a member of the PMI and a Fellow of the UK Institute of Risk Management. He is Director of the School's MSc program in Risk Management.

Professor Ward's teaching interests cover a wide range of management topics including: decision analysis, managerial decision processes, insurance, operational and project risk management, and strategic management. For more than 20 years his research and consulting activities have been concerned with project risk management systems and the effective management of uncertainty. His latest book, *Risk Management – Organization and Context* (2004), discusses organization-wide approaches to integrated risk management, building on emergent issues in project risk management.

**Peter Young** has over 25 years experience as an environmental consultant specializing in research, policy and practical implementation of risk management programmes associated with waste, soil and water contamination. He has a First Class Honours degree in Environmental Chemistry from Edinburgh University, is a Chartered Chemist and an active member of the Chartered Institutes of Water and Environmental Management and Waste Management. He is currently Strategy Director of Enviro Consulting formed some years ago by the amalgamation of several UK consultancies, including Aspinwall and Co. where he was formerly Managing Director. He has published over 80 scientific and technical papers, contributed to statutory environmental guidance published by UK, Singapore and Hong Kong governments, and is a long-term member of the UK BSI Soil Quality Committee EH/4 and ASTM Committee D34 on Waste.

**Arif Zaman BA (Hons) MBA FRSA** is Visiting Fellow in the John Madejski Centre for Reputation and the Centre for Board Effectiveness. He is the author of *Reputational Risk* (Financial Times Executive Briefing, 2004) developed from research at Henley Management College. He recently returned to British Airways, where he leads several commercial projects, after a two-year sabbatical as an Associate Fellow at Chatham House, where he authored *Corporate Responsibility in Japan* (2003), and managing projects for policy-makers and corporates in Asia as an Advisor to the Commonwealth Business Council (CBC) and the Asian Productivity Organisation. In 2005 he was a member of Mitsubishi Corporation's Stakeholder Panel and in 2004 served on the drafting committee of the European Conference on CSR, at the invitation of the Dutch Presidency of the EU. He remains an advisor to the CBC. Previously he was Global Market and Industry Analyst at BA from 1993 to 2002 where he received a 'Recognising our People' award for his contribution to the Code of Conduct and BA's first Social Report

and Sustainability Policy, and the leading award from the air cargo industry for his research on logistics and global supply chains. Prior to this, he was at Valin Pollen, a leading financial PR consultancy, and HSBC. He is on the Board of the Strategic Planning Society and the Editorial Board of the US-based *Journal of Business Strategy* and was a contributor to *Strategic Thinking in Tactical Times* (Palgrave, 2004). He is a Director and trustee of the Strategic Planning Society and the Red Shift Theatre Company. He is also an Associate of the Foreign Policy Centre, a Fellow of the Royal Asiatic Society and a Fellow of the Royal Society of Arts.

# *Foreword*

## ‘Everybody’s Business’: an introduction to the risk management universe

**Steve Fowler, CEO, Institute of  
Risk Management (IRM)**

Just what exactly is risk management? Until quite recently, the response to this apparently simple question would depend on who you asked: ask a safety expert and you’d get one interpretation; ask a banker and you’d get a completely different one. If you didn’t know otherwise, you’d assume these two interpretations came from different worlds. Increasingly, however, organizations are beginning to appreciate that these different worlds make up parts of the same universe – the risk management universe.

This book brings together insights into this universe from a range of leading commentators. Indeed, rarely has such a breadth of risk authors contributed to the same work. Whilst each paints a picture of risk management from their own viewpoint, a number of significant common themes come through time and again, the foremost amongst these being:

- uncertainty;
- opportunity;
- communication;
- complexity;
- leadership;
- skills.

Risk is not a finite science. Whilst mathematics can help us calculate probabilities, as David Hillson remarks in Chapter 1, we cannot know, understand, calculate or control everything. Risk is everywhere and derives directly from unpredictability. Risk management provides us with a framework for dealing with and reacting to such uncertainty. This is particularly important given the pace of change in life today. Ours is a world where product life cycles are typically measured in months not years and technological innovation makes whole industries, not just individual companies, obsolete almost overnight. In the space of less than 30 years, the main format used by the recorded music industry has moved from LP to cassette to CD to MP3 download: what will the next 30 years bring? To survive and thrive, organizations must keep one eye and an open and fertile imagination on the future through so-called ‘horizon scanning’, and at the same time learn from past experiences. Risk management provides an invaluable framework within which horizon scanning can be integrated into ‘business as normal’ activities. It’s a way of consciously thinking about change rather than just reacting to it, a theme raised by David Smith and Rob Politowski in Chapter 3. John Sharp echoes this in Chapter 5 with his comment that, with today’s faster speed of business, there is little time for gradual recovery when disaster strikes.

For businesses, taking risk is intrinsically linked to profit and value creation. ‘Who dares wins’ as the old adage goes. Richard Anderson gets this message over loud and clear in Chapter 2 and it is echoed again throughout the book. Proactive risk and opportunity management can be used by senior managers to drive performance: in such a context, compliance and governance are a by-product of risk management and not just primary drivers in their own respect. I particularly like Anderson’s idea of the ‘risk intelligent organization’. Such an organization optimizes future opportunity and current risk through the spread of good risk management practice.

Risk management also provides us with a common language for dealing with uncertainty, enabling professionals from different functions to better communicate with each other. At its most fundamental level, organizational and project failure is often driven by individuals speaking their own professional languages but failing to truly communicate: sales failing to communicate with production, and finance with IT for instance. Whilst each author writing in this book inevitably speaks from their own perspective, it is heartening to see an increasingly common ‘risk language’ also in use. This is echoed in the emergence of standards, mentioned throughout the text, and an area

in which my own organization, the Institute of Risk Management (IRM), is very active.

Risk management involves everyone and everything throughout an organization. Keith Blacker stresses this in Chapter 8 but again it is a common theme raised throughout the book. Whilst it is often relatively straightforward to identify and deal with pure risk in simple processes and systems, most of these do not stand alone and almost all require human interaction at some point. Reliance therefore on engineering solutions alone to minimize adverse risk will almost always fail: not only must the human element be considered, but the interactions between different systems in different functions are often so complex that in practice they can only be partly managed. In practice, the failure of such interactions is directly responsible for many well publicized risk failures. This in turn links back to my earlier point on the ‘ghettoization’ of professional languages and the opportunity this presents for the risk practitioner to step in to facilitate understanding between functions. This is an area where risk managers can add real value – through understanding, explaining and simplifying complexity, and consequently dealing with the sense of being overwhelmed that many directors feel.

A further sign of the growing maturity of risk as a field of study is the inclusion of many ‘softer’ non-engineering focused areas in this book, such as reputation, marketing and legal risk. Increasingly these regularly score highly in surveys of CEO risk attitudes, perhaps because failures in these areas are inexorably and directly linked to value destruction.

Effective approaches to risk management require strong and visible leadership. As a number of authors point out, without proactive leadership, risk management becomes a backroom function more concerned with technicalities, reporting and risk logs than with business development and performance. Risk management requires skills, not just in its technical execution but in creating the framework within which it can be exercised. Risk education organizations such as IRM have recognized the need for a broad range of education solutions. Consequently, programmes are now available to equip everyone from technical risk specialists up to CEOs with the risk skills they need.

In the future, risk specialists increasingly will need to become much more multi-skilled: able to understand and work with risk from the full range of perspectives discussed in this book. My own view is that only through such multi-skilling will risk management properly be recognized as a true vocation alongside accountancy, law, engineering

and the like. Risk, however, is also becoming a core part of general management education for all executives, whether in industry, commerce, public sector or charity.

Managing risk is something that everyone does. As Peter Bernstein (1996) comments in *Against the Gods: The Remarkable Story of Risk*, certainty is hugely seductive, and the history of mankind is the history of our attempts to transform uncertainty into risk. Acting effectively within a context where we understand risk will help differentiate tomorrow's winning organizations from those that will be less successful. In contrast, aiming for the elimination of all risk is like the quest for Eldorado: largely illusory and ultimately unfulfilling. The person that risks nothing, does nothing, has nothing, is nothing and will be nothing. To quote Baz Luhrmann's 1992 film 'Strictly Ballroom', 'A life lived in fear is a life half lived'. Through understanding and applying the range of insights, tools, skills and knowledge provided by this book, the reader will be better equipped for their exploration of the risk management universe.

## Reference

Bernstein, P L (1996) *Against the Gods – The Remarkable Story of Risk*. New York: John Wiley & Sons.

Editor's Note: The UK Government announced in November 2005 its intention to withdraw the requirement for full implementation of the proposed Operating and Financial Review (OFR). This announcement was made after the text for this book had been finalized. Consequently references to the OFR appear in Chapters 2, 3, 5, 6, 7, 11 and 13. We apologize for this small inaccuracy, which is the inevitable consequence of describing current conditions in a fast-changing environment.

DH

# *Surveying the Risk Management Universe – Where Are We Now?*

**David Hillson**

## **Risk in history**

The earliest records of human history and prehistory include stories of risk and its management. Historical documents, sacred writings, myths and legends – all tell tales of the human struggle against nature, the gods or the odds. Accounts of mankind’s earliest origins describe the urge to break boundaries, go beyond current confines, explore the unknown. Narratives describe risk-taking individuals ranging from Abraham, revered by three of the world’s great religions for his faith in leaving home and setting out to find a new country, through mythological heroes like Jason or Odysseus who undertook epic journeys, to modern entrepreneurs and innovators who change the lives of millions through ground-breaking discoveries and inventions. The broader sweep of human development has included risky phases as hunter-gatherers and agrarians, leading to the establishment of great civilizations like Egypt or the Mayans, to the present day.

Seen from a certain perspective, risk is everywhere. The world we inhabit is unpredictable, strange, incomprehensible, surprising, mysterious, awesome, different, other. This is true from the macro level of galaxies to the exotic nano-realm of subatomic particles, and everywhere in between. Irrefutable evidence forces people to accept the truth that we neither know nor understand everything, and we cannot control everything. Consequently, the word ‘risk’ has become a common and widely used part of today’s vocabulary, relating to

## 2 *The Risk Management Universe*

personal circumstances (health, pensions, insurance, investments, etc.), society (terrorism, economic performance, food safety, etc.) and business (corporate governance, strategy, business continuity, etc.).

And it seems that mankind has an insatiable desire to confront risk and attempt to manage it proactively. Many of the institutions of humanity could be viewed as frameworks constructed to address uncertainty, including politics, religion, philosophy, technology, laws, ethics and morality. Each of these tries to impose structure on the world as it is experienced, limiting variation where that is possible, and explaining residual uncertainty where control is not feasible. Sense-making appears to be an innate human faculty, seeking patterns in apparent randomness, applying a variety of templates or heuristics until a workable resolution is reached which allows an acceptable degree of comfort in the face of uncertainty.

As a result, not only is risk everywhere, but so is risk management. Just as the presence of risk is recognized and accepted as inevitable and unavoidable in every field of human endeavour, so there is a matching drive to address risk as far as possible. This has led to a proliferation of areas where the phrase ‘risk management’ is used to describe efforts to identify, understand and respond to risk, particularly in various aspects of business. Indeed it is possible to speak of a multidimensional ‘risk management universe’, with the word ‘universe’ derived from the Latin words *unus* (one) and *versum* (turn), describing a concept that combines all into one whole. Perhaps it is not too far-fetched to describe risk management as offering an integrative framework for understanding many parts of the human experience, if not all.

### **Risk in business**

In the world of business, risk management has a special place, being recognized as a management discipline in its own right, with a broad supporting infrastructure. Elements of this support include:

- *Academic base:* Many universities and educational establishments offer basic and advanced teaching in risk management, at degree, masters and doctoral levels, and both theoretical and applied research programmes are also available.
- *Professional bodies:* Many professional societies exist specifically to promote and support the discipline of risk management. Some of the most prominent are listed in Table 1.1.

**Table 1.1 Risk management professional bodies**

<i>Professional body</i>	<i>Web address</i>
ALARM – The National Forum for Risk Management In the Public Sector	<a href="http://www.ALARM-UK.org">www.ALARM-UK.org</a>
Association for Project Management Risk Management Specific Interest Group (APM Risk SIG)	<a href="http://www.APM.org.uk/RiskManagement/RiskProfile.asp">www.APM.org.uk/RiskManagement/RiskProfile.asp</a>
Association of Insurance and Risk Managers (AIRMIC)	<a href="http://www.AIRMIC.com">www.AIRMIC.com</a>
Business Continuity Institute (BCI)	<a href="http://www.theBCI.org">www.theBCI.org</a>
Engineering & Construction Risk Institute (ECRI)	<a href="http://ECRIonline.org">http://ECRIonline.org</a>
European Institute for Risk Management (EIRM)	<a href="http://www.EIRM.com">www.EIRM.com</a>
Federation of European Risk Management Associations (FERMA)	<a href="http://www.FERMA-asso.org">www.FERMA-asso.org</a>
Global Association of Risk Professionals (GARP)	<a href="http://www.GARP.com">www.GARP.com</a>
Institute of Risk Management (IRM)	<a href="http://www.theIRM.org">www.theIRM.org</a>
International Council on Systems Engineering Risk Management Working Group (INCOSE RMWG)	<a href="http://www.INCOSE.org/practice/techactivities/wg/risk">www.INCOSE.org/practice/techactivities/wg/risk</a>
Professional Risk Managers' International Association (PRMIA)	<a href="http://PRMIA.org">http://PRMIA.org</a>
Project Management Institute (PMI) Risk Management Specific Interest Group (PMI Risk SIG)	<a href="http://www.RiskSIG.com">www.RiskSIG.com</a>
Public Agency Risk Managers' Association (PARMA)	<a href="http://www.PARMA.com">www.PARMA.com</a>
Public Risk Management Association (PRIMA)	<a href="http://www.PRIMACentral.org">www.PRIMACentral.org</a>
Public Risk Management Organisation (PRIMO)	<a href="http://www.PRIMOEurope.org">www.PRIMOEurope.org</a>
Public Utilities Risk Management Association (PURMA)	<a href="http://www.PURMA.org">www.PURMA.org</a>
Risk & Insurance Management Society (RIMS)	<a href="http://www.RIMS.org">www.RIMS.org</a>
Risk Management Association (RMA)	<a href="http://www.RMAhq.org">www.RMAhq.org</a>
Risk Management Institution of Australasia (RMIA)	<a href="http://www.RMIA.org.au">www.RMIA.org.au</a>
Society for Risk Analysis (SRA)	<a href="http://www.SRA.org">www.SRA.org</a>

**Table 1.2 Risk management standards and guidelines**

<i>Reference/title</i>	<i>Standards body/publisher</i>	<i>Date</i>
AS/NZS 4360:2004, <i>Risk Management</i>	Standards Australia, Homebush NSW 2140, Australia, and Standards New Zealand, Wellington 6001, New Zealand.	2004
BS 25999-1:2006, <i>Business Continuity Management – Part 1: Code of Practice</i>	British Standards Institution, London, UK.	2006
BS 6079-3:2000, <i>Project Management – Part 3: Guide to the Management of Business-related Project Risk</i>	British Standards Institution, London, UK.	2000
BS 8444-3:1996 <i>Risk Management – Part 3: Guide to Risk Analysis of Technological Systems</i> (previously issued as IEC 300-3-9:1995)	British Standards Institution, London, UK.	1996
CAN/CSA-Q850-97 R2002, <i>Risk Management: Guideline for Decision-Makers</i>	Canadian Standards Association, Ontario, Canada.	2002
CP142, <i>Operational Risk Systems and Controls</i>	Financial Services Authority, London, UK.	2002
ISO/IEC FDIS 16085-2006, <i>Information Technology – Systems and Software Engineering – Lifecycle Processes – Risk Management</i> (previously issued as IEEE 1540-2001, <i>Standard for Software Life Cycle Processes – Risk Management</i> )	International Organization for Standardization, International Electrotechnical Commission, Geneva, Switzerland.	2006
ISO 14001:2004, <i>Environmental Management Systems – Requirements with Guidance for Use</i>	International Organization for Standardization, Geneva, Switzerland.	2004
ISO 14004:2004, <i>Environmental management systems – General Guidelines on Principles, Systems and Support Techniques</i>	International Organization for Standardization, Geneva, Switzerland.	2004
ISO/IEC 17799:2000, <i>Code of practice for Information Security Management</i>	International Organization for Standardization/International Electrotechnical Commission, Geneva, Switzerland.	2000
IEC 62198:2001, <i>Project Risk Management – Application Guidelines</i>	International Electrotechnical Commission, Geneva, Switzerland.	2001
JIS Q 2001:2001 (E), <i>Guidelines for Development and Implementation of Risk Management System</i>	Japanese Standards Association, Tokyo, Japan.	2001
NS 5814:1991, <i>Krav til risikoanalyse</i>	Norges Standardiseringsforbund (NSF).	1991

**Table 1.2 Risk management standards and guidelines (continued)**

<i>Reference/title</i>	<i>Standards body/publisher</i>	<i>Date</i>
PD 6668:2000, <i>Managing Risk for Corporate Governance</i>	British Standards Institution, London, UK.	2000
PD ISO/IEC Guide 73:2002, <i>Risk Management – Vocabulary – Guidelines for Use in Standards</i>	British Standards Institution, London, UK.	2002
<i>A Guide to the Project Management Body of Knowledge (PMBok®)</i> , Third Edition, Chapter 11 “Project Risk Management”	Project Management Institute, Philadelphia, US.	2004
<i>A Risk Management Standard</i>	Institute of Risk Management (IRM), Association of Insurance and Risk Managers (AIRMIC), and National Forum for Risk Management in the Public Sector (ALARM), London, UK	2002
<i>Continuous Risk Management Guidebook</i>	Software Engineering Institute (SEI), Carnegie Mellon University, USA	1996
<i>Enterprise Risk Management – Integrated Framework</i>	The Committee of Sponsoring Organizations of the Treadway Commission, USA	2004
<i>Guidelines for Environmental Risk Assessment and Management</i>	DETR, Environment Agency and IEH/The Stationery Office, London, UK.	2000
<i>Management of Risk – A Strategic Overview (The Orange Book)</i>	HM Treasury, London, UK	2001
<i>Management of Risk – Guidance for Practitioners</i>	UK Office of Government Commerce (OGC)/The Stationery Office, London, UK.	2002
<i>New Basel Capital Accord – Consultative Document</i>	Basel Committee on Banking Supervision, Switzerland	2001
<i>Project Risk Analysis &amp; Management (PRAM) Guide, (second edition)</i>	Association for Project Management/APM Publishing, High Wycombe, Bucks UK.	2004
<i>Risk Analysis and Management for Projects (RAMP, (second edition))</i>	Institution of Civil Engineers, Faculty of Actuaries and Institute of Actuaries Thomas Telford, London, UK.	2005
<i>Risk Management Guide for DoD Acquisition, 5th edn., Version 2</i>	US Department of Defense/ Defense Acquisition University, Defense Systems Management College. Published by DSMC Press, Fort Belvoir, VA, USA.	2003
<i>The Combined Code on Corporate Governance</i>	Financial Reporting Council, UK.	2003

## 6 *The Risk Management Universe*

- *Qualifications:* A range of examinations and qualifications are available for the risk professional, offered by academic institutions and professional bodies, though there is no clear consensus on a single certification which is recognized across all industries or countries.
- *Literature:* In addition to the wide range of national and international risk management standards and guidelines (see Table 1.2), there are a number of refereed journals covering the topic, as well as a huge variety of books on various aspects of risk.
- *Tools:* Software vendors offer a wide variety of tools to support all aspects of the risk process, as well as specialized tools for particular applications. There is also a growing market in enterprise risk management solutions, offering an integrated approach to managing risk across the organization. The current generation of risk tools have powerful functionality, good user interfaces and increasing integration capability.
- *Consultancies:* Solution providers also offer risk management support, allowing clients to benefit from their expertise and experience, and sharing best practice thinking and practical implementation.

Part of the recognition of risk management as an important management discipline has been the development of standards and guidelines which aim to capture and describe ‘best practice’. These are increasing in number, with some aiming to address risk management in its broadest sense while others have more limited scope. Some of the most widely used are listed in Table 1.2. The problem with having such a wide variety of ‘standards’ is the lack of ‘standardization’! The standard originally described a flag carried onto the battlefield to provide a rallying-point for the troops in the midst of the conflict. Having more than one standard in such circumstances would be a recipe for disaster. Yet in the professional arena it seems perfectly acceptable to have many standards in the same field, dividing the troops who rally to one or another, and leading to confusion and lack of focus.

### **Purpose and structure of this book**

There seems little doubt that risk management has been part of human activity for a very long time, and it is today a vital component of business. As a result, anyone asking the simple question ‘What is risk management?’ will not find a simple answer. Hence this book.

Even the most cursory exploration reveals a huge variety of differing perspectives, all claiming to represent the best way to address risk management. In fact risk management is not a single subject at all; it is a family of related topics. Application of risk processes has reached ever further across the boundaries of business. Risk management is not only practised formally in most industries, in many countries, and in both government and the private sector, but it also plays an important role at all levels in organizations. Types of risk management found in business today include:

- strategic risk management;
- corporate governance;
- financial risk management;
- business continuity and disaster recovery;
- reputational risk management;
- risk-assessed marketing;
- operational risk management;
- project risk management;
- environmental risk assessment;
- legal and contract risk management;
- technical risk management;
- fraud risk management;
- counter-terrorism risk management.

Even this long list is not exhaustive, as new and specialized applications are found in different areas of business. There are many common elements shared by these different types of risk management, but each has its own distinctive language, methodology, tools and techniques. They vary in scope from the broadest application to very specific areas of risk. They are at different levels of maturity, with some types of risk management being quite recent developments while others measure their history in decades. But each is important in its own way, representing part of the response of business to the uncertain environment within which it operates.

This book brings together leading experts from various risk management fields to share key insights into what makes their part of the risk management universe unique. While it would not be possible to include every aspect of risk management in all its diverse forms without making this a very large volume indeed, the main application areas found in most businesses are covered here. Each contributor describes current best practice in his area of expertise, as well as outlining areas for future

development. Following this unique guided tour of the main dimensions of the risk management universe, the book concludes with a final integrative discussion which attempts to draw the threads together, identifying underlying themes which unify all types of risk management, and setting the scene for new developments to maximize the effectiveness of risk management in all its diverse areas of application.

As a result, this book has something for everyone: business leaders who need to know where their risks are coming from and how they can be addressed; risk professionals seeking a broader and deeper understanding of their subject; lay people interested in developments of a key theme of our time; and teachers and students of business and management. All aspects of life have always been and still are risky, and this guided tour of the risk management universe provides essential insights into how to manage risk in business wherever it arises.

## References and recommended reading

- AS/NZS 4360:2004, *Risk management*. Homebush, Australia: Standards Australia; Wellington, New Zealand: Standards New Zealand.
- Association for Project Management (2004) *Project Risk Analysis & Management (PRAM) Guide* (second edition), High Wycombe, Bucks, UK: APM Publishing.
- Basel (2001) *New Basel Capital Accord – Consultative Document*. Basel: Basel Committee on Banking Supervision.
- Bernstein, P L (1996) *Against the Gods – the remarkable story of risk*. New York: J Wiley & Sons.
- BS 25999-1:2006, *Business Continuity Management – Part 1: Code of Practice*. London: British Standards Institution.
- BS 6079-3:2000, *Project Management – Part 3: Guide to the management of business-related project risk*. London: British Standards Institution.
- BS 8444-3:1996, *Risk Management – Guide to risk analysis of technological systems*. London: British Standards Institution.
- CAN/CSA-Q850-97 R2002, *Risk management: Guideline for decision-makers*. Ontario, Canada: Canadian Standards Association.
- COSO (2004) *Enterprise Risk Management – Integrated Framework*. Washington DC: The Committee of Sponsoring Organisations of the Treadway Commission.
- DETR, Environment Agency and IEH (2000) *Guidelines for Environmental Risk Assessment and Management*. London: The Stationery Office.
- Dorofee, A J *et al.* (1996) *Continuous Risk Management Guidebook*. Pittsburgh, PA: SEI Carnegie Mellon University.
- Financial Reporting Council (2003) *The Combined Code on Corporate Governance*. London: Financial Reporting Council.
- Financial Services Authority (2002) *CP142 Operational Risk Systems and Controls*. London: Financial Services Authority.

- Hillson, D A (2002) What is risk? Towards a common definition. *InfoRM (Institute of Risk Management)*, April, pages 11–12.
- HM Government Cabinet Office Strategy Unit (2002) *Risk: Improving government's capability to handle risk and uncertainty*. Report ref 254205/1102/D16. London: HM Government Cabinet Office Strategy Unit.
- HM Treasury (2001) *Management of Risk – A Strategic Overview (The Orange Book)*. London: The Stationery Office.
- IEC 62198:2001, *Project risk management – Application guidelines*. Geneva: International Electrotechnical Commission.
- IEEE 1540-2001, *Standard for Software Life Cycle Processes – Risk Management*. New York: The Institute of Electrical and Electronic Engineers.
- Institute of Risk Management (IRM), Association of Insurance and Risk Managers (AIRMIC), and National Forum for Risk Management in the Public Sector (ALARM) (2002) *A risk management standard*. London: IRM/ALARM/AIRMIC.
- Institution of Civil Engineers, Faculty of Actuaries and Institute of Actuaries (2005) *Risk Analysis & Management for Projects (RAMP)* (second edition). London: Thomas Telford.
- ISO 14001:2004, *Environmental management systems. Requirements with guidance for use*. Geneva: International Organisation for Standardisation.
- ISO 14004:2004, *Environmental management systems. General guidelines on principles, systems and support techniques*. Geneva: International Organization for Standardization.
- ISO/IEC FDIS 16085:2006, *Information technology – Systems and software engineering – Life cycle processes – Risk management*. Geneva: International Organisation for Standardisation/International Electrotechnical Commission.
- ISO/IEC 17799:2000, *Code of practice for information security management*. Geneva: International Organisation for Standardisation/International Electrotechnical Commission.
- JIS Q2001:2001(E), *Guidelines for development and implementation of risk management system*. Tokyo: Japanese Standards Association.
- NS5814:1991, *Krav til risikoanalyse*, Oslo: Norges Standardiseringsforbund (NSF).
- PAS 56:2003, *Guide to Business Continuity Management*. London: British Standards Institution.
- PD 6668:2000, *Managing risk for corporate governance*. London: British Standards Institution.
- PD ISO/IEC Guide 73:2002, *Risk management – Vocabulary – Guidelines for use in standards*. London: British Standards Institute.
- Project Management Institute (2004) *A Guide to the Project Management Body of Knowledge (PMBOK®)* (Third Edition). Philadelphia, PA: Project Management Institute.
- Raz, T & Hillson, D A (2005) A comparative review of risk management standards. *Risk Management: An International Journal*, 7:4 53–66.
- UK Office of Government Commerce (OGC) (2002) *Management of Risk – Guidance for Practitioners*. London: The Stationery Office.
- US Department of Defense (2003) *Risk Management Guide for DoD Acquisition* (Fifth edition, Version 2). Fort Belvoir, VA: Defense Systems Management College.

# *Strategic Risk Management*

**Richard Anderson**

## **Why risk management?**

No one can turn a profit unless they are taking risk. Equally, everyone intuitively knows that turning risk to positive organizational advantage is not easy. That is what makes risk a strategic issue. The risk management issues discussed here are equally applicable to smaller companies, not-for-profit organizations and public sector bodies as they are to large multinational groups.

Risk management is the optic through which senior managers are now able to drive better performance. Improved performance is being driven by more effective processes, closer collaboration with partners and better motivated people in a finely tuned organization. This is a contrary view to one held by many people who regard risk as negative and risk management as bureaucracy. Viewing risk as a strategic issue and risk management as a strategic tool can turn negative, energy-sapping, compliance-driven risk management programmes into performance-enhancing, energy-releasing, positive programmes.

Corporate governance is a theme of the time, whether it is Higgs and the Combined Code (Financial Reporting Council, 2003; Higgs, 2003), the Financial Services Authority's (FSA's) new principles for listed companies, the new Operating and Financial Review (OFR), the Sarbanes-Oxley Act of 2002 or activist shareholders. Risk management is at least a part of the response demanded by all of these corporate governance initiatives. This has fostered a negative perspective of risk management in many organizations. In sharp contrast the aim of strategic risk management should be to help managers to remove the downside bias of many risk programmes and to liberate energy around a positive risk management approach that enhances an organization's ability to achieve its legitimate objectives. Regulatory compliance