Models as mediators: is AS/NZS ISO 31000 a mediator for risk and risk management?

Author

Chris Peace
Principal consultant
Risk Management Ltd
PO Box 7430
Wellington 6242
04 389 2665
chris.peace@riskmgmt.co.nz

This working paper is a revised version of a paper presented at the New Zealand Society for Risk Management biennial conference in Wellington on 7 September 2012. **It may be subject to further revisions which will be posted on the Risk Management Ltd website** www.riskmgmt.co.nz.

Comment on the paper is welcome.

Reference is made in this paper to the international standard ISO 31000; in Australia and New Zealand this has been adopted as AS/NZS ISO 31000. The content and language are identical.

Abstract

Model: something used as an example.

Mediator: in general terms, a variable that explains the process by which one variable causes another.

Metaphor: a thing regarded as symbolic of something else.

Models are important tools in science, as instruments of investigation and to help understand theories. They mediate between theory and the world, acting as autonomous agents. To know if models are valid we need to understand how they were constructed, how they function, what they represent and the extent to which we can learn from and with them.

The risk management process set out in ISO 31000:2009 "Risk management – Principles and guidelines" can be regarded as a model to help understand risk and how risk can be managed. Can the model be regarded as valid, supported by academic research and real-world experience? This question is of considerable importance to risk practitioners (who may rely on application of the standard as a key tool) and decision-makers (who rely on effective risk assessments). It is also of significance to academic research if that research is based on the standard.

To try to answer the question this paper explores research evidence for each of the stages in the standard and compares the research with some real-world experience. The outcomes may then help assure users of the standard as to its research-based validity and inform future revisions of the standard.

Introduction

In his review of the history of risk management, Kloman (2010) argued that evolution favoured those members of the human species able to manage the uncertainties of food, warmth and shelter leaving sufficient time for cultural activities that further favoured those able to take advantage of opportunities.

Development of human culture enabled record keeping beyond the lifetimes of individuals and an increasing ability to try to forecast the future. Blind uncertainty about the future (unknown unknowns) had been replaced with an ability to forecast some of the future (known unknowns). The Middle Ages brought the concept of free will and, over the subsequent 1000 years, steady growth of risk-related concepts.

The 20th century saw a dramatic growth in risk concepts, terms and definitions. Growth in academic research and practitioner pontificating has resulted in many and diverse definitions of risk, risk management and related terms and the development of risk management processes and frameworks. Some are generic while others are topic- or sector-specific.

This raises questions of importance to risk practitioners and researchers that may be summarised as "which definitions and risk management processes are sufficiently generic to be widely applicable under a majority of situations to academic research and applied risk management?".

This paper attempts to cast light the question in relation to processes by regarding them as research-related models that may mediate between data and theory.

Risk theories, models and data

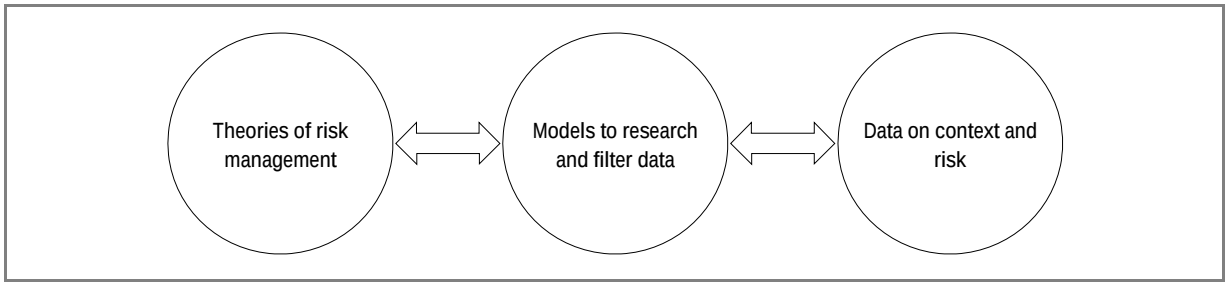
Using the term "model" to describe the risk management process may seem strange to risk management practitioners. However, the following quotation may help understand why this approach has been taken.

> *A model is expected to provide a setting, a common frame – in other words, it is expected to make visible a set of constraints, within which certain problems can be enunciated in a*

> *particular way, and certain problems solved. Let us be clear about this. A model is a convention – a way of talking about something in a manner that is understandable and useful in a community of observers. It is not a description of reality, but a tool in terms of which a group of observers in a society handle the reality they find themselves interacting with. … an individual may never communicate what is accessed to another individual except in terms of models. This is not a limitation, but is precisely the motor for the generation of a consensual domain. A consensual domain is none other than the play of a particular set of interacting models.*
>
> (Espejo, 1989)

Morrison & Morgan argued that models not only act as mediators between theory and data (see Figure 1 below) but that models can be used to aid in the construction of theory using data gathered from the world (1999, p. 10 and 18) , a point discussed further later in this paper.

Figure 1. Relationship between theories of risk management, models and data



Morrison & Morgan (p. 35) further argued that "models have certain features which enable us to treat them as a technology. They provide us with a tool for investigation, giving the user the potential to learn about the world or about theories or both. Because of their characteristics of autonomy and representational power, and their ability to effect a relation between scientific theories and the world, they can act as a powerful agent in the learning process. That is to say, models are both a means to and a source of knowledge".

Thus, a risk management model may act as a mediator between theories of risk management and data specific to the context of an organisation or risk management activity. It also may enable gathering of data from the world and its synthesis into a form that enables testing or development of theory.

What is theory?

Bacharach (1989, p. 496) defined theory as:

> *… a statement of relations among concepts within a boundary set of assumptions and constraints. It is no more than a linguistic device used to organize a complex empirical world. ... the purpose of a theoretical statement is twofold: to organize (parsimoniously) and to communicate (clearly).*

The primary goal of a theory is to answer how, when and why questions. "What" questions are answered by descriptions.

Theory was defined by Gill & Johnson (2010) as "a formulation regarding the cause and effect relationships between two or more variables" while the Concise English Dictionary (Soanes & Stevenson, 2008) defined "theory" as:

> *1. A supposition or a system of ideas intended to explain something, especially one based on general principles independent of the thing to be explained.*
>
> *2. A set of principles on which an activity is based.*

Evaluation of a theory uses two criteria (Bacharach, 1989):

- falsifiability
- utility.

Theories must be constructed so they can be tested to determine if they are falsifiable. That is, they cannot be proved correct, only proved to be false. They also must have utility in the form of explanation and prediction.

Some management theories are applicable to specific types of organisations but can operate over different periods of time (eg, finance) while other management theories may operate in a narrow period of time but be applicable to many, possibly all, types of organisations (Bacharach, 1989, p. 500).

Theories of risk management

Articles and textbooks frequently refer to the "theory of risk management" without stating the nature of the theory or citing a source. Some authors may refer to one of more components of what a theory covers (eg, market risks, commercial risks and external event risks (Servaes, Tamayo, & Tufano, 2009)) although they are naming types of risks. Some claim their work will demonstrate the underlying characteristics of a specific theory of risk management (Tworek, 2012). Others refer to risk as part of the decision-making process (see, for example, Simon, 1979, who mentioned risk as part of statistical decision theory). A theory and model for dynamic risk management developed by Fehle & Tsyplakov (2005) was found to represent (in AS/NZS ISO 31000 terms) a risk control or treatment model.

Authors have discussed risk management for many years, usually with a suffixed adjective to distinguish their specific form of risk management. For example, Meulbroek (2002) writing about the challenge and promise of integrated risk management but essentially discussed financial risk management in relation to the value of a firm. Such theories seem to be those applicable to a narrow range of organisations over different periods of time (Bacharach, ibid)

Contingency theory explains how organisations and their systems of controls (sometimes called internal controls) vary with external and internal context-related factors such as legislation, competition, size, ICT, strategy, technology and environment (Woods, 2009). It can be used to explain how risk management is implemented in organisations.

Work by Baird & Thomas (1985) (who developed a contingency model of strategic risk taking) used language broadly aligned with AS/NZS ISO 31000 and hypothesized effects of variables on risk taking.

Collier & Woods (2011, p. 117) used a pluralist perspective to compare risk management in four case study local authorities "using institutional, contingent, resource dependence and power" theories to show that the four theories, taken together, provided an explanatory framework for both the similarities and differences between the small and large local authorities in England and Australia. The individual theories provided a necessary but insufficient explanation for the factors motivating the introduction and use of risk management systems.

However, Woods, Baird & Thomas and Collier & Woods were not using a general theory of risk management applicable to many organisations, albeit in a limited period of time. Does this imply there is no generic theory of risk management and that each theory is more in the nature of a model to describe data? Do most theories of risk management describe a world view held by academics or practitioners operating in a specific field with, generally, no attention to other fields? If so, this is hardly helpful to multi-disciplinary practitioners but it does present opportunities for cross-disciplinary research.

Some theories have been adapted from other fields of research (eg, agency theory, general deterrence theory, prospect theory, social control theory in relation to compliance and utility theory) while others have been developed in relation to specific activities in specific industries (eg, bank risk-taking, the drugs industry, large risks and small risks). Other theories have been developed to describe classes of events or activities. For example, decision theory, disaster theory, game theory, marketing theory, mindful response theory, multi-attribute value theory and organisation theory.

Alone, none of the above theories are sufficient to describe risk management generally or enable predictions to be made about risk management activities in practice. It therefore is suggested the Morrison & Morgan theory/model/data description needs revision for risk management to allow for multiple theories.

Mediators in research and practice

MacKinnon, Coxe, & Baraldi (2012) provided guidelines for the investigation of mediating variables in business research. Based on their work and using the ISO 31000 risk management process as a

source of possible mediators, it is argued that, for example, effective treatment of risk requires mediation by communication or consultation. It is further argued the whole risk management process acts as a mediator that can predict the effectiveness of risk management. Inadequate or non-application of any part of the process will result in an incomplete understanding of risk or ineffective management of risk.

From experience this makes sense. For example, failure to consult stakeholders may result in:

- an incomplete understanding of their views
- the context of the organisation or risk
- the nature or level of risk or the acceptability of a given risk.

Risk management processes as models

As noted earlier, Morrison & Morgan (p. 35) argued that models have certain features which enable us to treat them as a technology that provides us with:

- tools for investigation (giving the user the potential to learn about the world or about theories or both)
- an agent in the learning process
- a means to and a source of knowledge.

Which risk management model (process) has sufficient diversity to provide a generic model for a majority of researchers and practitioners?

The range of risk management models is considerable but the significant or commonly used models seems to be limited to less than 20 and may be reducing. For example, a British Standard *Code of practice for risk management* BS 31100 was published in 2008 but withdrawn in 2011.

Raz & Hillson (2005) analysed some, but not all, of the commonly used models then in use and showed how they compared with each other. Their work has been adapted and updated here.

Risk standards and documents

Two generic risk management processes, the COSO framework for enterprise risk management (ERM) (COSO, 2004) and the international standard ISO 31000: 2009 *Risk management – Principles and guidelines* (ISO, 2009c), are in common use internationally. ISO 31000 was derived from the earlier joint Australia/New Zealand standard AS/NZS 4360. The application of ISO 31000 and COSO has substantially narrowed approaches to risk management in general use.

In 2011, a survey of 1823 respondents in 111 countries indicated that more than 37% of organisations were using ISO 31000, 17% were using the COSO ERM model and 14% were using AS/NZS 4360 (Goy *et al.*, 2012). The results were probably biased as the survey formed part of a conference on ISO 31000 but they give a broad indication that about 50% of respondents were using ISO 31000 or the earlier AS/NZS 4360 and a further 17% were using the COSO document.

To these generic standards can be added specialist and technical risk standards and frameworks. Some, such as the *Sanitary and Phytosanitary Agreement* (WTO, 1997) and the *Terrestrial Animal Health Code* (WOAH, 2009) are of considerable economic significance to NZ, as they help manage risks to our food exports and from imported animal and plant diseases.

Some of the standards and documents identified by Raz & Hillson and in this study are activity-specific. For example, the:

- International Electrical and Electronic Engineers Standard 1540 (IEEE, 2001) sets out processes for risk management in software life cycle processes
- British Standard BS6079-3 (BSI, 2000), draft International Electrotechnical Standard IEC 62198 (IEC, 2012 - the draft version of the standard was reviewed), the Project Management Institute Book of Knowledge (PMI, 2008, the PMBok) and Association for Project Management PRAM guide (Association for Project Management, 2012) set out processes for project risk management
- New Zealand Ministry of Civil Defence and Emergency Management (MCDEM) 4Rs is about emergency management processes
- UK HSE 5 Steps (HSE, 2011) is a simplified approach to safety-related risk assessments in the UK.

BS6079-3 had not been reviewed at the time of writing.

Other standards are generic but are country-specific or have not been adopted outside the country of origin. For example:

- IRM/ALARP/AIRMIC published a *Risk Management Standard* in 2002, based on terms and definitions from the now-out-of-date ISO Guide 73 (2002)
- BIP 2154:2008. *Good Governance: A risk-based management systems approach to internal control* (BSI, 2008) is a revision of the earlier BSI publication PD 6668 and deals with managing risk for corporate governance
- HM Treasury *Management of Risk - Principles and Concepts* (HM Treasury, 2004, the "Orange Book") applies to the public service in the UK
- JIS Q 2001 is a Japanese standard on risk management; it had not been reviewed at the time of writing
- CAN/CSA-Q850 is a Canadian risk management standard; it had not been reviewed at the time of writing.

The IRM/ALARP/AIRMIC standard is still available but has not been revised to take account of the new ISO Guide 73 (2009b).

A number of international agreements or similar documents relate to specific aspects of risk management and are of considerable economic, environmental and public health significance. For example, the:

- Article 2.1 of the Terrestrial Animal Health Code (WOAH, 2009) deals with risk associated with the importation of animals and animal products
- World Trade Organisation phytosanitary agreement (WTO, 1997) deals with “measures necessary to protect human, animal or plant life or health” that could act as barriers to trade.

Some documents were reviewed (eg, the NSW Department of Planning, 2000 risk assessment guidelines for hazardous industry planning) but not included as they were both local within a country and dealt with only one aspect of risk assessments.

Variations between standards, documents and research

The COSO and ISO 31000 documents define risk in similar ways with ISO 31000 defining risk as “the effect of uncertainty on objectives” and COSO as “the possibility that an event will occur and adversely affect the achievement of objectives”.

The COSO ERM and ISO 31000 definitions of risk appear quite similar (both refer to objectives, both use similar terms for uncertainty). However, the key difference between the definitions is ISO 31000 is about the likelihood of consequences of an event whereas COSO is about the possibility of an event that may affect achievement of objectives.

Earlier standards and documents based on the ISO Guide 73: 2002 define risk as “the combination of the probability of an event and its consequence” but the UK Treasury “Orange Book” defines risk as “uncertainty of outcome, whether positive opportunity or negative threat, of actions and events. It is the combination of likelihood and impact, including perceived importance”.

Reducing to two predominant non-academic definitions of risk is something of an improvement. However, academic definitions continue to proliferate as noted by Althaus (2005) who noted:

> *Each [academic] discipline applies a particular form of knowledge to uncertainty so as to order its randomness and convert it into a risk proposition*

There are other differences between the two major models and variations of earlier academic and practitioner approaches and definitions continue in older textbooks and articles with new variations continuing to appear. For example:

- Risk evaluation is defined in ISO 31000 as the “process of comparing the results of risk analysis against risk criteria to determine whether the level of risk is acceptable or tolerable” (ie, evaluation follows analysis). A note then states: “risk evaluation assists in the decision about risk treatment”.

- Risk evaluation in COSO is part of risk monitoring and so follows the risk response, risk control and information & communication activities and appears to be more like the review stage in ISO 31000.
- Risk evaluation in the Terrestrial Animal Health Code (WOAH, 2009) is the process of comparing the risk estimated in the risk assessment with the Member's appropriate level of protection. This is broadly comparable with risk evaluation in AS/NZS ISO 31000.

Some recent articles have criticised the COSO ERM model for being too dependent on controls (Blaskovich & Taylor, 2011) and because "lack of organizational realism may be the most significant source of risk" (Martin & Power, 2007). These provided further reasons for considering ISO 31000 to be superior to the COSO model.

Table 1. Analysis of risk management documents

		AS/NZS ISO 31000:2009	IEEE Standard 1540-2001	CEI/IEC 62198: 2001	JIS Q 2001: 2001	BS 6079-3 2000	CAN/CSA-Q850-97	HM Treasury Orange Book	IRM/ALARP/AIRMIC	PMBoK	PRAM	COSO	HSE 5 steps	4Rs	**Terrestrial Animal Health Code**	WTO Sanitary and phytosanitary measures
Planning step	Communicate and consult	✓		✓			✓	✓					(✓)		✓	✓
	Context															
	• Internal	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			(✓)	(✓)
	• External	✓		✓			✓	✓				✓			(✓)	(✓)
	• Risk management	✓	✓	✓	✓			✓	✓		✓				(✓)	
	• Criteria	✓	✓	✓				(✓)		✓		✓			(✓)	(✓)
Risk assessment step	Identify	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	(✓)
	Analyse	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓	✓
	Evaluate	✓					✓	✓				✓	✓		✓	✓
Risk control step	Treat	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
	Monitor and review	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓		✓	✓
	Documentation	✓		✓				✓					✓		✓	✓

Notes to the table

Source: Raz & Hillson (2005) with amendments by author 2008-2012. NB: the table is subject to review and revision to take account of recent versions of standards.

(✓) = implied or partial or different term used

Based on the foregoing comments and analysis in Table 1, it is argued the AS/NZS ISO 31000 process and definitions provide the best available model for risk management because they:

- had been published relatively recently (2009)
- provide generic guidance (see the scope statement on page 1 of the standard)
- are in wide usage (Goy et al., 2012)
- are based on experience in Australia and New Zealand over a 14 year period with the AS/NZS AS/NZS 4360
- (crucially) respond to relevant research evidence.

The following notes discuss some of the research supporting this last claim.

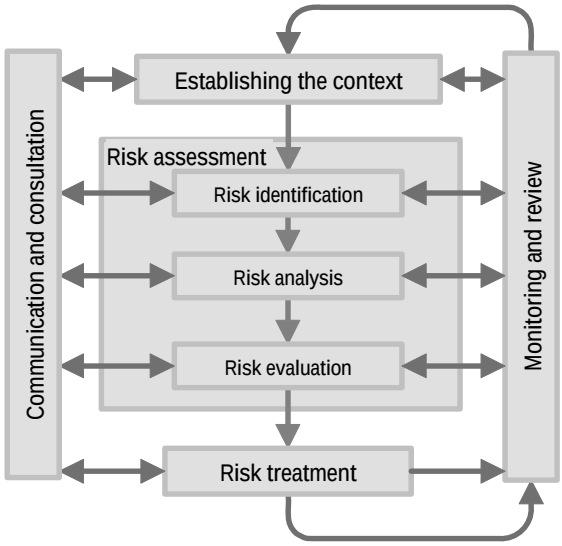
Research evidence

A literature review was carried out using a key word search in the Business Source Complete (EBSCO) and Scopus databases and Google Scholar search engine. The key words used matched the stages in the ISO 31000 risk management process shown in Figure 2. Records already held in the author's Endnote database were also searched. A total of 1686 titles were identified and reviewed and categorised into:

- context
- communication and/or consultation
- risk identification
- risk analysis
- risk evaluation
- risk treatment
- monitoring and/or review.

Some references were in two or more categories and some were categorised using ISO 31000 keywords, not the author-supplied keywords.

Figure 2. Risk management process from ISO 31000



Context

Collier & Woods (2011) used contingency theory to show the importance of the external and internal context to understanding why risk management systems in four local authorities varied in style. Fiegenbaum & Thomas (2004) argued the external context of organisations strongly influenced the organisational culture and attitude to risk.

From an HR perspective, Gould-Williams & Gatenby (2010) found the internal context (eg, structure, culture, leadership style and internal politics) of local authorities strongly influenced the success of team-working activities and thus achievement of organisational objectives.

The community context was found by Hindle (2010) to be significant in the success or failure of an entrepreneurial business.

Experience has shown the author that understanding the current context of an organisation is crucial to effective assessment of risks. This can lead to short- and medium-term projections into the future to anticipate, for example, demographic changes that might create risk (Ballingall & Eaqub, 2012). The use of scenario planning or horizon scanning for long-term planning (Brown, 2007), as popularised by Schwartz (Schwartz, 1996) and others working for Shell in the early 1970s (Cornelius, Alexander, & Mattia, 2005), has been used to develop possible futures, risks and treatment options (Miller & Waller, 2003).

Communication and consultation

Identifying and understanding the needs of stakeholders (Bourne & Walker, 2005) (including during crises, Alpaslan, Green, & Mitroff, 2009) is important if there is to be effective communication and consultation (Frooman, 1999; Hance, Chess, & Sandman, 1989; Johnson & Chess, 2003; Lofstedt, 2011).

The Social Amplification of Risk Framework (SARF) was developed in the 1980s from research showing that context-related factors influence risk assessments (Renn, Burns, Kasperson, Kasperson, & Slovic, 1992). SARF suggested "that psychological, social, institutional and cultural processes can extend or constrain the temporal, sectoral and geographical scales of impacts" and had been used to analyse use of the media by stakeholders (Bakir, 2005).

By 2001, SARF had evolved from a general framework towards being a model with some predictive power and practical utility with the potential to make predictions about the effects of media and public perceptions of risk but has now fallen short of expectations (Breakwell, Barnett, Lofstedt, Kemp, & Glaser, 2001). It remains a useful way of viewing risk communication and consultation needs.

Criteria

Risk criteria are the "terms of reference by which the significance of risk is assessed" and are based on organizational objectives, and external and internal context; they can be derived from standards, laws, policies and other requirements.

An early and well-known applications of criteria was the UK HSE publication *The Tolerability Of Risk From Nuclear Power Stations* (HSE, 1992) which set out conceptual levels of intolerable risk, tolerable risk that should be reduced "as low as reasonably practicable" and acceptable risk.

The HSE approach has now been widely used internationally as a way to set boundaries for risk with negative consequences that are intolerable, risk that must be reduced and risk that is broadly acceptable. It has been applied to, for example, design of the channel tunnel (Geyer, Morris, & Hacquart, 1995), road tunnel safety (Holicky, 2007), societal risks from flooding (Jonkman, Jongejan, & Maaskant, 2011) and tolerable storm damage to coastal properties (Wright, Fisher, & Overton, 2002).

Problems with the use of quantitative risk criteria for fatal accidents in the hydrocarbon and chemical industries have been recognised by many authors (Griffiths, 1981, pp. 54-76; Holden, 1984) and some have argued such criteria are unethical and should not be used (Aven, 2007; Aven & Vinnem, 2005). It has been argued that criteria might be used to bring such risks to the attention of decision-makers who can then decide whether a risk is tolerable using data gathered as part of the risk analysis.

Risk appetite

The term risk appetite is not mentioned in ISO 31000 but is defined in ISO Guide 73. Its use and definition is controversial for some in workers in risk management (see, for example, Purdy, 2012) who argue it should be seen as a subset of risk criteria.

One of the difficulties with risk appetite lies in its definition. While ISO Guide 73 defines it as the "amount and type of risk an organisation is prepared to pursue, retain or take", in the COSO ERM Integrated Framework it is "the broad-based amount of risk a company or other entity is willing to accept in pursuit of its mission (or vision)". However, others use the term in a vague or ill-defined way (Semple, 2007). However, "a problem arises because an organization cannot determine this benchmark. Rather, individual actors within the organization determine the tolerance for risk" (Blaskovich & Taylor, 2011).

A consequent difficulty arises with the use of risk appetite: some authors provide a useful explanation of how to use it while avoiding any definition (Semple, ibid). In some cases, authors call on users to define the term (Chase-Jenkin, Farr, & Lebens, 2010; Kapel, 2011).

On balance, it seems best to develop the risk appetite at a later stage in risk management when the risk profile has been established and risks are understood.

Risk assessment

A key issue in the risk assessment stage is the variability of terms and definitions between standards, documents and authors. Some models do not include risk identification at all or place it separately

from risk assessment. Other models define risk assessment as a stage in risk analysis and some describe risk evaluation as risk assessment.

Logically, it is essential to recognise and name a risk before a detailed examination of its elements can be conducted. Using the understanding of the risk this gives it then becomes possible to form an idea amount or value of the risk and decide if the risk is acceptable "as is".

In this paper it is argued the ISO 31000 model provides the best model for understanding risk and risk management and so the risk assessment stage in risk management uses three steps:

- identification of risk
- analysis of risk
- evaluation of the analysed risk.

ISO 31000 defines risk assessment as "the overall process of risk identification, risk analysis and risk evaluation". Risk identification is defined as the "process of finding, recognising and describing risks". Risk analysis is the "process to comprehend the nature of risk and to determine the level of risk" and provides the basis for risk evaluation and decisions about risk treatment; it includes risk estimation. Risk evaluation is the "process of comparing the results of risk analysis against risk criteria to determine whether the level of risk is acceptable or tolerable" and assists in the decision about risk treatment.

ISO 31000 makes clear that, in the risk analysis stage, "existing controls and their effectiveness and efficiency should also be taken into account".

Literature found to date focuses on techniques that can be applied to the identification, analysis and evaluation of risk.

Risk treatment

Risk treatment is defined in ISO 31000 as the "process of developing, selecting and implementing controls". The standard suggests a hierarchy for developing and then selecting treatment options.

No research-based evidence for the ISO 31000 treatment hierarchy had been found at the time of writing. A further review of decision making literature may find relevant articles.

Monitoring and review

Monitoring and review are defined in broad terms in ISO 31000 and can be seen as activities carried out by the Board or similar and at different levels of management. They may also refer to activities carried out in-house by specialists (eg, internal auditors) or externally (eg, by regulatory agencies as described by Gilliland & Manning, 2002). The German system for mandatory reporting on the risk management framework and process by the external auditor of publicly listed companies is another form of external monitoring (Dobler, 2003).

At the governance level monitoring provides assurance to external investors that expected returns are being delivered. This seems to be true across a wide range of countries and legal requirements for good governance (Bruno & Claessens, 2007).

Relationships between risk management and internal audit have been investigated by a number of authors. Perhaps the most comprehensive, covering 27 organisations in Europe, the USA, Canada, Australia and New Zealand, developed a model encompassing the need to monitor major risks and key controls for governance purposes (Selim & McNamee, 1999).

"Business-as-usual" risks should be monitored by line management leaving senior managers and the Board to keep major risks under review (Drew & Kendrick, 2005; Kaplan & Mikes, 2012) while sovereign finance-related risks need to be monitored at a government level (Irwin & Parkyn, 2009).

Health and safety reporting to the Board (Cross & Locke, 2009)

When some risks eventuate they can become disasters that threaten the continued existence of organisations. Davies & Walters (1998) argued that monitoring the external and internal contexts by experienced staff can help anticipate events.

Data

Data is "facts, opinions and statistics that have been collected together and recorded for reference or for analysis" (Saunders, Lewis, & Thornhill, 2007, p. 595). For risk management purposes, data may

be derived from the context or relate to risks, controls or treatments. Data may be used in communication or consultation or observed as evidence for monitoring or review. As such data is not explored further in this paper other than to note the need to use techniques to gather data that are relevant to the context, stakeholders, risks, controls and treatments under assessment (see, for example, the techniques discussed in ISO, 2009a).

Discussion

Based on the above analysis and review (albeit a very limited review) of the extensive literature and the survey by Goy et al. , it is claimed the ISO 31000 risk management process can be used as a generic model for risk management that contains components commonly agreed to be essential in risk management and that is acceptable to about 50% of users.

The ISO 31000 model makes reasonably clear that communication and consultation are key to:

- understanding of the context of an organisation and the context of the risk management process
- development of risk criteria for the evaluation of risks
- identification, analysis and evaluation of risks
- selection and implementation of risk treatments if risks are found to be unacceptable “as is”.

Similarly, monitoring and review are also key to maintaining a good understanding of risks and how effectively they are being managed. However, the ISO 31000 model does not make clear that monitoring and review should extend to communication and consultation.

The literature review found some good evidence for the components of the model. It is argued the relationship of the components to each other is logical although, as noted, the need to monitor communication and consultation is not explicitly stated.

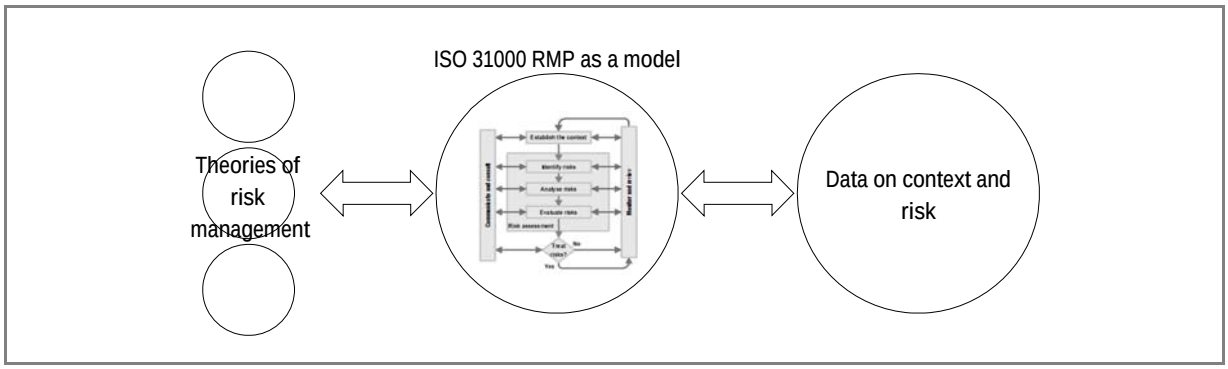
Experience and logic show it is essential to recognise and name a risk before a detailed examination of its elements can be conducted. Using the understanding of the risk this gives it then becomes possible to form an idea amount or value of the risk and decide if the risk is acceptable “as is”. In the language of ISO 31000, this is risk identification, analysis and evaluation and these three components form the risk assessment stage.

Again from experience and logic, if a risk is not acceptable “as is”, some action must be taken to modify it to change the nature or level of the risk. In ISO 31000 terms, this is risk treatment.

Use of a diagram as a model was discussed by Karaca (2012, p. 365) who concluded the use of “non-sentential, visual modes of scientific representation are as essential as sentential (propositional) modes to the production, confirmation and dissemination of scientific knowledge”.

From this review it is argued the risk management process is an epistemological model that acts as a mediator that can explain and predict risk management outcomes (Frigg, Roman, & Hartmann, 2006). The Morrison & Morgan theory/model/data approach has therefore been adapted as shown below in Figure 3.

Figure 3. Revised relationship between theories, models and data



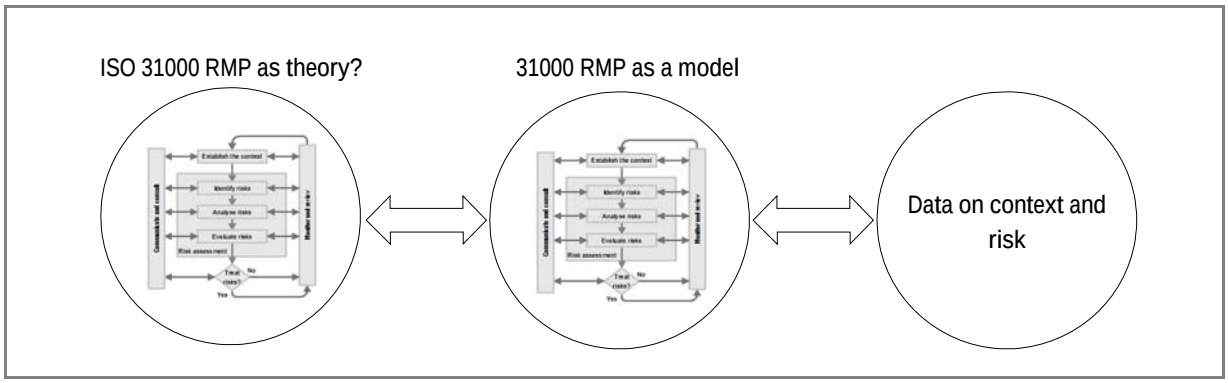
It also became clear there is no general theory of risk management. It is argued this gap is significant because it has left scholars and practitioners to develop narrow and sometimes idiosyncratic risk

management models. Such models might be needed, indeed acceptable, for narrowly focused research or application but they have not contributed to a wider understanding of how risk should be researched or assessed and managed in practice.

It is therefore proposed to further investigate whether the ISO 31000 risk management process might also be assessed as the basis for such a general theory. Such a theory would need to predict and explain the effectiveness of the management of risks.

The place of the ISO 31000 model as theory in the Morrison & Morgan theory/model/data approach is suggested in Figure 4.

Figure 4. Suggested ISO 31000 risk management process as theory and model



Summary of findings

The research to date has found:

- good evidence for inclusion of each component of the ISO 31000 risk management process
- some evidence for cross-linkages between two or more stages
- no evidence for use of specific terms as defined in the standard.

The latter is not regarded as a key issue as definitions and usage of terms is likely to change over time.

References

Alpaslan, C. M., Green, S. E., & Mitroff, I. I. (2009). Corporate Governance in the Context of Crises: Towards a Stakeholder Theory of Crisis Management. *Journal of Contingencies & Crisis Management, 17*(1), 38-49.

Althaus, C. (2005). A disciplinary perspective on the epistemological status of risk. *Risk Analysis, 25*(3), 567-588.

Association for Project Management. (2012). *APM Body of Knowledge*. Princes Risborough, UK: Author. Retrieved from http://www.apm.org.uk/

Aven, T. (2007). On the ethical justification for the use of risk acceptance criteria. *Risk Analysis, 27*(2), 303-312.

Aven, T., & Vinnem, J. E. (2005). On the use of risk acceptance criteria in the offshore oil and gas industry. *Reliability Engineering and System Safety, 90*(1), 15-24.

Bacharach, S. B. (1989). Organizational Theories: Some Criteria for Evaluation. *Academy of Management Review, 14*(4), 496-515.

Baird, I. S., & Thomas, H. (1985). Toward a Contingency Model of Strategic Risk Taking. *The Academy of Management Review, 10*(2), 230-243.

Bakir, V. (2005). Greenpeace v. Shell: media exploitation and the Social Amplification of Risk Framework (SARF). *Journal of Risk Research, 8*(7/8), 679-691.

Ballingall, J., & Eaqub, S. (2012). *Demographic change a force that firms ignore at their peril* (Research Report NZIER Insight 37). Wellington, NZ: New Zealand Institute of Economic Research. Retrieved from http://nzier.org.nz/publications, 19 July 2012

Blaskovich, J., & Taylor, E. Z. (2011). By The Numbers: Individual Bias and Enterprise Risk Management. *Journal of Behavioral & Applied Management, 13*(1), 5-23.

Bourne, L., & Walker, D. (2005). Visualising and mapping stakeholder influence. *Management Decision, 43*(5), 649-660.

Breakwell, G., Barnett, J., Lofstedt, R., Kemp, R., & Glaser, C. (2001). *The impact of social amplification of risk on risk communication* (Research Report CRR 332 Health and Safety Executive). Sudbury, UK: HSE Books. Retrieved from www.hse.gov.uk/research/, 21 February 2004

Brown, D. (2007). Horizon scanning and the business environment — the implications for risk management. *BT Technology Journal, 25*(1), 208-214.

Bruno, V., & Claessens, S. (2007). *Corporate Governance and Regulation: Can There Be Too Much of a Good Thing?* (Research Report 4140). New York: World Bank. Retrieved from http://www.worldbank.org/, 14 April 2009

BSI 6079-3:2000. *Guide to the management of business related project risk* London, UK: British Standards Institution.

BSI BIP 2154:2008. *Good Governance: A risk-based management systems approach to internal control* London, UK: British Standards Institution.

Chase-Jenkin, L., Farr, I., & Lebens, J. (2010). *Risk Appetite: The Foundation of Enterprise Risk Management* (Working Paper). London, UK: Towers Watson. Retrieved from http://www.towerswatson.com/,

Collier, P. M., & Woods, M. (2011). A Comparison of the Local Authority Adoption of Risk Management in England and Australia. *Australian Accounting Review, 21*(2), 111-123.

Cornelius, P., Alexander, V. d. P., & Mattia, R. (2005). Three Decades of Scenario Planning in Shell. *California Management Review, 48*(1), 92-109.

COSO. (2004). *Enterprise Risk Management - Integrated Framework* (Report). Jersey City, USA: Committee of Sponsoring Organizations of the Treadway Commission,

Cross, J., & Locke, S. (2009). Safety reporting to the board. *Journal of Occupational Health and Safety - Australia and New Zealand, 25*(2), 137-143.

Davies, H., & Walters, M. (1998). Do all crises have to become disasters? Risk and risk mitigation. *Disaster Prevention and Management, 7*(5), 396-400.

Dobler, M. (2003). Auditing Corporate Risk Management - A Critical Analysis of a German Particularity. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=540862 on 15 July 2010

Drew, S. A. W., & Kendrick, T. (2005). Risk management: the five pillars of corporate governance. *Journal of General Management, 31*(2), 19-36.

Espejo, R. (1989). The Viable System Model: Interpretations and Applications of Stafford Beer's VSM. In R. Espejo & R. Harnden (Eds.), *The Viable System Model: Interpretations and Applications of Stafford Beer's VSM B2 - The Viable System Model: Interpretations and Applications of Stafford Beer's VSM*. New York: Wiley.

Fehle, F., & Tsyplakov, S. (2005). Dynamic risk management: Theory and evidence. *Journal of Financial Economics, 78*(1), 3-47.

Fiegenbaum, A., & Thomas, H. (2004). Strategic risk and competitive advantage: an integrative perspective *European Management Review, 1*(1), 84-95.

Frigg, Roman, & Hartmann. (2006, 25 June 2012). Models in Science, Stanford University. Retrieved 16 September 2012, from http://plato.stanford.edu/archives/fall2012/entries/models-science.

Frooman, J. (1999). Stakeholder influence strategies. *Academy of Management Review, 24*(2), 191-205.

Geyer, T. A. W., Morris, M. I., & Hacquart, R. Y. (1995). *Channel Tunnel Safety Case: development of the risk criteria.* Paper presented at the International Conference on Electric Railways in a United Europe.

Gill, J., & Johnson, P. (2010). *Research methods for managers* (4th ed.). London, UK: Sage Publications Ltd.

Gilliland, D. I., & Manning, K. C. (2002). When Do Firms Conform to Regulatory Control? The Effect of Control Processes on Compliance and Opportunism. *Journal of Public Policy & Marketing, 21*(2), 319-331.

Gould-Williams, J. S., & Gatenby, M. (2010). The Effects Of Organizational Context And Teamworking Activities On Performance Outcomes. *Public Management Review, 12*(6), 759-787.

Goy, J., Purdy, G., Schanfield, A., Lark, J., Talbot, J. W., du Plessis, J., et al. (2012). Global ISO 31000 survey 2011 [PowerPoint Slide Show]. Paris: G31000. Retrieved from http://www.iso31000survey.com/Global_Survey_ISO_31000_English.pdf

Griffiths, R. (1981). Problems in the use of risk criteria. In R. Griffiths (Ed.), *Dealing with Risk: The Planning, Management and Acceptability of Technological Risk* Manchester, UK: Manchester University Press.

Hance, B. J., Chess, C., & Sandman, P. (1989). Setting a Context for Explaining Risk. *Risk Analysis, 9*(1), 113-117.

Hindle, K. (2010). How community context affects entrepreneurial process: A diagnostic framework. *Entrepreneurship & Regional Development, 22*(7/8), 599-647.

HM Treasury. (2004). *Management of Risk - Principles and Concepts* (Guidance Note). London, UK: Author. Retrieved from http://www.hm-treasury.gov.uk/orange_book.htm, 12 January 2005

Holden, P. L. (1984). Difficulties in formulating risk criteria. *Journal of Occupational Accidents, 6*(4), 241-251.

Holicky, M. (2007, Jun 25-27). *Optimization of risk criteria for road tunnels.* Paper presented at the 2nd International Conference Safety and Security Engineering, Malta.

HSE. (1992). *The Tolerability Of Risk From Nuclear Power Stations*. Sudbury, UK: HSE Books.

HSE. (2011). *Five Steps to Risk Assessment* (Advisory Paper INDG163(rev1)). Sudbury, UK: HSE Books,

IEC 62198 [draft]:2012. *Managing risk in projects – Application guidelines* Geneva: International Standards Organisation.

IEEE 1540:2001. *Standard for Software Life Cycle Processes – Risk Management*: Institute of Electrical and Electronic Engineers.

Irwin, T., & Parkyn, O. (2009). *Improving the Management of the Crown's Exposure to Risk* (Working Paper WP 09-06). Wellington, NZ: The Treasury. Retrieved from http://www.treasury.govt.nz/publications/research-policy/wp/2009/09-06/, 10 October 2009

ISO Guide 73:2002. *Risk management - vocabulary - guidelines for use in standards* Geneva, Switzerland: International Standards Organisation.

ISO 31010:2009a. *Risk Management - Risk Assessment Techniques* Geneva, Switzerland: International Standards Organisation.

ISO Guide 73:2009b. *Risk management - vocabulary - guidelines for use in standards* Geneva, Switzerland: International Standards Organisation.

ISO 31000:2009c. *Risk management – Principles and guidelines* Geneva: International Standards Organisation.

Johnson, B. B., & Chess, C. (2003). Communicating Worst-Case Scenarios: Neighbors' Views of Industrial Accident Management. *Risk Analysis, 23*(4), 829-840.

Jonkman, S. N., Jongejan, R., & Maaskant, B. (2011). The Use of Individual and Societal Risk Criteria Within the Dutch Flood Safety Policy-Nationwide Estimates of Societal Risk and Policy Applications. *Risk Analysis: An International Journal, 31*(2), 282-300.

Kapel, A. (2011, June). Hungry? Why you should develop a risk appetite statement. *Insights*. Retrieved from http://www.towerswatson.com/

Kaplan, R. S., & Mikes, A. (2012). Managing risks: a new framework. *Harvard Business Review, 90*(6), 48-60.

Karaca, K. (2012). Philosophical reflections on diagram models and diagrammatic representation. *Journal of Experimental & Theoretical Artificial Intelligence, 24*(3), 365-384.

Kloman, F. (2010). A brief history of risk management. In J. Fraser & B. Simkins (Eds.), *Enterprise Risk Management - Today's Leading Research and Best Practices for Tomorrow's Executives* (pp. 19-30). New Jersey: Wiley.

Lofstedt, R. (2011). Communicating Food Risks in an Era of Growing Public Distrust: Three Case Studies. *Risk Analysis*, no-no.

MacKinnon, D., Coxe, S., & Baraldi, A. (2012). Guidelines for the Investigation of Mediating Variables in Business Research. *Journal of Business & Psychology, 27*(1), 1-14.

Martin, D., & Power, M. (2007). *The End of Enterprise Risk Management* (Working Paper 07-22). AEI-Brookings Joint Center For Regulatory Studies,

Meulbroek, L. (2002). The Promise and Challenge of Integrated Risk Management. *Risk Management and Insurance Review, 5*(1), 55-66.

Miller, K., & Waller, G. (2003). Scenarios, Real Options and Integrated Risk Management. *Long Range Planning, 36*(1), 93-107.

Morrison, M., & Morgan, M. (1999). Models as mediating instruments. In M. Morgan & M. Morrison (Eds.), *Models as mediators: perspectives on natural and social science* (pp. 10-37). Cambridge, UK: Cambridge University Press.

NSW Department of Planning. (2000). *Risk Assessment* (Hazardous Industry Planning Advisory Paper HIPAP No. 3). Sydney, Australia: New South Wales Government. Retrieved from http://www.shop.nsw.gov.au/, 4 March 2004

PMI 2008. *The Standard for Portfolio Management* Pennsylvania: Project Management Institute.

Purdy, G. (2012). *Demystifying risk appetite*. Paper presented at the SOPAC 2012 conference, 4-7 March 2012, Sydney. Institute of Internal Auditors.

Raz, T., & Hillson, D. (2005). A Comparative Review of Risk Management Standards. *Risk Management: an international journal, 7*(4), 53-66.

Renn, O., Burns, W. J., Kasperson, J. X., Kasperson, R. E., & Slovic, P. (1992). The Social Amplification of Risk: Theoretical Foundations and Empirical Applications. *Journal of Social Issues, 48*(4), 137-160.

Saunders, M., Lewis, P., & Thornhill, A. (2007). *Research Methods for Business Students* (4th ed.). Harlow, UK: Pearson Education Ltd.

Schwartz, P. (1996). *The Art of the Long View*. New York: Doubleday.

Selim, G., & McNamee, D. (1999). The risk management and internal auditing relationship: developing and validating a model. *International Journal of Auditing, 3*(3), 159-174.

Semple, B. (2007). Risk Appetite: How Hungry Are You? *Accountancy Ireland, 39*(3), 24-27.

Servaes, H., Tamayo, A., & Tufano, P. (2009). The Theory and Practice of Corporate Risk Management. *Journal of Applied Corporate Finance, 21*(4), 60-78.

Simon, H. A. (1979). Rational Decision Making in Business Organization. *American Economic Review, 69*(4), 493-513.

Soanes, C., & Stevenson, A. (Eds.). (2008) The Concise Oxford Dictionary (11th ed.). Oxford, UK: Oxford University Press Ltd.

Tworek, P. (2012). Integrated risk management in construction enterprises - theoretical approach. *Journal of Economics & Management, 8*, 125-135.

WOAH. (2009). *Terrestrial Animal Health Code* (International agreement). Paris: World Organisation for Animal Health. Retrieved from http://www.oie.int/eng/normes/Mcode/en_sommaire.htm, 21 February 2011

Woods, M. (2009). A contingency theory perspective on the risk management control system within Birmingham City Council. *Management Accounting Research, 20*(1), 69-81.

Wright, L. E., Fisher, J. S., & Overton, M. F. (2002). *Development of risk criteria for storm damage to oceanfront structures.* Paper presented at the Solutions to Coastal Disasters 2002. Retrieved from https://www.scopus.com/scopus/inward/record.url?eid=2-s2.0-0036388761&partnerID=40

WTO. (1997). *Agreement on the application of sanitary and phytosanitary measures* (International agreement). Geneva: World Trade Organisation. Retrieved from https://www.wto.org/english/docs_e/legal_e/15-sps.pdf, 5 August 2012