
Munich Personal RePEc Archive

Risk Management Standards: Towards a contemporary, organisation-wide management approach

Koutsoukis, Nikitas-Spiros

University of Peloponnese

2010

Online at https://mpra.ub.uni-muenchen.de/61031/
MPRA Paper No. 61031, posted 02 Jan 2015 11:07 UTC

International Journal of Business Policy and Economics
Vol. 3, No. 1, (2010) : 47-64

RISK MANAGEMENT STANDARDS: Towards a Contemporary, Organisation-Wide Management Approach

Nikitas-Spiros Koutsoukis
University of Peloponnese, Dervenakion 47 & Adimantou, Korinthos, Greece

Risk management has been progressively evolving into a systemic approach for organisational decision making in today's dynamic economic environment of the global era. In this context, risk management is reaching beyond its traditional finance and insurance application context and is entering the sphere of generic, organisation-wide management approaches. In support of this argument we consider four generic risk management standards issued at the institutional, national or international level, and identify their management-related attributes and characteristics.

Keywords: *Risk management; risk management standards; management; management approach; decision making; organisational decision making.*

1. INTRODUCTION

Risk refers to the possibility of an event that affects a decision maker with potentially undesirable consequences that may, or may not be complemented by desirable or, to be more precise, "non-undesirable" consequences. In this context, risk management refers to deliberate actions that allow the decision maker to anticipate and prepare for the set of probable events and their consequences in order to minimize the likelihood, impact, or both, of the undesirable consequences in favour of the non-undesirable ones (Borge, 2001.) However, in everyday parlance, the term Risk is also used, often interchangeably, to refer to the probability of the event, or the probability distribution of its consequences. Strictly speaking, however, a risk event is a tangible or intangible milestone in time, where nature (or the environment) unfolds a particular reality which may lead to consequences for the decision maker (French, 1988). Since consequences always follow [the] events, much of the success in risk management lies in identifying successfully the events to anticipate, their corresponding consequences and their likelihood, and to prepare in advance for dealing with the undesirable consequences in way that is most favourable for the decision maker.

Although, in its essence, risk management has been a human undertaking since the early days of humanity, it is mostly in the past decade or so that Risk

* Corresponding Author: *E-mail: nkoutsou@uop.gr*

Management emerged as a unified and systematic approach for dealing effectively with risks, especially in a business-wide and organisation-wide context (Kloman 1999, Bernstein 1998). In its relatively short life-span as a separable and discrete business practice and academic discipline however, Risk Management has found widespread acceptance in numerous fields; that is, in addition to and beyond the fields of finance, insurance, or actuary science in general. This argument is further supported by the extensive literature available for applying Risk Management in a variety of contexts; for brevity, we provide an illustrative tabulation of Risk Management literature in Table 1.

Table 1
Illustrative Tabulation of Risk Management Literature Contexts

Risk Management Context	*Reference examples*
(Holistic) Management: Enterprise-wide risk management.	Lam (2003), Merna & Al-Thani (2008)
Software and Information Systems Development.	DeMarco & Lister (2003), Lientz & Larssen (2006)
Project Management	Chapman & Ward (2003), Kendrick (2009). PMI (2009)
Construction	Smith *et al*. (2006), Barrie (2006)
Events Management	Ratherford Silvers (2008)
Corporate Value and Branding	Knight & Pretty (2000), Dallas (2006), Abrahams (2008)
Law, Institutions and Regulation	Sparrow (2000), Shapiro & Glickson (2004), Woodman and Klippel (2009)
Politics and Policy Implementation	Morgan & Henrion (1990), Clark & Marois (1996), Deuchars (2004)
Public Sector, Government and Governance	Akintoye *et al*. (2003), Fone & Young (2005), Drennan & McConnell (2007)
Security and Safety	Ericson & Haggerty (1997), Borodzicz (2005)

Taking into consideration the illustrative list in Table 1 we support the view that, for all practical purposes, Risk Management is emerging as an organisation-wide management approach (as opposed to management of an organisational function, *i.e*. the management of risks.) On one hand, this implies that risk management is extending its reach beyond its otherwise 'traditional' role as a 'problem-solving' technique, as it tends to be in its typical application context in the realms of designing and developing financial and insurance instruments (e.g. Doherty 2009, Crouhy *et al*. 2006, Bouchaud & Potters 2000, Butler 1999). On the other hand, it shows that contemporary management is also evolving, and in need of acquiring the ability to perform effectively in dynamic economic environments and business settings (e.g. Barton *et al*. 2002, Koutsoukis & Mitra 2003, Merna & Al-Thani 2008). The vibrant trends and shifts that take place in today's globalised economy closely resemble risk events; hence risk management lends itself well as a management 'philosophy,' especially

in the contemporary globalised, dynamic, and often turbulent business and economic environment.

This argument is further supported by the comparatively recent development and introduction of "Risk Management Standards," by various institutions at the national and international level. These standards are being described, and hence promoted as generic management methodologies for dealing with risk across the organisation, and are presumed to be 'context-free.' In this paper we take into consideration a selected set of well-known standards in support of our main argument. By analysing these standards we establish that contemporary risk management has evolved to include all the important elements to be used in-line with regular management practices, instead of pertaining to its traditional actuary-like role as a parallel [organisational] function, or some equivalent organisational performance improvement exercise.

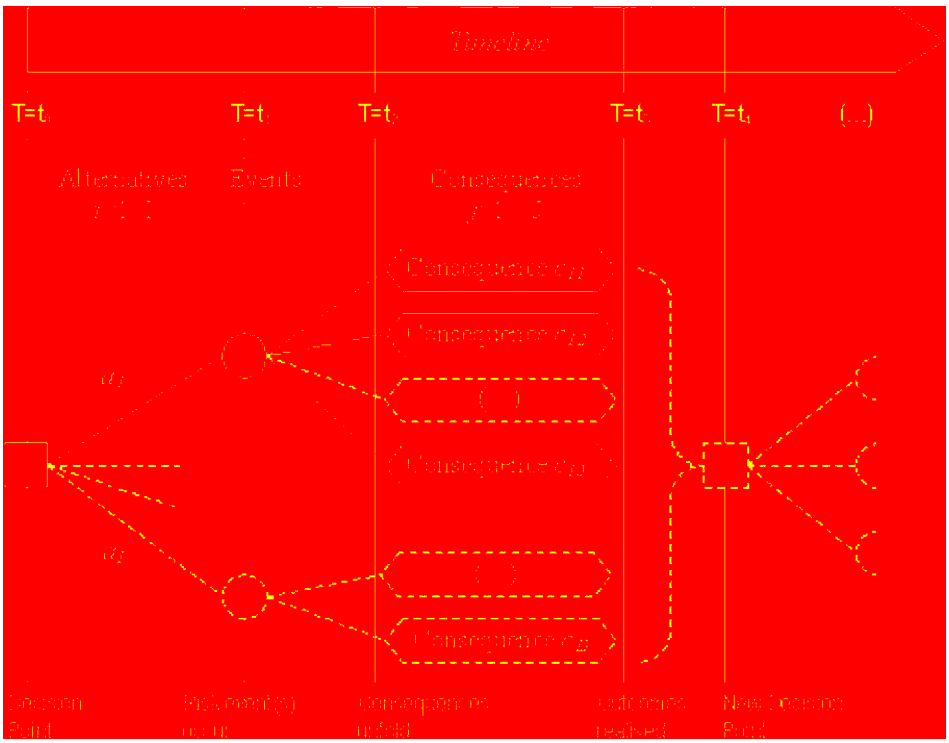
The rest of this paper is organised in the following way: in Section 1.1, we consider a timeline view of risk management and use it to identify the differences between Risk, Crisis and Disaster (or Emergency Planning) Management. In section 2, we consider five well-known risk management standards and identify their important attributes as management approaches. In section 3 we discuss our findings and present our concluding remarks.

1.1 A timeline View of Risk Management

From a decision analysis perspective and using a decision tree as the stereotypical Risk Management modelling technique, it is easily seen that risk management adheres to a particular timeline of proceedings from a decision maker's perspective. We note that we use the term decision-maker to denote the person or organisation who is affected by the risk-consequences. In situations where the decision making is being carried out by a representative (for example an investment broker) then our decision-maker is equivalent to the stakeholder, since (s)he is the one affected directly by the risk consequences. Henceforth, stakeholder and decision-maker are considered as equivalent unless otherwise noted.

In context of our time-aligned illustration, the essence of risk management is to make an informed decision, so that an(y) alternative chosen is a rationally 'best' choice in anticipation of anything that follows after the decision point. Accordingly, in Figure 1, risk-related decisions take place at an initial time point, where $T = t_0$. A risk event may occur at a subsequent time point, where $T = t_1$ for which the anticipated consequences are assumed with a probability distribution for the likelihood of each consequence c_{ij} following a particular event. However, the actual consequence(s) can only unfold at time point $T = t_2$, *i.e.* after the trigger-event occurs. Then, according to the alternative chosen at t_0, the 'final' outcome is realised for the decision maker only at $T = t_3$ (*i.e.* once the consequences have been fully rendered). Soon after, the decision maker is in a position to make new decisions regarding new risks, at time point $T = t_4$, and so on.

Figure 1
A Timeline View of Risk Management



For simplicity of illustration we are presenting all the time points as discrete and sequential; however, it is easily seen that actual risk management situations and time sequences may be significantly more complex: For instance, decision makers may be facing multiple decision points between t_0 and t_1, with seemingly unrelated choices, but correlated outcomes; true events may actually correspond to chains of events, and consequences may continue to unfold even after a new decision point presents itself. Similarly, an alternative may infer a risk management 'strategy' that includes a set consecutive choices and events, each based and dependent on the (final) outcome(s) of the previous choice, as is frequently seen in sophisticated decision trees. However, we used this simplified version to show a procedural view of risk management which, as we support in this paper, lends itself to management as a generic managerial approach.

All the same, it is important to note that in risk management, especially as practiced in finance and insurance, decision making takes place in advance of events and without the ability to revise this alternative once a risk event occurs – this option, when available, points to crisis management; the alternative chosen initially is equivalent to a risk management strategy and the decision maker simply awaits the future to unfold, hopefully in his favour (unless, of course, the initial decision is part of a more complex strategy anticipating multiple events before the final outcomes are rendered).

The timeline approach also allows us to draw a threshold between Risk Management and two comparable approaches for managing the non-desirable consequences of adverse events and situations: *Crisis* Management, and *Disaster* Management sometimes referred to also as Catastrophe Management or Emergency Planning.

In the timeline view, the bulk of '*in action*' Crisis Management takes place between time points t_1 and t_3. A crisis occurs after a *trigger* event initiates a set of undesirable consequences, but before the consequences are transformed to fixed, or definite, outcomes for the decision maker (e.g. Heath 1998). This crisis definition is in line with the literature on Crisis Management, and has important implications: it implies that, after the trigger event in t_1 and while the consequences are still unfolding between time points t_2 and t_3, the decision maker still has the opportunity to manage the crisis, *i.e.* to influence, against the 'worst' and perhaps in his favour, the final outcomes, which (will) become facts at time point t_3 but not before that.

Likewise, the greater part of '*in action*' Disaster Management takes place from time point t_3 onwards and until a new disaster management cycle begins at, say, point t_4. The trigger event occurs at t_1 and its primary and direct disastrous consequences are immediately unfolded at t_2 and rapidly become [definite and adverse] outcomes by time point t_3. In accordance with the corresponding literature the aim of disaster management is to be able to recover operational status as soon as possible after the disaster(s), to contain or to avoid knock-on effects from the primary consequences, and to revive the system to its pre-disaster state, before preparing for the next cycle (e.g. Alexander 2002). Inherently, immediately after the disastrous event and while recovering operations and containing secondary consequences, disaster management is equivalent to crisis management; it continues post-crisis however, until system restoration is completed. We note that, disaster management is mostly associated with low frequency, high impact risks, typically those associated with extreme events, such as acts of nature, large scale accidents, terrorist attacks or territorial conflicts.

We used the term '*in-action*' for Crisis and Disaster management to indicate that both of these approaches also include a 'planning/preparation' stage, i.e. identifying in advance the probable trigger events that may lead to a crisis or a disaster and to prepare in anticipation for their dire or non-desirable consequences (Augustine 1995, Alexander 2002.) However, this planning/preparation stage is directly equivalent to risk management, or what we would analogously call 'in action' risk management, which takes place only until time point t_0 in anticipation of everything that may take place past that point, and similarly for every consecutive decision point.

Hence, the timeline is an intuitive approach which defines risk management and indentifies it from related forms of risk-like management, namely Crisis or Disaster Management. Alternatively, from a decision-making taxonomy standpoint we could identify risk management as a normative approach, whereas crisis and disaster management are closer to descriptive approaches or heuristic methods.

Based on the procedural, time-aligned view of risks and their management, a number of standards have emerged in the past decade or so, as generic guidelines for applying organisation-wide risk management irrespective of the risk situations and application context(s). Notably, these are the following:

1. The Canadian Standards Association (CSA) issued the national standard CAN/CSA-Q850-97 "Risk Management: A guide for decision makers" in 1997. The standard was reaffirmed in 2002.
2. The *Risk Management Standard* developed by The Institute of Risk Management (IRM),The Association of Insurance and Risk Managers (AIRMIC) and ALARM The National Forum for Risk Management in the Public Sector (2002). This standard is frequently referred to as AIRMIC/IRM/ALARM Standard and is also adopted by the Federation of European Risk Management Associations (FERMA – 2003).
3. The standard developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) commonly referred to as the *COSO Enterprise Risk Management* (COSO-ERM) or simply COSO Standard (2004).
4. The Australian/ New Zealand Standard 4360:2004 (AS/NZS 4360:2004). This standard has only just been superseded by ISO 31000:2009; we refer to it because it is a major part of the Risk Management Standards chronology and the basis for the ISO standard.
5. The standard introduced recently by the International Organization for Standardization (ISO) as *ISO 31000:2009, Risk management – Principles and guidelines* (2009).

A number of other professional institutions have also developed equivalent standards which are closely related to particular professional practices, business or organisational contexts, and situations. For example the Project Management Institute has recently introduced a Project Management "Practice Standard" (PMI 2009); the National Health Service Litigation Authority (NHSLA, UK) regularly issues various risk management-related standards for negligence claims or similar healthcare issues (NHSLA, 2009). Similarly, the Basel Accords (I & II) are well known standards for financial institutions (Basel Committee 1988, 2004). Chronologically, the two Basel Accords are the main culprits for bringing organisation-wide Risk Management to the foreground of management, albeit for the banking and finance sector. As it is easily seen that these types of standards are targeted towards specific business sectors and application contexts, although they could also be elicited to generic management approaches. However, we find that the four generic standards identified above, support our main point sufficiently and make such an elicitation process unnecessary for the purposes of this paper.

2. GENERIC RISK MANAGEMENT STANDARDS

Considering the Basel Accord of 1988 as the first conventional risk management standard and ISO 31000:2009 as the most recent one, we note that organisation-wide risk management has been steadily evolving over the past two decades,

with the generic standards becoming so only the last decade, implying that a critical maturity stage has been reached for risk management to come 'out of the box.' For a comparison of the standards from a strictly risk management perspective, however, we refer to AIRMIC's comparison (2005), and Saner (2005) who also considers related issues in the U.S.A. although there are no issued standard(s) there, at least as equivalent to those we consider in this paper. In this section we provide an overview of the four selected risk management standards, focusing largely on their organisation-wide, management-related attributes and their similarities and differences as appropriate, in chronological order. For each standard we consider three main analysis points: organisational perspective, procedural view, and its organisation-wide implementation schema or attributes, in order to identify the elements of each as a [holistic] management approach.

2.1 CAN/CSA-Q850-97: 2002

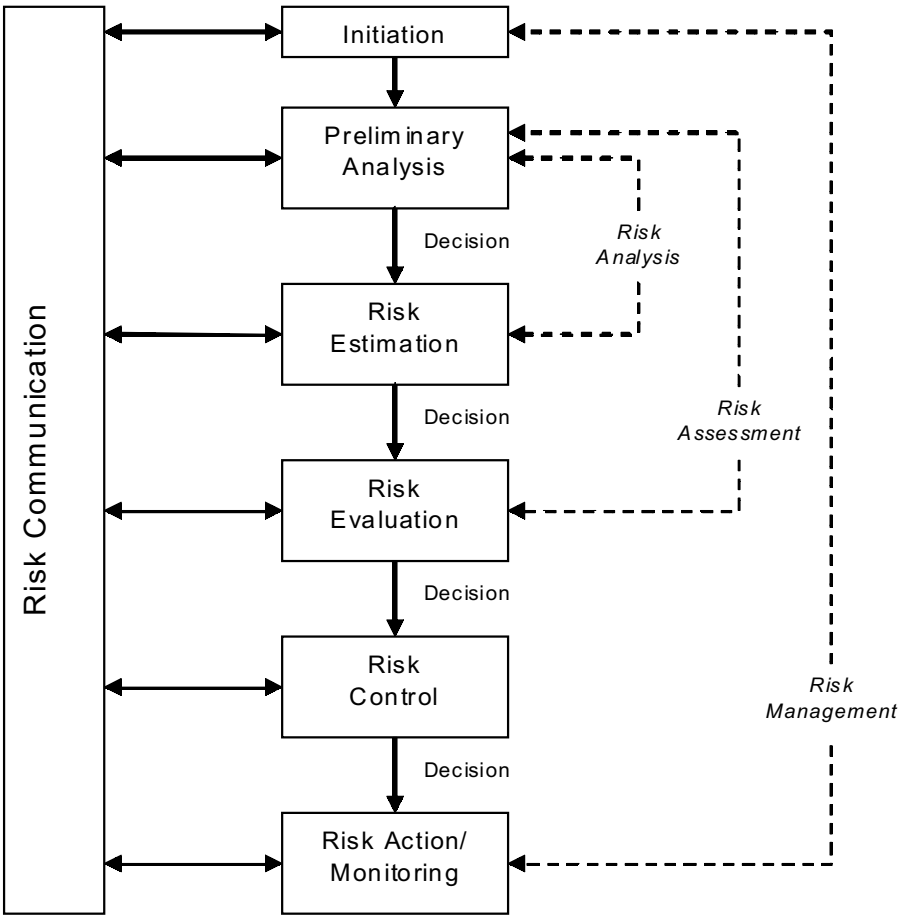
The CAN/CSA-Q850-97 standard adopts a decision-maker perspective, with the view that risk management is a process that can be adhered to any decision-making process, be it activities carried out by individual(s), organisation(s) or government(s). The standard considers risks 'pessimistically,' *i.e.* mostly as events that may incur loss to the decision-maker or stakeholder, and analyses loss(-es) according to three main attributes, namely: (a) The *Frequency* of the loss, or likelihood of the loss, (b) the *Consequences* of the loss, or the identifiable and measurable impact of the loss, and (c) the *Perception* of the loss, or the relative importance of the loss based on the stakeholder own preferences.

While Likelihood and Impact are considered elementary for quantifying risk and their consequences in an objective-like and comparable form, perception is an important attributes since it sorts the outcomes by their relative importance to the decision maker. For example, an identical investment of $1mil gone 'sour' will mean different things to different stakeholders and affect them differently, even though the investment's pre-risk likelihood and impact were equivalent for both, as typically identified in the 'small print' of agreements. Still, we note that the decision-making perspective of the standard allows it to blend in well in any organizational context, public or private, for profit or not, at all echelon levels, regardless of a top-down or bottom-up approach.

The standard's procedural viewpoint highlights the decision making perspective, as can be seen in Figure 2.

The decision points shown in Figure 2 lead to one of three possible activities: Stop the process, reiterate to a previous step, and take action or go to the next step – closely resembling flowchart(s) and algorithmic iterations. In Figure 2 it is also seen that every step works in tandem with communication inputs and outputs across and throughout the risk management process. Hence, at each step of the risk management process there are two main activities which set out the organizational context: (a) the decision points and (b) the communication points. The algorithmic nature of the CSA process suggests that risk management is a per-risk function, which may take place horizontally each time (i.e. in any single level of the management hierarchy) and that vertical integration (top

Figure 2
The CAN/CSA-Q850-97 Risk Management Process [Adapted from CSA 1997]



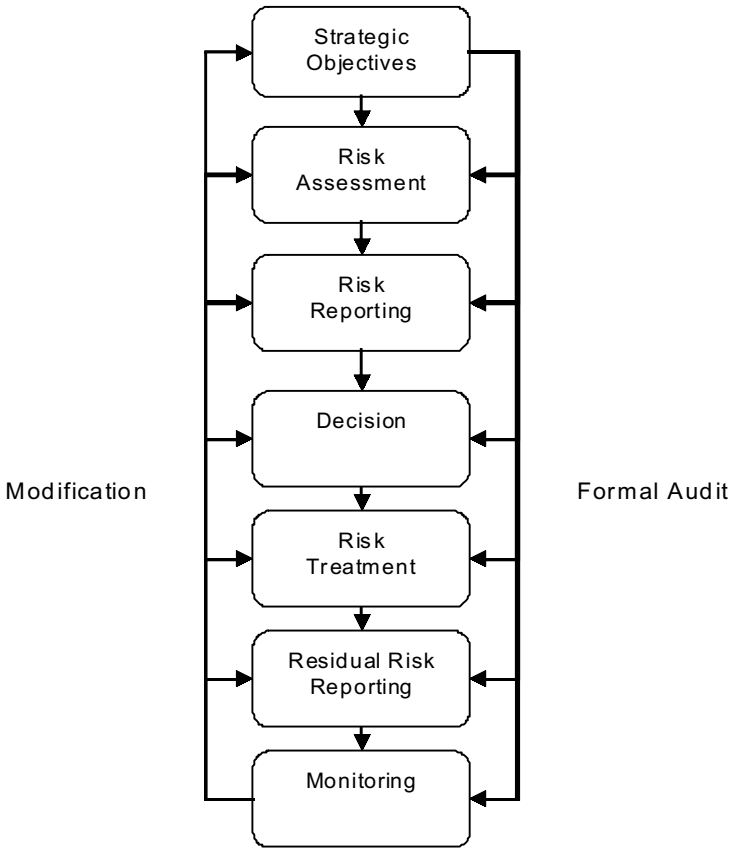
down or bottom up) is more likely to be achieved via aggregation paths: either by consolidating multiple risks (bottom-up) or by disaggregating them (top-down) and repeating the process each time. In any case, the communication route(s) ensure that risk management retains its organization-wide perspective.

2.2 AIRMIC / IRM / ALARM / FERMA : 2002

This standard considers risk management as a core organisational strategy which should also take a functional form at the tactical and operational levels. Risk events may have an upside and a downside and hence, the context or risk is neutral can be part of forward-looking positive strategies, instead of strategies that are mostly defensive against the worst. This top-down perspective subsequently requires that an organisation should be (re-)structured accordingly and maintain a multi-echelon view of risk(s); it also requires, by definition, top-management and stakeholder involvement in the risk management process.

Procedurally, the risk management step-wise approach is illustrated in Figure 3. Clockwise from top, each step's implementation and success is to be assisted or verified by formal audit processes of the organisation; similarly, each step's scope and objectives are subject to modification according to feedback loops from risk monitoring or intermediate steps.

Figure 3
AIRMIC/IRM /ALARM 's Risk Management Process



According to the standard's description, the most important decision point takes place after Risk Assessment, which captures, sequentially and iteratively, Risk Analysis and Risk Evaluation. The all important decision point is a equivalent to a milestone where the decision-maker decides on the importance of the risk(s) and selects the ways with which to treat the risks in question.

In addition to the strategic objectives setting the scene for the remainder of the risk management process as seen in Figure 3, the top-down approach is also evident in the standard's description of "Risk Analysis" (part of the "Risk Assessment" step). Organizational risk exposure is identified at the top organizational level in relation, mostly, to its environment and how that affects

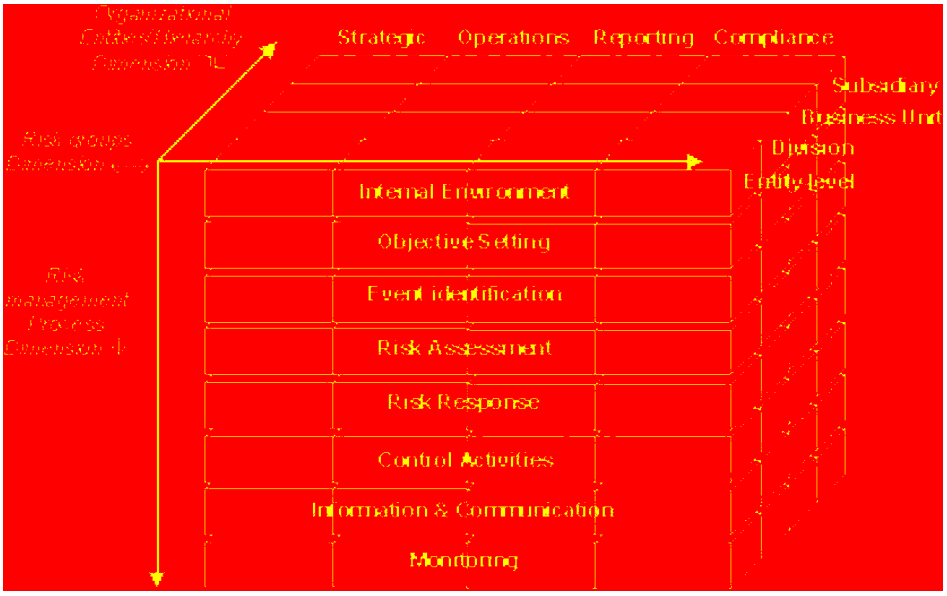
organizational objectives and operational status. Through the risk analysis step, risks are further classified according to the organization part they (may) affect the most, such as strategy, operations, finance, knowledge, and compliance. Subsequently the Risk Reporting and Communication step ensures that risk management objectives and objectives are communicated, internally to other management levels and business units, or externally to major stakeholders, and puts the emphasis on residual risks, or risks than remain unaffected by the risk treatment(s). It follows that through the internal risk communication path, the top-down risk-management schema leads to 'compartmentalized' risk management iterations in business unit level and so on until the operational level.

This standard's particular procedural setting points to a top-down and a star-like organizational approach, reminiscent of a strategically aligned and goal-seeking enterprise. Risk management objectives are set out centrally each time, in alignment with strategic objectives, and are disseminated once a milestone is reached (the decision point in Figure 3). Risk(s) are communicated vertically and horizontally to the organization, until each constituent becomes accordingly aware and can act accordingly.

2.3 COSO-ERM: 2004

The COSO-ERM standard adopts an entity-based view of the organisation, putting the emphasis on achieving stakeholder value as a positive balance between risk and opportunity. The value-based risk approach hence maintains a neutral perspective on risk, while hinting towards a quantifiable risk perception (the stakeholder value). Risk management is achieved through a component-based,

Figure 4
COSO's Entity-Based Risk Management Framework [Adapted from COSO 2004]



multidimensional framework, that spans horizontally and vertically in the organisation; the procedural structure is formed in layers of two-dimensional components. The approach is illustrated in Figure 4.

In Figure 4 the risk management step-wise process is equivalent to the top-down progression of eight layers on the vertical axis. The sequence is initiated internally through management which sets a risk management 'philosophy' regarding the organization's 'risk appetite,' or the balance between risk taking and risk avoidance. As noted in the standard, the risk appetite is supposed to reflect the organizational culture, inferring a bottom-up approach in determining risk appetite, rather than a [top-down] management agenda that is to be pursued. Obviously, although a managerial agenda is likely to influence strongly the organizational culture, we believe that the point being made is regarding a pragmatist's, bottom-up view of the organizational culture as opposed to a top-driven, mission-based and goal-seeking organization. Hence, this paradigm lends itself well even to organizations that are in the process of transforming themselves or their culture, and allows for at least slight variations in risk management within the individual organizational compartments, with the aim of course being to achieve organization-wide synchronization in the end. Following the initiation phase, the risk management continues layer by layer until risk controls have been put into place, communicated to the entities involved, and risk monitoring commences.

A "hidden" attribute of the visual representation shown in Figure 4 is that there is a constant information and communication process taking place between each compartment in all directions. Essentially, in the 'Risk Groups' and the 'Organizational Hierarchy' dimensions, each risk management step may be initiated in any compartment and spread or replicate in any direction until the whole of the organization is involved. This differs slightly from the feedback loops in the risk management process, which should always commence at the internal environment and proceed serially along the Risk management dimension.

One implication of COSO's compartmentalized, and realistic-like view of enterprise risk management is that risk management can also be carried out asynchronously throughout the organization. Although some kind of harmony and concurrence is likely to be necessary for efficiency and effectiveness purposes, this is more likely to be semantic (*i.e.* along the information and communication dimensions) than time-based (*i.e.* along the risk management sequence). Hence the matrix-like COSO approach lends itself well to large-scale, multi-faceted and multinational organizations often found in the global arena, including state-wide public organizations, and less so in smaller-scale organizations. This approach implies that 'uniformity' in the application of organization-wide risk management is likely to be achieved progressively through repetition, exactly because it is all the more difficult to impose it top-down in such organizations.

2.4 AS/NZS 4360:2004

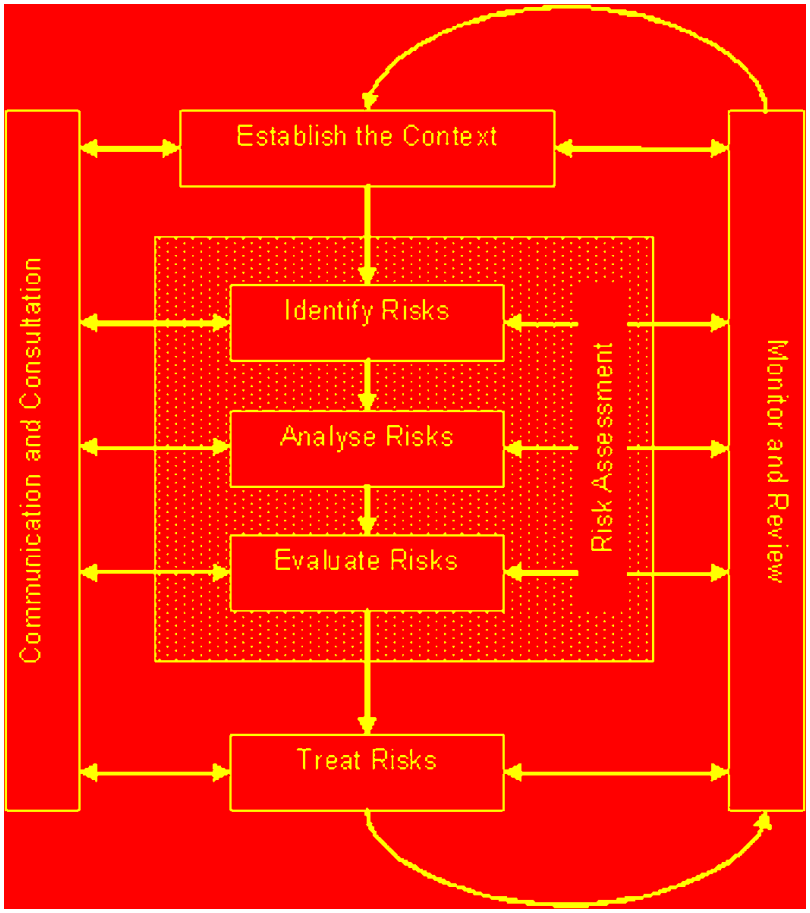
This is one of the most widely known standards in circulation. The standard was originally published in 1999 and was revised in 2004, which is the edition

under consideration. As mentioned previously, the AS/NZS standard has been superseded by ISO 31000:2009 which has been adopted by AZ/NCS instead. To avoid repetition, in this section we consider the main characteristics of AS/NZS 4360:2004 including those that are also found in the ISO standard, unless otherwise noted.

Similar to CAN/CSA-Q850-97 the AS/NZS standard adopts a decision-making perspective, with the view that risk management is a process that can be adhered to any decision-making process, carried out by individuals, groups and entire organisations. In contrast to the CAN/CSA however, and similar to the other standards, the AS/NZS standard, the notion of risk is neutral and so, the risk management setting "applies to the management of potential gains and potential losses."

The AS/NZS risk management process is illustrated in Figure 5.

Figure 5
The AS/NZS 4360:2004 Risk Management Process



In Figure 5 initiation of the risk management process commences with communication and consultation on the right, quickly passing on to establishing the [risk management] context at the top centre, before carrying downwards to the rest of the steps. Similar to the other standards we have considered, monitoring and reviewing is a means for carrying out feedback loops, ensuring that each step of the process remains sharp and focused as appropriate.

In the case of AS/NZS, the prime emphasis on communication serves a two-fold purpose. As an initiation step, the emphasis is on consultation, which allows risk management's context to be suitably outlined before any step-wise process carries on with the specific risk-management tasks of identifying, analyzing, evaluating and treating risks. The aim is to narrow-down the context for the rest of the process to carry on more focused and hastily, similar to a troubleshooting technique. Subsequently, once the step-wise process commences, the emphasis shifts to communication, that is dissemination of each step's outputs across the organization, internally or externally to other stakeholders and process owners in the risk management framework.

The consultation-based initiation allows (and aims for) organization wide involvement in establishing the risk management context as an outline for more detailed processes to follow across the organization. Subsequently, the process can be further compartmentalized during the 'Establish the context' step, where the scope of the risk management sequence is sketched in more detail, in accordance with the consultation outputs. It is at this step that unit-based or entity-based risk management deals with details of internal and external risks, risk criteria, and the subsequent components are defined.

Decision-making milestones are part of the risk treatment step, and vary according to the nature of risk outcomes: positive or negative. Respectively, the overall aim of decisions for risks with positive outcomes (*i.e.* opportunities) is to increase the likelihood of the outcomes, and to decrease the likelihood or impact of the negative outcomes in the other case.

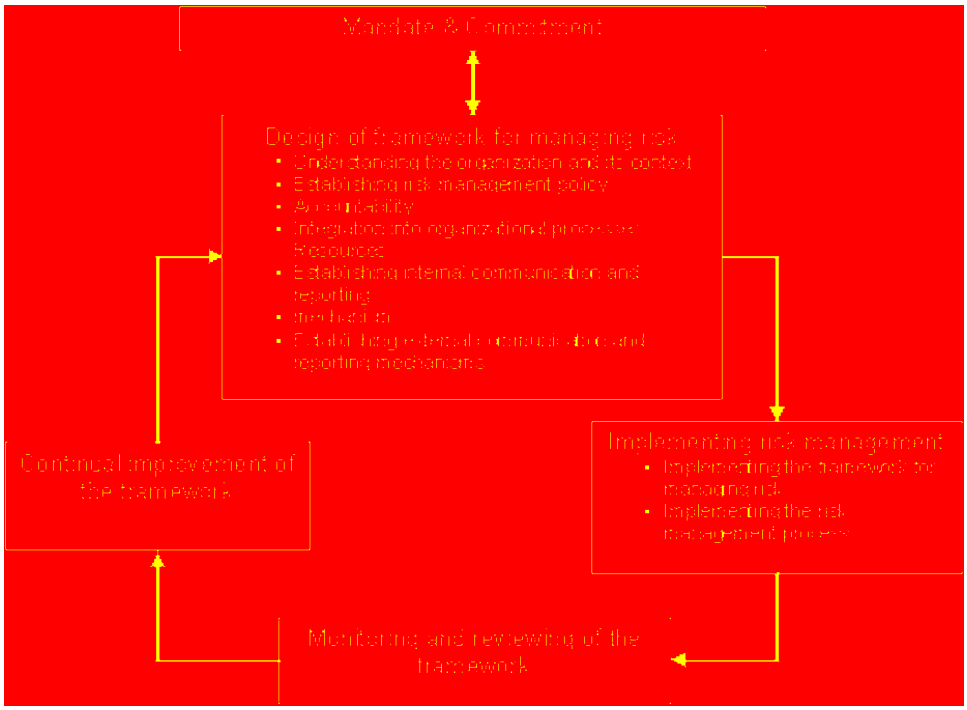
The initially umbrella-like, organization-wide consultation serves as a preparatory step for applying risk management, subsequently, in more detailed form. This is similar to a mission-statement-like approach that is progressively refined from the higher to the lower echelon levels, until the operational level is reached and individuals share and contribute to the organisational [risk management] mission.

2.5 ISO 31000:2009

The ISO 31000:2009 has been largely based on the AS/NZS 4360:2004 which results in a similar approach to [generic] risk management. Namely the risk neutrality and the procedural view can be considered equivalent for all practical purposes.

The ISO standard, however, puts the emphasis on establishing an organisation-wide risk management structure that is integral to the organisation and hence, designed, implemented, monitored and continually improved. Thus, the main novelty of the ISO standard in relation to the AS/NZS standard is the procedural view of integrating risk management within the organisation; a component-based, procedural view of this 'integration' process is shown in Figure 6.

Figure 6
The ISO Risk Management Framework Components



We note that the risk management process illustrated in Figure 6 for the AS/NZS standard, is now part of the "Implementing risk management" component and the "implementing the risk management process" step in particular.

It is easily seen that the ISO emphasis on an organisational framework, shifts the emphasis from applying an iterative process to establishing an organisation-wide risk-management structure. Hence, instead of applying an iterative process on an organization-wide scale or repeatedly across the organisation, as is the case with the other standards, the emphasis is now to (re-)structure the organisation so that the iterative risk management process is routinely applied as part of the organisational activities, much like any other operational process. From this perspective, what becomes more significant than applying risk management is to continually evaluate, monitor and improve, as necessary the risk management function on an organisation-wide, as opposed to simply applying a risk-management routine, in parallel to other organisational functions or quality assurance exercises.

3. DISCUSSION AND CLOSING REMARKS

In this paper we set out to show that Risk Management, as a discipline has reached a critical maturity level to be applied in a variety of contexts that are

beyond the realms of finance and insurance. Indeed in the last decade, at least, risk management as a systematic decision making approach has gained widespread acceptance in various fields and is being implemented in several application contexts, as briefly discussed in the beginning of this paper.

As a result risk management is increasingly being viewed as a systemic component of contemporary decision-making as applied in an organisational context. From this perspective risk management appears to be evolving into a generic management approach, one that can be applied in any organisational context and level, and regardless of whether the organisation belongs to the private, non-profit, or public sector(s). We find that this is natural evolutionary step, especially when considering the sway and rapid dynamics of today's globalised economic environment and it's Chaos-theory-like, extended reach across the globe.

In order to communicate our argument we have adopted a timeline perspective to illustrate the main mechanisms of risk management as a decision-making routine, and used to distinguish risk management from two additional approaches for managing the non-desirable consequences of adverse events and situations: Crisis management and Disaster management. We consider risk management as the prime step and hence an integral part of these approaches, albeit with the purpose to prepare the decision maker for anticipating and subsequently dealing effectively with crises or, god forbid, disasters.

In support of our argument we have considered a set of well known risk management standards that have been introduced at the institutional, national, or international level, but as generic, context-free approaches. These standards are: the 'Canadian' national standard, CAN/CSA-Q850-97; the AIRMIC/IRM/ALARM Standard; the COSO-ERM standard; The Australian standard, AS/NZS 4360:2004; and the ISO standard, ISO 31000:2009. All the standards pertain to specific risk management processes, which with slight differences in terminology and the level of detail pertains to the following an iterative decision-making sequence: Identification of risks, assessment of risks in terms of their likelihood and the impact of their consequences, evaluation and selection of risk treatment methods, monitoring of the risks following implementation(s) and providing feedback to all the previous steps as necessary.

In analysing these standards for the purposes of supporting our argument we have identified a number of interesting, management-oriented attributes.

Three out of five standards point towards a top-down approach: the CAN/CSA, AIRMIC/IRM/ALARM and AS/NZS standards. The CAN/CSA adopts risk management as an algorithmic process and achieves organisation-wide integration through aggregating and disaggregating risk management as necessary; The AIRMIC/IRM/ALARM standard follows more closely a Strategic approach, whereby risk management becomes a core strategic and strategy component and is subsequently disseminated as part of the strategy refinement towards the operational level; The AS/NZS standard seems to follow a mission statement setting, which is then refined towards the operational level. Between AIRMIC/IRM/ALARM and AS/NZS the main difference is hence the strategic,

objectives-based focus of the strategy in comparison to the generic and softer focus of a mission-statement-like approach.

The COSO-ERM standard, with its multidimensional approach, identifies a less-hierarchical perspective, but still well-structured organisational view of implementing risk management. The risk management sequence can thus be initiated from any organisational entity and spread via communication paths to the rest of the organisation. This setting showcases a risk management approach that is well suited to large scale, multinational or state-wide public organisations where the complex structure can pose as an obstacle to achieving top-down, uniform risk management throughout.

Finally, the ISO standard sets forth the case for integrating risk management within an(y) organisation, putting the emphasis on setting an organisation-wide framework and 'demoting' the risk management sequence to a routine operation, within the larger organisational context. And this is, perhaps, the most notable way of showing that risk management has evolved into an organisation-wide management approach.

References

Abrahams D., (2008). *Brand Risk: Adding Risk Literacy to Brand Management*, Gower Publishing.

AIRMIC, (2005), *Risk Management Standards Comparison*, AIRMIC, Available Online at *http://www.airmic.com/en/Library/Risk_Management_Standards/Comparison_of_Standards.cfm - accessed on 20.11.2009*

AIRMIC, ALARM, IRM, (2002), *A Risk Management Standard*, AIRMIC, ALARM, IRM, Available Online at *http://www.theirm.org/publications/PUstandard.html*, (Accessed on 20.11.2009).

Akintoye A., Beck M., and Hardcastle C., (Eds), (2003), *Public Private Partnerships: Managing Risks and Opportunities*, Blackwell.

Alexander D., (2002), *Principles of Emergency Planning and Management*, Terra Publishing.

AS/NZS-Standards Australia/Standards New Zealand, (2004), *Risk Management*, AS/NZS.

Augustine N., (1995), Managing the Crisis You Tried to Prevent, *Harvard Business Review*, November-December 1995, HBR.

Basel Committee on Banking Supervision, (1988), International Convergence of Capital Measurement and Capital Standards (Updated to 1998), BIS–Bank for International Settlements, Available Online at *http://www.bis.org/publ/bcbsc111.htm*, (Accessed on 20.11.2009),

Basel Committee on Banking Supervision, (2004), Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework. BIS–Bank for International Settlements, Available Online at *http://www.bis.org/publ/bcbs107.htm*, (Accessed on 20.11.2009).

Bernstein P. L., (1998), *Against the Gods: The Remarkable Story of Risk*, Wiley.

Borge D., (2001), *The Book of Risk*, Wiley.

Borodzicz E. P., (2005), *Risk, Crisis and Security Management*, Wiley.

Bouchaud J-P., and Potters M., (2000), *Theory of Financial Risks: From Statistical Physics to Risk Management*, Cambridge University Press.

Butler C., (1999), Mastering Value at Risk: A Step-by-Step Guide to Understanding and Applying VaR, *Financial Times*, Prentice Hall.

Chapman C., and Ward S., (2003), *Project Risk Management: Processes, Techniques and Insights*, (2nd Edition), Wiley.

Clark E., and Marois B., (1996), Managing Risk in International Business, Thomson.

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

Crouhy M., Galai D., and Mark R., (2006), *The Essentials of Risk Management*, McGraw-Hill.

CSA–Canadian Standards Association, (1997), CAN/CSA-Q850-97 – *Risk Management: Guideline for Decision Makers*, Reaffirmed, 2002, CSA.

Dallas M., (2006), Value & Risk Management: *A Guide to Best Practice*, Blackwell.

DeMarco T., and Lister T., (2003), *Waltzing with Bears: Managing Risk on Software Projects*, Dorset House Publishing.

Deuchars R., (2004), *The International Political Economy of Risk: Rationalism, Calculation and Power*, Ashgate.

Doherty N., (2000), *Integrated Risk Management: Techniques and Strategies for Reducing Risk*, McGraw-Hill.

Drennan L., and McConnell A., (2007), *Risk and Crisis Management in the Public Sector*, Routledge.

Ericson R. V., and Haggerty K. D., (1997), *Policing the Risk Society*, Oxford University Press.

FERMA–Federation of European Risk Management Associations, (2003), A Risk Management Standard, FERMA, Available Online at *http://www.ferma.eu/AboutFERMA/ARiskManagementStandard/tabid/195/Default.aspx*, (Accessed on 20.11.2009).

Fone M., and Young P. C., (2005), *Managing Risks in Public Organisations*, Perpetuity Press.

French S., (1988), *Decision Theory: An Introduction to the Mathematics of Rationality*, Reprint 1993, Ellis Horwood.

Heath R., (1998), *Crisis Management for Managers and Executives*, Financial Times, Pitman.

ISO–International Organization for Standardization, (2009), *Risk Management – Principles and Guidelines*, ISO.

Kendrick T., (2009), *Identifying and Managing Project Risk: Essential Tools for Failure-Proofing Your Project*, Amacom.

Kloman F., (1999), Milestones: 1900 to 1999, *Risk Management Reports*, December, 26(12), Available Online: *http://www.riskinfo.com/rmr/rmrdec99.htm*, (Accessed on 20.11.2009).

Knight R. F., and Pretty, (2000), *Brand Risk Management in a Value Context*, Templeton College.

Koutsoukis N-S., and Mitra G., (2003), *Decision Modelling and Information Systems: The Information Value Chain*, Kluwer Academic Publishers.

Lam J., (2003), *Enterprise Risk Management: From incentives to Controls*, Wiley.

Lientz B. P., and Larssen L., (2006), *Risk Management for IT Projects*, Butterworth-Heinemann, (Elsevier).

Merna T., and Al-Thani F. F., (2008), *Corporate Risk Management*, (2nd Edition), Wiley.

Morgan M. G., and Henrion M., (1990), *Uncertainty: A Guide to Dealing with Uncertainty in Risk and Policy Analysis*, (8th Printing, 2006), Cambridge University Press.

NHSLA–National Healthcare Service Litigation Authority, (2009), *Framework Document*, NHSLA, Available Online at *http://www.nhsla.com/RiskManagement/*, (Accessed on 20.11.2009).

PMI–Project Management Institute, (2009), *Practice Standard for Project Risk Management*, Project Management Institute, (PMI).

Ratherford Silvers J., (2008), Risk Management for Meetings and Events, Butterworth-Heinemann, (Elsevier).

Saner M., (2005), *Information Brief on International Risk Management Standards*, Institute on Governance (IOG), Available Online at *http://www.iog.ca/publications/2005_intl_risk_mgt_standards.pdf*, (Accessed on 20.11.2009).

Shapiro S. A., and Glickson R. L., (2004), *Risk Regulation at Risk: Restoring a Pragmatic Approach*, Stanford University Press.

Smith N. J., Merna T., and Jobling P., (2006), *Managing Risk in Construction Projects*, (2nd Ed.), Blackwell.

Sparrow M. K., (2000), *The Regulatory Craft: Controlling Risks, Solving Problems, and Managing Compliance*, The Brookings Institution.

Woodman G. R., and Klippel D., (Eds), (2009), *Risk and the Law*, Routledge.