Best Management Practice

Management of Risk: Guidance for Practitioners and the international standard on risk management, ISO 31000:2009

Michael Dallas, Director, APM Group Ltd

bsi.

White Paper
April 2013

Contents

1 Introduction

The purpose of this White Paper

This White Paper is intended to show how *Management of Risk: Guidance for Practitioners* (M_o_R®)[1] can be used to help organizations ensure their risk management approach meets the requirements of ISO 31000:2009: *Risk Management – Principles and Guidelines*.[2]

Why standards help improve risk management effectiveness

Standards can improve the effectiveness of risk management by providing generic guidelines and drawing attention to the key principles and activities required. This happens in two ways:

- The content of ISO 31000 forms a checklist against which an organization can assess the completeness of its own approaches in terms of both principles and activities. This leads to fewer organizations missing vital activities that national (or international) consensus deems necessary for the effective management of risk.
- Effective management relies on good communications and these, in turn, rely on the use of a consistent vocabulary. By standardizing the use of words in a particular context, people are able to work together more easily and with fewer misunderstandings. *ISO Guide 73:2009*[3] provides a risk management vocabulary.
- Once standards have been established, they can promote continuous improvement by being periodically reviewed and updated. This ensures the latest consensus on best practice is included and any omissions or clarifications dealt with. In this way all users of standards benefit from the collective experience of all other users.

A comparison of both publications

M_o_R was first published in 2002 and has since undergone two revisions to reflect comments received from users and changes in management methods. It is broadly consistent with the principles and guidelines in ISO 31000 (but with some differences) as summarized here:

- M_o_R is designed for practical use and provides much more detailed guidance on how to implement risk management. Consequently it is some six times longer than the standard. ISO 31000 provides principles and generic guidelines on harmonizing standards and introducing risk management within an organization or for an activity.
- Both documents see risk management as a fundamental requirement to help organizations deliver their objectives.
- There are no significant areas of disagreement between the two publications in the overall approach and processes for risk management.
- Terminology is provided in both publications, but differs. A comparative table is provided in Appendix A.
- Whereas M_o_R provides the basis for qualifications in the management of risk, ISO 31000 does not.

ISO 31000

Standards seek to provide their readers with a concise summary of the topic covered. ISO 31000 summarizes the key concepts and activities that an organization needs to undertake in order to manage risk effectively, and thus increase its chances of achieving its objectives, comply with relevant legal and regulatory requirements and respond to arising opportunities and threats. It does not define any particular techniques to be used but stresses that the organization should apply risk identification tools and techniques that are suited to its objectives. Another ISO publication, ISO/IEC 31010, *Risk Management – Risk Assessment Techniques,*[4] does include details of some risk assessment techniques. Risk assessment provides an understanding of risks that could affect an organization's achievement of its objectives and the adequacy and effectiveness of controls already in place. ISO/IEC 31010 provides a basis for decisions to be made about which approach to use to treat particular risks and to select the best options. By contrast, M_o_R contains an extensive appendix devoted to the description of commonly used techniques.

ISO 31000 provides a set of principles to inform a framework within which an organization can manage risk and a process by which it can do this. It is not intended to promote uniformity of risk management throughout all organizations, as each should customize its approach to address its particular objectives and operational needs. However, legislation in certain countries may require organizations to comply with ISO 31000. In this respect it is comforting that M_o_R is compliant with ISO 31000.

The international standard ISO 31000 covers the key concepts and activities for managing risk and is intended to harmonize risk management processes in existing and future standards. It sets out the guidelines for implementing effective risk management in an organization. As its title implies, M_o_R provides guidance for practitioners on managing risk, embedding good risk management practice and improving maturity in its application; something which is also recommended in ISO 31000.

The different purposes served by both publications

Rather than reflecting inconsistencies, the differences between ISO 31000 and M_o_R referred to in the preceding paragraph highlight the fact that each document is designed to serve a different purpose. In simple terms:

- ISO 31000 defines *what* needs to be done and by whom, but not *how* activities are done.
- M_o_R describes both *what* needs to be done, through a set of principles, activities and roles, and *how* to undertake the activities.

As such:

- M_o_R is designed for practical application of risk management methods.
- ISO 31000 is designed to help assess how completely the risk management method has been applied.

Although it is designed for practical use, M_o_R does not prescribe how an organization should implement risk management but allows it to customize its approach within the guidelines to suit its operating environment and processes. In this respect it serves a similar purpose to ISO 31000.

Compatibility with BS 31100:2008

One of the quality criteria for the 2010 revision of M_o_R was that the guidance must be compatible with BS 31100:2008, the standard that was in place at the time.

This White Paper shows the relationship between M_o_R and ISO 31000. The ISO 31000 principles are identified by a letter notation that was adopted in BS 31100:2011, *Risk Management. Code of Practice and Guidance for the Implementation of BS ISO 31000.*[5]

The comparison of M_o_R principles with ISO 31000 also holds for a comparison of the principles of M_o_R with those in BS 31100:2011, which has replaced BS 31100:2008. The BS 31100:2011 principles are not repeated here as this would be an unnecessary duplication.

2 Section-by-section comparison

Appendix B provides a tabular comparison of the two publications. The summary in this section seeks to emphasize the similarities as much as the differences between them. M_o_R is longer and much more detailed; however, the main components are very similar. We have structured the comparison in seven parts, reflecting the contents of M_o_R: introduction; structure; principles; approach (M_o_R) and framework (ISO 31000); embed and review; perspectives; and miscellaneous.

Introduction

In their introductions both publications outline their intended audiences. The main difference is that M_o_R is aimed at those responsible for implementing and overseeing risk management practice, while the standard is aimed at those responsible for developing policy, ensuring risks are effectively managed, assessing its effectiveness and setting up the organizational standards.

Both documents see effective risk management as being very relevant to the achievement of an organization's objectives and describe consistent approaches to managing risk.

M_o_R defines risk as 'an uncertain event or set of events that, should it occur, will have an effect (positive or negative) on the achievement of objectives'. ISO 31000's definition is similar and defines risk as 'effect of uncertainty on objectives'.

While both publications list similar benefits of risk management in an organization, the emphasis within M_o_R is on how it contributes to corporate governance and internal control. Only M_o_R is designed to underpin qualifications in risk management.

Structure

Although superficially different, the main components of each publication are very similar. M_o_R is based on four core concepts – principles; approach; process; and embedding and review – while ISO 31000 describes principles, a framework and a process.

M_o_R supplements the above core concepts with sections on perspectives, covering application at strategic, programme, project and operational levels, together with document outlines, techniques, a health check and maturity mode. While the standard acknowledges some of these aspects, it provides no detail.

Principles

The third edition of M_o_R reduces the number of principles from twelve to eight. These are informed by corporate governance principles and ISO 31000. It is hardly surprising, therefore, that there is a strong alignment between the two. While M_o_R states that they are essential for the maintenance of good practice, ISO 31000 simply emphasizes that they should be adhered to. One area of difference is that M_o_R includes the principle of creating a supportive culture within the organization. ISO 31000 emphasizes the need for such a culture but does not include it as one of the principles.

Approach (M_o_R) and framework (ISO 31000)

These sections describe how the principles should be applied within an organization and cover similar ground, although they use different terms. For example, whereas M_o_R uses the term 'risk register', ISO 31000 speaks of keeping records without specifying what form these records should take.

Both publications describe setting up a policy aligned with the organization's objectives, activities that should be undertaken, creating and maintaining records and monitoring and reporting progress. ISO 31000 includes the need for continuous improvement, which in M_o_R is dealt with in a separate section. M_o_R includes the need for a plan to embed risk management in the culture of the organization.

Process

The process for managing risk is essentially the same in both publications, consisting of identification, assessment, treatment, monitoring and review. Since M_o_R is designed

to guide the practitioner, its coverage of the process is more detailed than that of ISO 31000. It comprises four key stages – identify, assess, plan and implement – all underpinned by effective communication.

Embed and review

Both documents stress the need to embed risk management into the organization's management processes. However, M_o_R places greater emphasis on integrating it into the culture of the organization; in fact it devotes a specific chapter to this subject. While the need to do so is acknowledged within ISO 31000, the requisite steps are only outlined under various headings, particularly within 'framework'.

Perspectives

ISO 31000 refers to the application of risk management throughout the life of an organization and across a wide range of activities, strategies and decisions, operations, processes, functions, projects, services and assets. M_o_R devotes an entire chapter to how risk management may be applied at strategic, programme, project and operational levels. For more detail, please refer to Appendix A.

Miscellaneous

M_o_R contains appendices giving outlines of commonly used documents and techniques and a process for assessing how well risk management is used in an organization. It describes a suggested maturity model to measure the current level of risk management maturity and to identify areas for improvement. ISO 31000 refers to the need for these things but provides little in the way of detail or method.

Both publications contain glossaries explaining the meaning of the terms used but these are different in each one. A comparative table is included in Appendix A.

3 How M_o_R meets ISO 31000

This section summarizes how M_o_R meets the requirements of the International Standard. Because M_o_R and ISO 31000 have a different structure and purpose, clause-by-clause comparisons are inappropriate. Appendix B contains a detailed comparison.

The main points of consistency are:

- Risk management is very relevant to the achievement of an organization's objectives
- They share consistent principles
- They recommend a similar approach to the application of risk management
- They promote the use of similar risk management processes
- They encourage the integration within the organization's culture and management processes
- They both emphasize risk management application throughout the life of an organization and its activities.

Thus it may be concluded that if an organization is using M_o_R it meets the requirements of ISO 31000 and, indeed, exceeds them in that it provides much of the detail and method that is not covered in the standard.

4 Key areas of similarity and difference

M_o_R is designed as a guide for practitioners in risk management. Its use enables an organization to comply with the requirements of ISO 31000 in full.

ISO 31000 is intended to set out the principles and generic guidelines for organizations to manage risk; it does not prescribe which tools and techniques to use. It does aim, however, to enable organizations to harmonize risk management processes in existing and future standards.

Figure 1 outlines the main areas of overlap between M_o_R and ISO 31000. Both publications contain the same scope of principles, processes and approaches to managing risk. Both state similar aims for risk management and contain compatible terms (area A).

As a guide to practitioners, M_o_R contains descriptions of commonly used techniques and explains how the approach and processes are used at strategic, programme, project and operational levels. It provides the basis for Foundation and Practitioner qualifications (area B). ISO 31000, on the other hand, specifically states that it is not intended for the purpose of certification.

ISO 31000 outlines a rather broader range of areas of application for the management of risk across an organization and suggests its use throughout the life of the organization (as distinct from that of a programme or project). It also sets out what is needed for compliance with legal and regulatory requirements and international norms (area C).

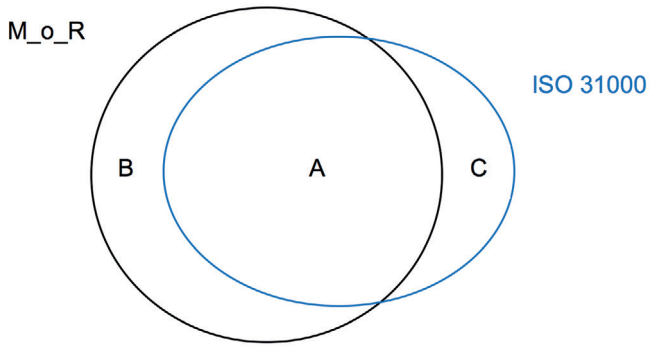

Figure 1 Key areas of similarity and difference between M_o_R and ISO 31000

Appendix A Comparative glossary

Terminology differs in some respects between M_o_R and ISO 31000 but each publication includes equivalent terms. The table below provides a comparison of Section 2 of ISO 31000 (terms and definitions) with the equivalent terms in M_o_R. The M_o_R glossary is more extensive than the one in ISO 31000.

M_o_R term	ISO 31000 term
Same terms used in both publications	
Residual risk	Residual risk
Risk	Risk
Risk evaluation	Risk evaluation
Risk identification	Risk identification
Risk management	Risk management
Risk management policy	Risk management policy
Risk owner	Risk owner
Risk profile	Risk profile
Stakeholder	Stakeholder
Different terms used in each publication	
Broadly covered by 'approach'	Risk management framework
Communications plan describes the process	Communication and consultation
Included in 'embed and review'	Review
Covered by 'identify context'	External context
Covered by 'identify context'	Internal context
Covered by 'identify context'	Risk criteria
Identify context	Establishing the context
Impact or risk effect	Consequence
Implement	Risk treatment
Included in 'implement'	Monitoring
Probability	Likelihood
Risk appetite	Risk attitude
Risk cause	Risk source
Risk estimation	Risk analysis
Risk event	Event
Covered by 'risk identification', 'estimation' and 'evaluation'	Risk assessment
Risk management process guide describes the process	Risk management process
Risk management strategy	Risk management plan
Risk response. See also 'implement'	Control
Severity of risk	Level of risk

Appendix B Map of M_o_R against ISO 31000

The table below provides a direct comparison of M_o_R with ISO 31000 against categories that are common to both publications.

Category	M_o_R	ISO 31000
Introduction	Organization-focused, covering four perspectives (strategic, programme, project and operational), relevant to both the public and private sectors.	Organization- and activity-focused, relevant to any public, private or community enterprise, group or individual.
	Audience includes people who are: ■ Responsible for putting in place a risk management framework ■ Responsible for reviewing and improving risk management ■ Managing risk within one of the four perspectives ■ Responsible for risk management guidance.	Audience includes people who are: ■ Responsible for developing risk management policy ■ Accountable for ensuring risk is managed ■ Evaluating the effectiveness in managing risk ■ Engaged in developing standards, guides, procedures, etc.
	Provides a route map for undertaking risk management in a repeatable and consistent manner, bringing together principles, an approach and a process.	Describes a generic approach for managing any sort of risk in any context, linking together principles, a framework and a process.
	Defines risk as 'an uncertain event or set of events that, should it occur, will have an effect (positive or negative) on the achievement of objectives'.	Defines risk as 'effect of uncertainty on objectives'.
	Lists main benefits but also emphasizes the contribution made to corporate governance and internal control.	Lists just the main benefits.
	Part of Cabinet Office Best Management Practice Guidance portfolio.	An International Organization for Standardization publication.
	Basis for APMG Certification.	Not intended for certification.
Summary	**While each document has a different approach to its introduction, they are not contradictory but see effective risk management as being very relevant to the achievement of an organization's objectives.**	

Structure	Based on four core concepts: **M_o_R principles** ■ Eight universal, self-validating and empowering principles that provide a guide to effective risk management **M_o_R approach** ■ The way in which the principles may be implemented. This should be customized for the organization **M_o_R process** ■ Describes the four primary steps of identify, assess, plan and implement, plus the communicate activity **Embedding and reviewing M_o_R** ■ Guidance on the need to integrate risk management into the organization's culture and how to do this The above is supplemented by chapters/appendices on: **Perspectives** ■ Describes how the principles, approach and process are applied at strategic, programme, project and operational levels **Document outlines** ■ Typical contents for key risk management documents **Common techniques** ■ Overviews of a selection of techniques that may be used and guidance on which to select **Health check** ■ How to check the current health of application in an organization and identify where it might be improved **Maturity model** ■ A format for benchmarking an organization's current capability and maturity in risk management and how to improve areas to increase maturity levels.	Based on three main clauses: **Principles** ■ Eleven principles that an organization should comply with for risk management to be effective **Framework** ■ Provides the foundations and arrangements that will embed risk management in the organization **Process** ■ Describes the five activities of communication and consultation; establishing the context; risk assessment; risk treatment; and monitoring and review The standard is silent on the supplements to the framework provided within M_o_R.
Summary	**The main components of each document are very similar, with the ISO 31000 framework being addressed by M_o_R's approach and embedding, and reviewing M_o_R. However, M_o_R provides more depth of coverage, comprising 145 pages, compared with the 24 pages of ISO 31000.**	

Principles	Essential for the development and maintenance of good risk management practice. Informed by corporate governance principles and ISO 31000.	Organizations should comply with these principles for risk management to be effective. Prefix letters indicate those used in ISO 31000 (placed in same order as the M_o_R principles to which they relate).
	Aligns with objectives ■ Focuses on those uncertainties that have the potential to impact the achievement of an organization's objectives	d) Explicitly addresses uncertainty ■ Its nature and how it may be addressed ■ Aligns with M_o_R's objectives
	Fits the context ■ Bespoke design of the risk management approach to match the organization's context	g) Tailored ■ Aligns with external and internal context and risk profile j) Dynamic, iterative and responsive to change ■ Is revised to take account of changes in context g) and j) align with M_o_R's fits the context
	Engages stakeholders ■ To understand their requirements and perceptions of risk, and to influence their contribution	i) Transparent and inclusive ■ Involves stakeholders at all levels h) Takes account of human and cultural factors ■ People, external or internal can affect achievement of objectives i) and h) align with M_o_R's 'engages stakeholders'
	Provides clear guidance ■ All stakeholders understand how the organization identifies, assesses and controls risk	b) An integral part of all organizational processes ■ Not a stand-alone activity e) Systematic, structured and timely ■ Leading to efficiency and consistent, comparable and reliable results b)and e) align partially with M_o_R's 'provides clear guidance' principle
	Informs decision-making ■ Helps decision-makers understand the relative merits, threats and opportunities related to their decisions	c) Part of decision-making ■ Helps decision-makers make informed choices ■ Aligns with M_o_R's 'informs decision-making'

	Facilitates continual improvement ■ Uses historical data to inform estimates, risk responses, forecasts and decisions	k) Facilitates continual improvement ■ Organizations should develop and improve their maturity f) Based on best available information ■ Some factual, some may be uncertain or require judgement k) and f) align with M_o_R's 'facilitates continual improvement'
	Creates a supportive culture ■ A culture that recognizes uncertainty and supports considered risk-taking	■ None of the ISO 31000 principles align to M_o_R's 'creates a supportive culture'
	Achieves measurable value ■ Using a structured approach to risk management creates and protects organizational value.	a) Creates and protects value ■ Contributes to achievement of objectives and improved performance ■ Aligns with M_o_R's 'achieves measurable value'.
Summary	**The ISO 31000 principles have been reordered to demonstrate an approximate alignment between the two documents. There is good alignment over most of the principles, although ISO 31000 is far less detailed.**	
Approach (M_o_R) and framework (ISO 31000)	The way in which the principles should be applied in the organization. **Risk management policy** ■ How risk management will be implemented throughout an organization to support the realization of its objectives	Underpins successful management of risk. **Mandate and commitment** ■ Define policy, align with culture, determine performance indicators ■ Align with organizational objectives ■ Legal and regulatory compliance **Design of framework for managing risk** ■ Understanding the organization and its context ■ Establishing a policy ■ Ensure accountability ■ Integrate into other processes ■ Allocate appropriate resources ■ Establish internal and external communications and reporting

	Risk management process guide ■ Describes how the M_o_R process steps will be carried out in the organization **Risk management strategies** ■ Describes the specific risk management activities that will be undertaken for a particular organizational activity	**Implementing risk management** ■ Implement framework ■ Implement processes **Monitoring and review of framework** ■ Ensure effectiveness and continuity in support of organization performance **Continual improvement of framework** ■ Decide how to improve framework, policy and plan
	Records and documentation **Risk register** ■ Captures and maintains information on all identified threats and opportunities relating to a specific organizational activity **Issue register** ■ Captures and maintains information on all identified issues that are happening now and require action **Risk improvement plan** ■ Assists with embedding risk management into the culture of the organization **Risk communications plan** ■ Describes how information will be disseminated to and received from stakeholders of an organizational activity **Risk response plan** ■ Detail specific plans for responding to a single risk or linked set of risks **Risk progress report** ■ Provides regular progress information on risk management within a particular organizational activity.	Process guidance including keeping records (ISO does not use the term 'risk register' or 'issue log') are contained under 'process' below.
Summary	**The ground covered under M_o_R's 'approach' is dealt with by the 'frameworks' and other clauses in ISO 31000 and in much less detail.**	

Process	Describes the management of risk process steps. Provides a comparison with HM Treasury's *Orange Book*.[6] The key process steps described are:	Outlines main process steps, stressing that these should be integrated in management, embedded in the culture and tailored to suit the organization. Similar to the processes described in M_o_R but less detail.
	Communication throughout the process ■ An activity that is carried out throughout the whole process. Key to the identification of new risks of changes to existing risks	**Communication and consultation** ■ With external and internal stakeholders at all stages of the process
	Identify context ■ Understand how the planned activity fits into the wider organization and market/society and the organization's approach to risk management, in order to shape the risk management strategy	**Establishing the context** ■ Articulates its objectives, defines parameters to take into account when managing risk and sets the scope of the process itself
	Identify risks ■ Identify risks to the activity objectives with the aim of minimizing threats while maximizing opportunities **Assess – estimate** ■ Prioritize individual risks so that it is clear which are most important and urgent by understanding the probability, impact and proximity of each risk **Assess – evaluate** ■ Understand the risk exposure faced by the activity by looking at the net effect of identified threats and opportunities on an activity when aggregated together	**Assessment** ■ Includes identification, analysis and evaluation of risks ■ Identification generates a comprehensive list of risks ■ Analysis to understand causes and sources of risks, their consequences and their likelihood of occurring ■ Evaluate to assist decision-making by comparing with criteria, to determine how to treat risk if at all
	Plan ■ Prepare specific management responses to remove or reduce threats and to maximize opportunities. Pre-empt surprises **Implement** ■ Ensure that the planned risk management actions are implemented and monitored and to take corrective action where responses do not match expectations	**Treatment** ■ Selecting and implementing options for modifying risks ■ Take account of costs and efforts against benefits ■ Develop and implement plans **Monitoring and review** ■ Part of plan. Assessing effectiveness, obtaining new information, identifying new risks
	See details of documentation under M_o_R 'approach' in previous section.	Recording the process to provide traceability and basis for improvement.
Summary	**ISO 31000 covers very similar ground to M_o_R but in less detail. Both publications include helpful figures showing the relationship between the key process steps.**	

Embed and review	Integrating risk management into the organization's culture, including regular reviews to ensure effective management. **Embedding the principles** ■ Start with the principles and by appreciating what the organization would look and feel like should these be embedded **Changing the culture for risk management** ■ The M_o_R approach needs to be understood, valued, implemented and improved by staff across the organization **Measuring the value** ■ Using a range of indictors to judge the success of building a risk management culture **Overcoming the common barriers to success** ■ By regular communications and by obtaining and developing senior management commitment and support **Identifying and establishing the opportunities for change** ■ Using trigger points to establish a continual cycle of monitoring, review and update/improvement.	The need to integrate risk management into the organization's management processes, align it with the organization's objectives and culture and provide appropriate resources and management support are referred to within Clause 4, Framework. There are also references under ■ Introduction: implicit references to the need to integrate risk management ■ Principles: integral part of all organizational processes, part of decision-making ■ Process: an integral part of management, embedded in culture and practice, tailored to the business ■ Establishing the context as an activity at the start of the risk management process ■ Annex A: Attributes of enhanced risk management.
Summary	**M_o_R devotes a specific chapter to integrating risk management into the organization. While the need to do so is acknowledged within ISO 31000, the requisite steps are only outlined under various headings, particularly within 'framework'.**	

Perspectives	Describes how the principles, approach and process are applied at the strategic, programme, project and operational perspectives. **Strategic** ■ Ensuring overall business success, vitality and viability **Programme** ■ Transforming business strategy into new ways of working that deliver measurable benefits to the organization **Project** ■ Delivering defined outputs to an appropriate level of quality with agreed scope, time and cost constraints **Operational** ■ Maintaining appropriate levels of business services to existing and new customers.	Refers to the application of risk management throughout the life of an organization and across a wide range of activities, strategies and decisions, operations, processes, functions, projects, services and assets (Section 1, Scope). Also refers to application at differing levels implicitly under ■ Section 5.3, Establishing the context ■ Annex A, Attributes of enhanced risk management.
Summary	**M_o_R contains a much more detailed analysis of the difference in approach from the different management perspectives. ISO 31000 merely acknowledges that risk management may be used at all these levels and more.**	
A. Document outlines	Suggested outlines of commonly used risk management documents.	Refers to the need for documentation but provides no details.
B. Common techniques	Outline descriptions of commonly used techniques for each step of the M_o_R process.	Refers to the need for specific techniques but provides no details.
C. Health check	Describes a process and framework for assessing how well risk management is used in an organization. The framework is based on the M_o_R principles.	Refers to the need to continually improve but does not provide a method.
D. Maturity model	Describes a suggested maturity model to measure the current level of risk management maturity and to identify areas for improvement. Also refers to other maturity models and provides a high-level description of the Portfolio, Programme and Project Management Maturity Model (P3M3).	Annex A, Attributes of enhanced risk management, refers to developing an appropriate level of performance in risk management. The attributes described are: ■ Continual improvement through setting of performance goals ■ Full accountability for those involved ■ Application in all decision-making ■ Continual communications ■ Full integration in the organization's governance structure.
E. Risk specialisms	Provides introductions to specialist areas of risk management and references to additional information on them.	Section 3, Principles a) to c) require an organization to apply risk management across all its activities. Annex A refers to full integration in the organization's governance structure. These requirements would include the specialist areas in Appendix E of M_o_R.
Summary	**While the need to improve organizational performance is acknowledged in ISO 31000, no mechanism is proposed for doing so. M_o_R, on the other hand, provides a template for a maturity model that can be customized to the needs of the organization.**	

	M_o_R identifies the following eight risk specialisms and directs the reader to more detailed information on these: ■ Business continuity management ■ Incident and crisis management ■ Health and safety management ■ Security risk management ■ Financial risk management ■ Environmental risk management ■ Reputational risk management ■ Contract risk management.	Although application in these specialist areas is implicit in the way the document is drafted, no specific guidance is provided.
Summary	**Once again, M_o_R provides guidance for good practice in these areas whereas ISO 31000 does not.**	
Glossary	Commonly used terms consistent with the Best Management Practice glossary	Terms and definitions provided. These differ from M_o_R. Some common terms such as 'risk register' are not used
Index	Alphabetical index to key terms and topics	Contents list by topic

References

1 *Management of Risk: Guidance for Practitioners*, third edition. Office of Government Commerce. The Stationery Office, 2010.

2 ISO 31000:2009, *Risk Management – Principles and Guidelines*. International Organization for Standardization, 2009.

3 ISO Guide 73:2009, *Risk Management – Vocabulary.* International Organization for Standardization, 2009

4 ISO/IEC 31010:2009, *Risk Management – Risk Assessment Techniques.* International Organization for Standardization, 2009.

5 BS 31100:2011, *Risk management. Code of Practice and Guidance for the Implementation of BS ISO 31000.* British Standards Institution, 2011.

6 *The Orange Book. Management of Risk – Principles and Concepts.* HM Treasury, 2004.

7 *Best Management Practice Portfolio: Common Glossary of Terms and Definitions.* Best Management Practice, 2012. Available at http://www.best-management-practice.com/gempdf/BMP_Common_Glossary_2012.pdf

Acknowledgements

Sourced by TSO and published on www.best-management-practice.com

Trade marks and statements