

A Comparative Review of Risk Management Standards

Tzyi Raz and David Hillson¹

We present and compare nine major standards for risk management, in terms of their scope, process steps and specific emphasis. We discuss their commonalities and differences, point out how they complement each other, and draw conclusions for future standards work in the risk management area.

Introduction

During the last decade there has been a major surge of interest in improving our ability to deal with uncertainty, and especially with its negative impact at the organisation level. This has led to the development and application of tools, techniques, processes and methodologies which are typically classified under the label of 'risk management'. It is important to distinguish between the management of business risks—a sub-specialty area in the fields of finance and insurance, mainly concerned with monetary gains and losses—and the management of operational risks, which is concerned with the uncertainty inherent in the execution of the activities that organisations do in order to fulfil their goals and objectives. The origins of operational risk management can be traced to the discipline of safety engineering, which is mainly concerned with the physical harm that may occur as a result of improper equipment or operator performance. However, modern risk management has evolved substantially from there, due to a number of factors, including:

- the shift away from dangerous physical work and towards knowledge-intensive work;
- an expanded view of the organisation in the context of its various stakeholders;
- the growing importance of projects as the framework for planning and executing work in organisations;
- the central role of technology, and its inherent uncertainty;
- ever-increasing competitive pressures to shorten lead times, causing organisations to start planning and executing their activities with incomplete information;
- increasing turbulence in the business environment;
- the rapid increase in the degree of complexity embodied in business and projects;
- the continuing trend towards globalisation, and the resulting emphasis on virtual business and teams; and
- the increasing burden of regulation with which businesses must comply.

All these, and possibly other factors as well, have resulted in growing numbers of books, articles and conferences being devoted to operational risk management. In fact, the field has grown to the point where the qualifier 'operational' is no longer needed, and the meaning of risk management as distinct from financial or business risk management is clear. This level of activity has also led to the development of a number of standards that prescribe for and advise organisations on the best way to manage their risks.

The purpose of this paper is to present and compare the main standards for risk management that are currently available today, extending earlier work on project risk management standards (Hillson, 2002; 2003). The main part of the paper consists of a series of tables that present the contents of the standards in a manner that facilitates their comparison. This is followed by a discussion regarding the commonalities among the standards and some thoughts regarding the need for additional work in the area.

Comparison of the standards

Table 1 lists the nine standards that were selected from a comprehensive survey, carried out with the help of the librarian of the Standards Institute of Israel. The nine standards selected consist of six national or international standards that were developed or adopted by standardisation bodies, and three standards that were developed by professional organisations with an interest in risk management. They were all published recently, the earliest publication date being 1997.

In addition to bibliographic information, Table 1 also indicates the scope of each standard. We distinguish between two levels of standard scope: project and organisation. The distinction is based on whether the standard states that the process, steps and procedures it contains are meant to be implemented at the project level, or by the entire organisation; this includes organisations that are not specifically engaged in project work. In general, it was easy to classify the standards according to their scope, with the exception of IEEE Standard 1540-2001: *Standard for Software Life Cycle Processes – Risk Management* (Institute of Electrical and Electronic Engineers, 2001) which states in its introduction that 'The risk management process defined in this standard can be adapted for use at an organization level or project level' (p iii).

A number of other standards were considered for inclusion in this review, but were eventually excluded due to their limited or specific scope of application.

The first risk-related standard ever published was Norsk Standard NS5814:1991: *Krav til risikoanalyser* (Norges Standardiseringsforbund, 1991), but this only addresses risk analysis and does not cover other portions of the risk assessment or risk management processes. The same is true of CEI/IEC 300-3-9:1995: *Dependability Management, Part 3: Application Guide – Section 9: Risk Analysis of Technological Systems* (International Electrotechnical Commission, 1995). BSI PD 6668:2000: *Managing Risk for Corporate Governance* (British Standards Institute, 2000b) is limited to addressing the risk elements of corporate governance requirements. Finally, the *Risk Management Guide for DoD Acquisition* (US Department of Defense, 2002) was not included in this review, as its scope of application is limited to US defence acquisition projects.

Most of the standards in Table 1 are meant for application to projects or organisations in any area of activity, with two exceptions. IEEE Standard 1540-2001 is specifically designed for software, and CEI/IEC 62198:2001 states in its 'Scope' section (page 11) that 'This International Standard is applicable to any project with a technological content. It may also apply to other projects' (p 11).

It is interesting to note that none of these standards are currently used for certification purposes, though in some cases this has been proposed and is being actively pursued. Rather, they all provide guidance and advice, and encourage the adopting organisations to adapt them to their own needs.

Table 1. The standards reviewed

Title	Author	Year	Pages	Comments	Scope*
National and international standards					
1. IEEE Standard 1540-2001: <i>Standard for Software Life Cycle Processes – Risk Management</i>	Institute of Electrical and Electronic Engineers, USA	2001	24	Recognised as American National Standard	P/O
2. CEI/IEC 62198:2001: <i>International Standard, Project Risk Management: Application Guidelines</i> , 1st edition, 2001–04	International Electrotechnical Commission, Switzerland	2001	37		P
3. JIS Q2001:2001(E): <i>Guidelines for Development and Implementation of Risk Management System</i>	Japanese Standards Association	2001	20		O
4. AS/NZS 4360:2004: <i>Risk Management</i>	Standards Australia/Standards New Zealand	2004	28		O
5. BS 6079-3:2000: <i>Project Management – Part 3: Guide to the Management of Business-related Project Risk</i>	British Standards Institution (BSI)	2000	22		P
6. CAN/CSA-Q850-97: <i>Risk Management: Guideline for Decision-Makers</i>	Canadian Standards Association (CSA)	1997	62		O
Professional standards					
7. <i>Risk Management Standard</i>	Institute of Risk Management (IRM)/National Forum for Risk Management in the Public Sector (ALARM)/Association of Insurance and Risk Managers (AIRMIC), UK	2002	18	Adopted by Federation of European Risk Management Associations (FERMA) in 2003	O
8. <i>Project Risk Analysis & Management (PRAM) Guide</i> , 2nd edition	Association for Project Management (APM), UK.	2004	186	Substantial revision of 1997 edition	P
9. <i>Guide to the Project Management Body of Knowledge (PMBOK®): Chapter 11, Project Risk Management</i> , 3rd edition	Project Management Institute, USA	2004	32		P

* P = project; O = organisation

The focus of the comparative analysis was to ascertain the extent to which the processes and steps described by the various standards are similar to each other. A high degree of similarity and consistency across the standards would indicate the emergence of a worldwide consensus regarding the way risk management ought to be conducted. A review of the process steps described by the selected standards identified the following main steps: planning, identification, analysis, treatment and control. Terminology differs between the standards, though the structure of the process in each case is similar. For example, in some standards ‘analysis’ is called ‘assessment’; and in some cases analysis is broken down into ‘estimation’ (of probability and consequences of the risk events) and ‘evaluation’ (determining the overall magnitude of the risk event, from which its priority is derived).

The comparison of processes from the nine standards is presented in three separate tables (Tables 2, 3 and 5). Each table consists of nine rows corresponding to the nine standards, while the columns correspond to the steps. The entries in the table include the sections of the standard that apply to the particular step in the process, and are numbered accordingly.

The columns of Table 2 compare the way the different standards address the planning step, which is the step exhibiting the widest variability in terms of scope and level of detail. At one extreme there are standards that take a very broad view and include in this step organisation-wide issues such as establishing the risk management policy, defining roles and responsibilities at various levels, and establishing the process to be followed. At the other end there are those that follow a more focused approach, consisting simply of planning the application of an existing risk management process to a specific project or instance.

Table 3 pertains to the three central steps in the process (identification, analysis, treatment), which were addressed in a basically similar manner by the standards. A consolidated list of tools for risk identification appears in Table 4. Table 5 compares the way the standards deal with the issue of control. The control step may refer to two levels of control: of the residual risks that remain after implementation of the treatment actions selected, or of the effectiveness of the risk management process. To the extent possible we have tried to separate the two.

Table 2. Elements of the planning step

Planning for risk management	
1. IEEE 1540-2001	5.1.1 Plan and implement risk management <ul style="list-style-type: none">5.1.1.1 Establish risk management policies5.1.1.2 Establish the risk management process5.1.1.3 Establish responsibility5.1.1.4 Assign resources5.1.1.5 Establish risk management process evaluation 5.1.2 Manage the project risk profile <ul style="list-style-type: none">5.1.2.1 Define the risk management context (technical and managerial objectives, assumptions and constraints)5.1.2.2 Establish risk thresholds: criteria of acceptability of a risk5.1.2.3 Establish and maintain project the risk profile:<ul style="list-style-type: none">a. The risk management contextb. A chronological record of each risk’s statec. The priority of each riskd. Risk action requests and treatment status
2. IEC 62198	5 Organisational issues <ul style="list-style-type: none">5.1 Management responsibilities5.2 Resources5.3 Communication5.4 Documentation

Table 2. Elements of the planning step (continued)

	<p>6.1 Establishing the context The strategic context The organisational context The risk management context Develop criteria Decide structure</p>
<p>3. JIS Q2001: 2001 (E)</p>	<p>3.2 Organisational structure 3.2.1. Role of top management 3.2.2. Role of chief risk management officer</p> <p>3.3 Risk management policy: 3.3.1 Announcement of the risk management policy 3.3.2 Risk management conduct guide 3.3.3 Establishment of risk management objectives</p>
<p>4. AS/NZS 4360: 2004</p>	<p>4.2 Establish the context 4.2.2 Establish the internal context 4.2.3 Establish the external context 4.2.4 Establish the risk management context 4.2.5 Develop risk evaluation criteria 4.2.6 Define the structure for risk analysis</p>
<p>5. BS 6079-3 2000</p>	<p>4.4 Managing the process - Risk management policy - Organisational infrastructure - Risk management programme at organisational, cross-organisational, project and sub-project levels</p>
<p>6. CAN/CS-Q850-97</p>	<p>4 Initiation 4.2 Defining the problem or opportunity and the associated risk issues 4.3 Identifying the risk management team 4.4 Assigning responsibility, authority and resources 4.5 Identifying potential stakeholders 4.6 Risk communication considerations</p>
<p>7. IRM/ ALARM/ AIRMIC</p>	<p>9 Structure and administration of RM 9.1 Risk management policy 9.2 Role of the Board 9.3 Role of business units 9.4 Role of RM function 9.5 Role of internal audit 9.6 Resources and implementation</p>
<p>8. PRAM</p>	<p>Initiate Set the scope, objectives and context for the risk management process, further divided into two sub-phases: a. Define Project aims to ensure common understanding of the project to which the risk management process is to be applied. b. Focus Risk Management Process fits the details of the risk management process to the specific requirements of the project.</p> <p>Organisational structure Planning for risk management Responsibilities Functional roles: The Project Manager’s role The Risk Process Manager’s role</p>

Table 2. Elements of the planning step (continued)

	The Risk Manager's role
	The Risk owner's role
	The Action owner's role
	The Technical Specialist's role
	Other functional roles
	The executive sponsor's role
	Risk management and the project life cycle
	Resourcing the risk management process
	Resourcing risk response actions
9. PMBoK®	11.1 Risk management planning
	The process of deciding how to approach and conduct the risk management activities for a project.
	Inputs: enterprise environmental factors; organisational process assets; project scope statement; project management plan.
	Tools and techniques: planning meetings and analysis.
	Outputs: Risk Management Plan (methodology; roles and responsibilities; budgeting; timing; risk categories; definitions of probability and impact; stakeholder tolerances; reporting formats; tracking).

Table 3 compares the contents of the different standards in terms of the three main steps of the risk management process: identification, analysis and treatment. To improve clarity and avoid duplication, the tools and techniques prescribed for the risk identification step were consolidated and are presented separately in Table 4.

In the analysis step, there seems to be a dominant distinction between the following two main activities:

- risk estimation, which refers to an assessment of the likelihood of occurrence and possible consequences of the risk events identified in the previous step; and
- risk assessment, which refers to evaluation of the assessed risk by comparison with the criteria and thresholds of the decision maker(s) in order to determine the priority for treatment.

In the risk treatment step, the set of possible courses of action mentioned by most of the standards was quite limited, and includes the following:

- avoidance;
- probability reduction (preventive counter-measures);
- consequence limitation, including recovery and contingency planning; and
- risk transfer, including subcontracting.

The key exceptions are PRAM and PMBoK®, where equal emphasis is given to both threats and opportunities throughout the process. Consequently, the risk treatment step in these two standards includes equivalent strategies for dealing with opportunities, namely:

- exploitation;
- probability enhancement;
- consequence improvement, including contingency planning; and
- risk-sharing, including joint ventures.

Table 3. Elements of the identification, analysis and treatment steps

	Identification	Analysis	Treatment
1. IEEE 1540-2001	5.1.3.1 Risk identification	5.1.3.2 Risk estimation 5.1.3.3 Risk evaluation	5.1.4 Perform risk treatment 5.1.4.1 Selecting risk treatment 5.1.4.2 Risk treatment planning and implementation
2. IEC 62198	6.2 Risk identification (Consider the impact of risks upon all project objectives – cost, time, quality etc).	6.3 Risk assessment Risk analysis (qualitative/quantitative): Risk limits and boundaries; Dependencies; Probability of occurrence; Impact on objectives Risk evaluation: Risk level vs. tolerability criteria; Priorities for treating risks; Risk acceptance	6.4 Risk treatment
3. JIS Q 2001: 2001	3.4.1 Risk analysis a. Risk finding b. Risk identification	3.4.1 Risk analysis c. Risk estimation (quantitative/qualitative) 3.4.2 Risk evaluation: comparison to necessary risk criteria 3.4.3 Risk management targets	3.4.4 Selection of risk treatments 3.4.5 Establishment of risk management program 3.5.1 Implementation of risk management program 3.5.2 Additional considerations for emergencies 3.5.3 Additional considerations for resumption 3.5.4 Operative control – documentation and management of preventive measure implementation procedures.
4. AS/NZS 4360:2004	4.2 Risk identification 4.2.2 What can happen 4.2.3 How and why it can happen	4.4 Risk analysis 4.4.2 Determine existing strategies and controls 4.4.3 Consequences and probability 4.4.4 Types of analysis: a. qualitative analysis; b. semi-quantitative analysis; c. quantitative analysis 4.4.5 Sensitivity analysis 4.5 Evaluate risks	4.6 Risk treatment 4.6.2 Identifying options for risk treatment 4.6.3 Assessing risk treatment options 4.6.4 Preparing and implementing treatment plans

	Identification	Analysis	Treatment
5. BS 6079-3: 2000	4.3 Risk identification and strategy 4.3.1 Risk model clarification	4.3.2 Risk analysis 4.3.3 Risk evaluation: unacceptable threat; negligible threat; acceptable threat; critical opportunity; desirable opportunity;	4.3.4 Risk treatment 4.3.5 Implementation
6. CAN/CSA-Q850-97	5 Preliminary analysis 5.2 Defining scope of decision(s) 5.3 Identifying hazards 5.4 Beginning stakeholder analysis 5.5 Starting risk information library	6. Risk estimation 6.2 Defining methods for estimating frequency and consequences 6.3 Estimating frequency 6.4 Estimating consequences 6.5 Refining stakeholder analysis through dialogue 7 Risk evaluation 7.2 Estimating and integrating benefits and costs 7.3 Assessing acceptability of risk to stakeholders	8 Risk control 8.2 Identifying feasible risk control options 8.3 Evaluating risk control options 8.4 Assessing stakeholder acceptance 8.5 Risk financing 8.6 Assessing stakeholder acceptance of residual risk
7. IRM/ALARM /AIRMIC	4.1 Risk identification 4.2 Risk description	4.3 Risk estimation: Probability and Consequences: both threats and opportunities 4.4 Risk analysis methods and techniques 4.5 Risk profile summarises results of analysis, and provides a tool for prioritising risks	7 Risk treatment
8. PRAM	Identify phase: <ul style="list-style-type: none"> • search for sources of risk and responses; • classify: suitable structure for risks and responses, aggregating/disaggregating as appropriate; • characterise: simple label or description 	Assess phase: Structure: Search/brainstorm/interview; order risks and responses for discussion purposes; distinguish specific and general responses. Ownership: allocate responsibility; approve contractor allocations. Estimate: identify areas requiring careful decisions; identify areas requiring more data and analysis; estimates of likelihood and impact. Evaluate	Planning responses phase: <ul style="list-style-type: none"> • plan risk event responses; • plan project risk responses.
9. PMBok®	11.2 Risk identification	11.3 Qualitative risk analysis 11.4 Quantitative risk analysis	11.5 Risk response planning

Table 4. Consolidated list of tools and techniques for risk identification

Assumptions analysis	Examination of vulnerabilities and weaknesses	Prompt lists
Benchmarking	Expert opinion	Prototyping
Brainstorming	Fault tree analysis	Questionnaires
Cause and effect diagrams (Ishikawa or fishbone diagrams)	Flow charts	Risk assessment workshops
Checklists	Hazard and operability studies (HAZOP)	Root cause analysis
Constraints analysis	Historical data	Scenario analysis
Delphi technique	Incident investigation	Stakeholder analysis
Diagramming techniques	Influence diagrams	Structured interviews
Documentation reviews	Interviewing	SWOT analysis (strengths, weaknesses, opportunities, threats)
Evaluation of other projects	Lessons learned	System engineering techniques
Event tree analysis	Nominal group technique	Systems analysis
Examination of past risk experience in similar organisations	Peer review	Taxonomies
Examination of past risk experience in the organisation	Personal observation	Technology readiness levels
	Previous experience	Testing and modelling
	Project monitoring	

In addition, PRAM distinguishes between two levels of risk in projects, namely ‘risk events’ and ‘project risk’ (discussed further below), and the PRAM process splits the risk treatment step to deal with these differently. ‘Plan Risk Event Responses’ aim to address individual risks, whereas ‘Plan Project Risk Responses’ tackle the overall risk exposure of the project.

It is interesting to note that the majority of the tools and techniques listed in Table 4 are descriptive and qualitative in nature, and that there are very few tools based on statistical or mathematical techniques.

Table 5 compares the two aspects of control: control of the risk mitigation actions for the specific project/activity, and control of the risk management process. As can be seen from the table, all the standards do address the issue of monitoring and controlling the effectiveness of the risk treatment actions selected for implementation in the previous step of the process, but not all are concerned with managing and improving the risk management process itself.

Different individual standards emphasise particular points, and present differences in meaning of key terms, as summarised in Table 6.

One issue of particular interest and recent debate in the risk management community has been the question of the definition of the term ‘risk’, and in particular whether this should include upside opportunity as well as downside threat (see Hulett *et al*, 2002, for a summary of this debate). Some maintain that the term ‘risk’ refers exclusively to uncertainties with negative consequences (for example Chapman and Ward, 2002; 2003), while others favour a broader definition (for example Hillson, 2003). Table 7 presents the definitions used in the nine selected standards, divided into three groups: those which use an exclusively negative definition, equating ‘risk’ with ‘threat’; those which do not explicitly state whether consequences are positive or negative; and those defining ‘risk’ as including both threat and opportunity.

Table 5. Elements of risk control

	Control of risk treatment actions	Control of RM process
1. IEEE 1540-2001	5.1.5 Perform risk monitoring 5.1.5.1 Monitor risk 5.1.5.2 Monitor risk treatment 5.1.5.3 Seek new risks	5.1.6 Evaluate the RM process (quality, areas which should be improved, opportunities for modifying procedures) 5.1.6.1 Capture RM information 5.1.6.2 Assess and improve RM process 5.1.6.3 Generate lessons learned
2. IEC 62198	6.5 Risk review and monitoring 6.5.1 Continuous: identifying new risks; effectiveness of RM process; updating and maintenance of standards, documents and procedures; examination of project budget, network and other project input	6.5.2 Post-project: effectiveness of RM process; improvement on future projects
3. JIS Q 2001:2001	3.6 Evaluation of the RM performance and effectiveness 3.6.1 Evaluation of RM performance a. Monitoring and measurement of the RM activities: 1. activities related to planning for RM; 2. risk treatment execution b. Evaluation of RM performance: 1. related to emergency response measures; 2. related to resumption measures	3.6.2 Evaluation of effectiveness of the RM system 3.7 Implementation of corrective and improvement measures for the RM system 3.9 Review by the organisation's top management
4. AS/NZS 4360: 2004	1.7 Monitoring and review: Effectiveness of treatment measures; review estimates; actual progress against plan	2.3.10 Monitor and review 2.4 Management review
5. BS 6079-3: 2000	4.3.5 Implementation: monitoring of resources usage; monitoring of agreed risk indicators; monitoring of risks	4.4 Managing the process: monitoring and reviewing RM
6. CAN/CSA-Q850-97	9.4 Establishing a monitoring process 9.4.2 Changing circumstances 9.4.3 Performance 9.4.4 Ensuring proper implementation 9.4.5 Verify correctness of assumptions	9.5 Evaluating the effectiveness of the RM decision process
7. IRM/ALARM/AIRMIC	8. Monitoring and review of the RM process	
8. PRAM	Implement responses phase: implement responses to risk events; implement responses to project risk; monitor changes in risk exposure; provide risk information to stakeholders; address RM process effectiveness	Manage process: review approach for each phase; consider integration of RM with other project and business processes
9. PMBoK®	11.6 Risk monitoring and control	

Table 6. Special emphasis and semantic differences in the standards

	Special emphasis	Semantic differences
1. IEEE 1540-2001	<ul style="list-style-type: none"> • Mentions specifically the need to communicate with stakeholders (5.1.2.4) 	
2. IEC 62198	<ul style="list-style-type: none"> • Includes a chapter on communication (5.3), which addresses interfaces across disciplines and risk reporting and meetings 	
3. JIS Q 2001:2001	<ul style="list-style-type: none"> • Designed in terms of a Risk Management System, defined as the subset of the organisation management system concerned with risk 	<ul style="list-style-type: none"> • Risk planning includes analysis, prioritisation, and treatment planning. • Risk analysis includes identification and estimation • RM means monitoring and controlling the risks that were identified and analysed and for which treatment plans were devised.
4. AS/NZS 4360:2004	<ul style="list-style-type: none"> • Entire chapter (2) devoted to embedding RM in the organisation • Lists communication and consultation (4.1) as a main element in the process • Mention in the Preface that it applies to both the management of potential gains and losses; however, no further discussion of this in the standard 	
5. BS 6079-3:2000	<ul style="list-style-type: none"> • Focus on link to business objectives and strategy • Role of stakeholder analysis 	<ul style="list-style-type: none"> • Addresses opportunities as well as threats
6. CAN/CSA-Q850-97	<ul style="list-style-type: none"> • Emphasises risk communication at all steps in the process • Emphasises collaboration with stakeholders 	<ul style="list-style-type: none"> • ‘Risk Control option’ means ‘an action intended to reduce the frequency and/or severity of loss’
7. IRM/ALARM/AIRMIC	<ul style="list-style-type: none"> • Link to organisation strategic management • Chapter (9) devoted to roles of various functions in the organisation 	
8. PRAM	<ul style="list-style-type: none"> • Includes chapters on benefits of managing risk (2), establishing an RM organisation (5), behavioural aspects (6), and implementation/application issues (7) 	<ul style="list-style-type: none"> • Addresses opportunities as well as threats • Defines risk at two levels: ‘risk event’, as an individual uncertainty that could affect one or more project objectives; and ‘project risk’, as overall impact of uncertainty on project itself.
9. PMBoK®	<ul style="list-style-type: none"> • Strong process orientation (inputs/tools and techniques/outputs) 	<ul style="list-style-type: none"> • Addresses opportunities as well as threats

Table 7. Definitions of ‘risk’

Negative definitions	Neutral definitions	Broad definitions
CAN/CSA-Q850-97:1997: ‘the chance of <i>injury or loss</i> ’	AS/NZS 4360:2004: ‘the chance of something happening that will have an <i>impact</i> upon objectives’	PMBok® 2004: ‘an uncertain event or condition that, if it occurs, has a <i>positive or negative effect</i> on a project objective ... includes both <i>threats</i> to the project’s objectives and <i>opportunities</i> to improve on those objectives’
IEEE 1540:2001: ‘the likelihood of an event, <i>hazard, threat</i> or situation occurring and its <i>undesirable consequences</i> ; a <i>potential problem</i> ’	BS6079-3:2000: ‘uncertainty ... that <i>can affect</i> the prospects of achieving ... goals’	IRM/ALARM/AIRMIC 2002: ‘combination of the probability of an event and its consequence ... consequences can range <i>from positive to negative</i> ’
	IEC 62198:2001: ‘combination of the probability of an event occurring and its <i>consequences</i> for project objectives’	PRAM Guide 2004: ‘an uncertain event or set of circumstances which, should it occur, will have an <i>effect</i> on achievement of ... objectives ... <i>either positively or negatively</i> ’
	JIS Q2001 (E): ‘a combination of the probability of an event and its <i>consequence</i> ’	

Note: emphasis added

Discussion and conclusions

Four of the standards listed in Table 1 limit their scope of application, as indicated by their title, to risk management in projects, while the other five are formulated in general terms. However, there are no significant differences, either in terms of the structure of the process or the contents of the various stages, between the two groups. It appears that the best practices in the field, as embodied by these standards and others, are applicable to projects and to other types of activities carried out in organisations. Thus it seems reasonable that any new standard development should have a general scope rather than being restricted to projects.

As is apparent from Tables 2, 3 and 5, the risk management processes presented by all nine selected standards have a great deal in common, suggesting that there is a universal consensus regarding what the risk management process should cover. Where there are apparent differences in process, these are largely attributable to variations in terminology. There are, however, some genuine and material differences among the standards, and these arise from three sources:

- One source is the inclusion of additional elements beyond the central risk management process. The main such elements are communication, consultation and collaboration with stakeholders; links to the organisational objectives and strategy; guidance related to the

adoption and implementation of a risk management system/function in the organisation; description of the benefits which can be expected from a structured approach to managing risk; and consideration of the human aspects of risk psychology, and of their impact on risk management effectiveness. All these are valuable and enhance the value of the standard; however, none of the nine standards reviewed includes them all. Thus it seems that there is room for additional work to address these important issues explicitly.

- The second source of variability among the standards, which was alluded to in the discussion of Tables 2 and 5, goes beyond the actual risk management process, being related to the scope of coverage of the standard itself. Certain standards cover mainly (almost exclusively) the risk management process itself, and ignore the aspects involved in establishing the organisational infrastructure needed to apply the process. They also devote little if any attention to the aspect of managing the process as an organisational asset, including measuring the effectiveness of the process (which is different from measuring the effectiveness of risk treatment actions implemented in a specific instance of the process), generating lessons learned, and in general continuous improvement of the process. Examples of the first type include IRM/ALARM/AIRMIC, PRAM and PMBoK[®], and to some extent IEC 62198 and AS/NZS 4360:2004. Examples of the second type, taking a broader view, include PRAM, IEEE 1540-2001 and JIS Q2001 (E). Clearly, a standard which offers more coverage and which explicitly addresses the organisational issues involved in adopting and implementing a risk management process in the organisation would be more valuable.
- The third source of difference relates to the differing definitions of ‘risk’ among the selected standards, which can be seen in two areas. First, some standards explicitly state that risk includes both threat (risk with potential negative impact) and opportunity (risk with potential positive impact), while others focus exclusively on threats, or are ambiguous about the type of risk (as summarised in Table 7). Secondly, the PRAM *Guide* has introduced a new concept by distinguishing between ‘risk event’ and ‘project risk’, both in the terminology and in how these should be managed. The definition guide ISO/IEC Guide 73:2002 *Risk Management – Vocabulary – Guidelines for Use in Standards* (British Standards Institute, 2002), was intended to create a common language for all risk standards documents, but this has not yet been reflected in currently available standards such as the nine included in this review. As a result, any future standard should unambiguously clarify the definition issue.

Based on the above remarks we conclude that although there is a wide consensus regarding the main steps and activities of a generic risk management process, there is still room for a comprehensive document which will not only combine the best elements of the existing standards, but also provide broad coverage of the issues related to instituting such a process. We are aware of at least two current initiatives to develop new risk management standards: by the Project Management Institute, which intends to produce a standard covering project risk management, and by the British Standards Institute, which is investigating the need for a broad standard encompassing all aspects of risk management. In addition, the International Standards Organisation (ISO) are actively considering whether to develop a new risk management standard or to adopt an existing one (ISO 2005).

Despite the existence of these initiatives, we believe that they are not intending to address the shortfalls identified by our review of current risk management standards. This leaves a clear gap for development of a comprehensive document which addresses these areas of shortfall, as well as consolidating the current consensus.

Note

- 1 Tzvi Raz is Director of the Henry Crown Institute of Business Research in Israel (which partially funded this research) and Professor of Management in the Faculty of Management, Leon Recanati School of Business Administration, Tel Aviv University; email: tzvir@tauex.tau.ac.il. David Hillson is Director, Risk Doctor & Partners, Petersfield, UK; email: david@risk-doctor.com.

References

- Association for Project Management (2004) *Project Risk Analysis & Management (PRAM) Guide*. 2nd edn. High Wycombe: APM.
- British Standards Institute (2000a) BS6079-3:2000: *Project Management – Part 3: Guide to the Management of Business-related Project Risk*. London: BSI.
- British Standards Institute (2000b) PD 6668:2000: *Managing Risk for Corporate Governance*. London: BSI.
- British Standards Institute (2002) ISO/IEC Guide 73:2002: *Risk Management – Vocabulary – Guidelines for Use in Standards*. London: BSI.
- Canadian Standards Association (2002) CAN/CSA-Q850-97: *Risk Management: Guideline for Decision-makers*. Mississauga, Ont: Canadian Standards Association.
- Chapman, C.B. and Ward, S.C. (2002) *Managing Project Risk and Uncertainty*. Chichester: Wiley.
- Chapman, C.B. and Ward, S.C. (2003) *Project Risk Management: Processes, Techniques and Insights*. 2nd edn. Chichester: Wiley.
- Hillson, D.A. (2002) What Is Risk? Towards a Common Definition. *InfoRM, Journal of the UK Institute of Risk Management*. April, pp 11–12.
- Hillson, D.A. (2003) *Effective Opportunity Management for Projects: Exploiting Positive Risk*. New York: Dekker.
- Hulett, D.T., Hillson, D.A. and Kohl, R. (2002) Defining Risk: A Debate. *Cutter IT Journal*. Vol. 15, No. 2, pp 4–10.
- Institute of Electrical and Electronic Engineers (2001) IEEE Standard 1540-2001: *Standard for Software Life Cycle Processes – Risk Management*. New York: IEEE.
- Institute of Risk Management/National Forum for Risk Management in the Public Sector/Association of Insurance and Risk Managers (2002) *A Risk Management Standard*. London: IRM/ALARM/AIRMIC.
- International Electrotechnical Commission (1995) CEI/IEC 300-3-9:1995 *Risk Management: Part 3 – Guide to risk analysis of technological systems*. Geneva: IEC.
- International Electrotechnical Commission (2001) CEI/IEC 62198:2001 *International Standard: Project Risk Management: Application Guidelines*. Geneva: IEC.
- International Standards Organisation (ISO) (2005) ISO/IEC New Work Item Proposal: *General Guidelines for Principles and Implementation of Risk Management*. London: BSI.
- Japanese Standards Association (2001) JIS Q2001:2001(E): *Guidelines for Development and Implementation of Risk Management System*. Tokyo: JSA.
- Norges Standardiseringsforbund (1991) Norsk Standard NS5814:1991: *Krav til risikoanalyser*. lysaker: NSF.
- Project Management Institute (2004) *Guide to the Project Management Body of Knowledge (PMBOK®)*. 3rd edn. Philadelphia, PA: PMI.
- Standards Australia/Standards New Zealand (2004) Australian/New Zealand Standard AS/NZS 4360:2004: *Risk Management*. Homebush, NSW: Standards Australia / Wellington: Standards New Zealand.
- US Department of Defense (2002) *Risk Management Guide for DoD Acquisition*. Defense Acquisition University, Defense Systems Management College. 5th edn. Fort Belvoir, VA: DSMC.