1

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 Historical documents, sacred writings, myths and legends – all tell tales of the human struggle against nature, the gods or the odds.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

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

Professional body	*Web address*
Association for Project Management Risk Management Specific Interest Group (APM Risk SIG)	http://www.eurolog.co.uk/APMRiskSIG
Association of Insurance and Risk Managers (AIRMIC)	http://www.AIRMIC.com
European Institute of Risk Management (EIRM)	http://www.EIRM.com
Federation of European Risk Management Associations (FERMA)	http://www.ferma-asso.org
Global Association of Risk Professionals (GARP)	http://www.GARP.com
Institute of Risk Management (IRM)	http://www.theIRM.org
International Association of Contract and Commercial Managers (IACCM) Business Risk Working Group	http://www.IACCM.com/risk.php
International Council on Systems Engineering Risk Management Working Group (INCOSE RMWG)	http://www.INCOSE.org
Professional Risk Managers' International Association (PRMIA)	http://prmia.org
Project Management Institute (PMI) Risk Management Specific Interest Group (PMI Risk SIG)	http://www.RiskSIG.com
Public Risk Management Association (PRIMA)	http://www.PRIMAcentral.org
Risk Management Association (RMA)	http://www.RMAhq.org
Risk Management Institution of Australasia (RMIA, formed by a merger of the Association of Risk & Insurance Managers of Australasia, ARIMA, with the Australasian Institute of Risk Management, AIRM)	http://www.rmia.org.au
Society for Risk Analysis (SRA)	http://www.sra.org

- *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),

Table 1.2 Risk management standards and guidelines

Reference/title	*Standards body/publisher*	*Date*
AS/NZS 4360:2004, *Risk Management*	Standards Australia, Homebush NSW 2140, Australia, and Standards New Zealand, Wellington 6001, New Zealand.	2004
BS 6079-3:2000, *Project Management – Part 3: Guide to the Management of Business-related Project Risk*	British Standards Institution, London, UK.	2000
BS 8444-3:1996 (previously issued as IEC 300-3-9:1995), *Risk Management – Part 3: Guide to Risk Analysis of Technological Systems*	British Standards Institution, London, UK.	1996
CAN/CSA-Q850-97, *Risk Management: Guideline for Decision Makers*	Canadian Standards Association, Ontario, Canada.	1997
CP142 Operational Risk Systems and Controls	Financial Services Authority, London, UK.	2002
IEEE 1540-2001, *Standard for Software Life Cycle Processes – Risk Management*	The Institute of Electrical and Electronic Engineers, Inc., USA.	2001
ISO 14001:2004, *Environmental Management Systems – Requirements with Guidance for Use*	International Organization for Standardization, Geneva, Switzerland.	2004
ISO 14004:2004, *Environmental Management Systems – General Guidelines on Principles, Systems and Support Techniques*	International Organization for Standardization, Geneva, Switzerland.	2004
ISO/IEC 17799:2005, *Information Technology – Security Techniques – Code of Practice for Information Security Management*	International Organization for Standardization/International Electrotechnical Commission, Geneva, Switzerland.	2005
IEC 62198:2001, *Project Risk Management – Application Guidelines*	International Electrotechnical Commission, Geneva, Switzerland.	2001
JIS Q 2001:2001 (E), *Guidelines for Development and Implementation of Risk Management System*	Japanese Standards Association, Tokyo, Japan.	2001
NS 5814:1991, *Krav til risikoanalyser*	Norges Standardiseringsforbund (NSF).	1991
PAS 56:2003, *Guide to Business Continuity Management*	British Standards Institution, London, UK.	2003
PD 6668:2000, *Managing Risk for Corporate Governance*	British Standards Institution, London, UK.	2000

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

Reference/title	*Standards body/publisher*	*Date*
PD ISO/IEC Guide 73:2002, *Risk Management – Vocabulary – Guidelines for Use in Standards*	British Standards Institution, London, UK.	2002
A Guide to the Project Management Body of Knowledge (PMBoK®), 3rd edn, ch. 11 'Project risk management'	Project Management Institute, Philadelphia, PA, USA.	2004
A Risk Management Standard	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
Continuous Risk Management Guidebook	Software Engineering Institute (SEI), Carnegie Mellon University, USA.	1996
Enterprise Risk Management – Integrated Framework	The Committee of Sponsoring Organizations of the Treadway Commission, USA.	2004
Guidelines for Environmental Risk Assessment and Management	DETR, Environment Agency and IEH/The Stationery Office, London, UK.	2000
Guidelines on Risk Issues	The Engineering Council, London, UK.	1995
Management of Risk – Guidance for Practitioners	UK Office of Government Commerce (OGC)/The Stationery Office, London, UK.	2002
New Basel Capital Accord – Consultative Document	Basel Committee on Banking Supervision, Switzerland.	2001
Project Risk Analysis & Management (PRAM) Guide, 2nd edn.	Association for Project Management/APM Publishing, High Wycombe, Bucks, UK.	2004
Risk Analysis and Management for Projects (RAMP) 2nd edn.	Institution of Civil Engineers, Faculty of Actuaries and Institute of Actuaries/Thomas Telford, London, UK.	2005
Risk Management – Concepts and Guidance	Defense Systems Management College, Fort Belvoir, VA, USA.	1989
Risk Management Guide for DoD Acquisition, 5th edn.	US Department of Defense/ Defense Acquisition University, Defense Systems Management College. Published by DSMC Press, Fort Belvoir, VA, USA.	2002
The Combined Code on Corporate Governance	Financial Reporting Council, UK.	2003

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: Standards New Zealand.

Association for Project Management (2004) *Project Risk Analysis & Management (PRAM) Guide*, 2nd edn. 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: John Wiley & Sons.

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 – Part 3: Guide to Risk Analysis of Technological Systems*. London: British Standards Institution.

CAN/CSA-Q850-97, *Risk Management: Guideline for Decision Makers*. Ontario, Canada: Canadian Standards Association.

COSO (2004) *Enterprise Risk Management – Integrated Framework*. Washington, DC: The Committee of Sponsoring Organizations of the Treadway Commission.

Defense Systems Management College (1989) *Risk Management – Concepts and Guidance*. Fort Belvoir, VA: Defense Systems Management College.

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.

The Engineering Council (1995) *Guidelines on Risk Issues*. London: The Engineering Council.

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, J. UK Inst. Risk Mngmnt.*, April, pp 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.

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/AIRMIC/ALARM.

Institution of Civil Engineers, Faculty of Actuaries and Institute of Actuaries (2005) *Risk Analysis and Management for Projects (RAMP)*, 2nd edn. London: Thomas Telford.

ISO 14001:2004, *Environmental Management Systems – Requirements with Guidance for Use*. Geneva: International Organization for Standardization.

ISO 14004:2004, *Environmental Management Systems – General Guidelines on Principles, Systems and Support Techniques*. Geneva: International Organization for Standardization.

ISO/IEC 17799:2005, *Information Technology – Security Techniques – Code of Practice for Information Security Management*. Geneva: International Organization for Standardization/International Electrotechnical Commission.

JIS Q 2001:2001 (E), *Guidelines for Development and Implementation of Risk Management System*. Tokyo: Japanese Standards Association.

NS 5814:1991, *Krav til risikoanalyser*. 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 Institution.

Project Management Institute (2004) *A Guide to the Project Management Body of Knowledge (PMBoK®)*, 3rd edn. Philadelphia, PA: Project Management Institute.

Raz, T and 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 (2002) *Risk Management Guide for DoD Acquisition*, 5th edn. Fort Belvoir, VA: Defense Systems Management College.