Knowledge risk management: a framework

Peter Massingham

Peter Massingham is Director of the Centre for Knowledge Management, University of Wollongong, Wollongong, Australia.

Abstract

Purpose – *There has been increased interest in application of knowledge management (KM) in managerial issues as a way of demonstrating the field's value. There has also been an increasing focus on risk management (RM) in response to growing organisational awareness of corporate and social responsibilities. This paper seeks to contribute to the emergence of a new field of research – referred to as knowledge risk management (KRM), which applies KM tools and techniques to the management of organisational risk.*

Design/methodology/approach – *The approach takes the form of building on an empirical study of the Australian Department of Defence using case study methods.*

Findings – *The paper examines how conventional approaches to risk management based on decision tree methods are ineffective, and proposes and tests an alternative KRM model.*

Research limitations/implications – *A limitation is that the paper is based on a single case study.*

Originality/value – *The model provides managers with a way to differentiate amongst risks and prioritise for action. Its main value is to reduce the cognitive bias inherent in traditional decision methods for risk assessment. The KRM model improves the accuracy of risk assessment by reducing subjectivity caused by cognitive bias.*

Keywords *Knowledge management, Risk management*

Paper type *Research paper*

In recent years, corporate disasters, such as the collapse of Enron, have heightened the need for effective corporate governance, while catastrophic natural disasters, such as the tsunami of 2004, and man-made tragedies, such as the September 11 terrorist attacks, have increased awareness of risk and its consequences (see Otterson, 2005; Liesch *et al.*, 2006). A recent survey found that 81 percent of organisations feel they are vulnerable to a serious operational incident (Taub, 2002). The consequences of poor risk management – such as financial loss, safety violations, unethical behavior – are significant. Researchers have found that inadequate government regulation, poor internal controls, and misalignment of firm incentives are to blame (Marshall *et al.*, 1996). It is increasingly common for senior executives, held to account for corporate disasters, to plead ignorance (Neef, 2005). However, large institutional investors, which own 75 percent of the world's publicly listed companies' shareholdings, are no longer willing to accept that executives do not know what is going on in their organization (Emblemsvag and Kjolstad, 2002). Knowledge informs decision makers and improves the manageability of risk (Verhaegen, 2005).

Organizational risk management has typically been grounded in classical decision theory, where risk at a macro level is regarded as reflecting variation in the distribution of possible outcomes, their likelihoods, and their subjective values (March and Shapira, 1987). This approach is based on determining what the risk actually is, predicting the probability and the consequence and outcomes of that risk, deciding what path to take to either avoid or take

Received 14 June 2009
Accepted 19 October2009

the risk, and finally, developing and implementing strategies to respond to the risk (De Zoysa and Russell, 2003). However, some researchers argue that the normative approach of decision trees is ineffective due to environmental complexity and individuals' cognitive constraints (Adams, 1995). This paper presents a detailed discussion of the way the Royal Australian Navy (RAN) manages technical risk. The RAN offers an interesting case study for this research context because many of its activities may be considered risky and the consequences of poor risk management are significant: in terms of personnel safety, the environment, and national security. The RAN also provides an excellent opportunity to compare the traditional methods of organisational risk management with alternative methods.

The RAN has adopted a risk management approach based on two principles. The first principle is that levels of risk are identified using a Hazard Risk Index (HRI). The HRI uses a traditional decision tree method in that it estimates the likelihood and consequences of a risk event occurring. The second principle is that risk is managed by accredited individuals known as Competent Authorities (CAs). The paper will illustrate the strengths and weaknesses of the RAN's risk management approach. On the one hand, the RAN has done an excellent job to reduce cognitive error by aligning risk management with competency. This ensures that decision makers have necessary knowledge to anticipate and respond to risk. On the other hand, we will see that the RAN faces a new threat – the sheer volume of technical decisions – which makes it difficult for individuals to prioritize risks.

Knowledge risk management (KRM) is an emerging field which offers a solution to the problems associated with conventional risk management methods. The problem of environmental complexity is manifested by individuals not knowing enough about the risk to anticipate its likelihood and consequences. Environmental complexity creates uncertainty. Knowledge moves individuals along the spectrum of uncertainty towards certainty; making risk a 'learnable' rather than an entirely random event (Apgar, 2006). The problem of cognitive constraints is caused by subjectivity. Subjectivity is manifested in two ways. First, individuals' do not perceive risk in the precise logic of decision theory (cited in March and Shapira, 1987). The brain does not work in the way decision trees suggest it should. Second, individuals vary in their perception of reality. Knowledge can increase objectivity by training individuals to process risk the same way (e.g. HRI), and by providing individuals with better tools for understanding the nature of risk. This paper contributes to KRM theory by developing a decision support tool, i.e. conceptual model, to help this latter point. In this way, the paper provides a solution to the problem of cognitive constraints presented by conventional decision tree methods, by using KM tools and techniques to enable individuals to generate deeper insight about the real nature of organizational risk.

Literature review

Risk management theory

The word risk derives from the early Italian word *risicare*, which originally means ''to dare'', and, in this sense, risk is a choice rather than a fate (Bernstein, 1996). The early literature on entrepreneurship (Schumpeter, 1934) discussed risk as a good thing and risk taking was a positive action leading to market innovation. The most common contemporary view is that risk infers the possibility that something may go wrong. *The Stanford Encyclopedia of Philosophy* (2007) explains that risk is an unwanted event with negative consequences. Individual response to risk depends upon whether you feel it is entirely random or can be managed. Management researchers tend to take the latter position. This view argues that even if we cannot eliminate risk, we can at least anticipate it, and then put in place processes that may reduce its impact.

While conventional approaches to risk management, e.g. decision tree methods, still prevailed at our case study organization, recent research has argued against the utility of taxonomies and sole reliance of experts for effective organizational decision making. For example, Mercer *et al.* (2005) explains that the risk management literature argues for an analytic and deliberative strategy that promises better exchange of tacit knowledge. The

researchers explain that a new field called ''post-normal risk management'', requires ''dialogue among those who have an interest in the issue and are committed to its solution. It also suggests that the process towards a decision may be as important as the details of the decision that is finally achieved'' (Funtowicz and Ravetz, 1993, cited in Mercer *et al.* (2005)).

Post-normal risk management suggests the need to consider the interaction of individuals, as part of an organizational collective. Rather than framing risk management as an individual cognitive process bounded by the individual's knowledge, post-normal risk management argues that risk should be discussed by subject matters experts, which extends the boundaries of what is known about the risk. The contribution of knowledge management, from this perspective, is to examine the nature of the social interaction within this social setting of experts, e.g. through social network analysis (e.g. see Mischen and Jackson, 2008). Knowledge management theory can help through examining the nature of the tacit knowledge being exchanged by these experts and the processes involved in the social interaction.

Researchers have recently proposed complexity theory as a way to explain how cognition happens in social systems (McElroy, 2003), which has been lacking in knowledge management theory (Mischen and Jackson, 2008). Some researchers have suggested that complexity theory helps us understand the feedback processes leading to improved decision making in areas such as risk management (e.g. see Choo, 1998, Sherif, 2006). However, our view is that complexity theory's main contribution to risk management is in setting appropriate boundaries around the cognitive processes and the social setting of the expert group.

Boundaries define what issues are to be included, excluded or marginalized in analyses (cognitive limits) and who is to be consulted or involved (social limits) (see MacGillivray, 2007; Midgley, 2008). Decisions on appropriate boundaries involve value judgments grounded in an activity (Midgley, 2008). Effective boundary setting can reduce complexity by limiting the range of available possibilities (Seidl, 2007). In this way, encouraging discussion amongst suitable experts associated with the risk event, can broaden the general possibilities of the social system, i.e. the number of risk events and their consequences called secondary complexity; and reduce the number of unavailable possibilities, i.e. the unknown or what Seidl (2007) calls ''non-knowledge''. In this way, complexity theory from a system thinking perspective helps us understand how expert discussion can increase the range of the known (available possibilities) and reduce the size of the unknown (unavailable possibilities).

Knowledge risk management

Knowledge risk management (KRM) is an emerging field of academic enquiry. It intersects two previously separate fields: risk management (RM) and knowledge management (KM). Researchers argue that knowledge is necessary to comprehend and manage the risk. Previous KRM research has two main themes. First, researchers evaluate how knowledge can reduce risk leading to better risk management. Examples of this research include De Zoysa and Russell (2003) who examined how knowledge can assist risk identification, risk quantification, and risk response; and Verhaegen (2005) and Otterson (2005) who consider how knowledge informs decision makers. Second, researchers examine how the process of knowledge management can improve risk management. Examples of this research include Marshall *et al.* (1996) who identifies a series of KM ''levers'', such as transferring knowledge to decision makers, improving accessibility of knowledge, embedding knowledge in controls and systems, as a way of avoiding the financial catastrophes caused by poor RM. Some researchers try to explain the similarities between RM and KM; such as the need for employee insight, the importance of action, the value of lessons learned, and conclude that risk management is knowledge management (cited in Neef, 2005). These researchers propose common KM techniques such as knowledge mapping, communities of practice, ''hard tagging'' experts as the basis of a new KRM approach.

Our contribution

Previous KRM research explores how knowledge and knowledge management can help risk management (RM), but mainly from the perspective of informing decision makers. The KRM field has not addressed the two main problems associated with RM: environmental uncertainty and cognitive constraints. It might be argued that KRM researchers are trying to address the first problem – environmental complexity – by using KM tools and techniques to reduce uncertainty, and make risk ''learnable'', but the researchers fail to make this connection explicit. The contribution of this paper is to address the second problem – cognitive constraints – which has been ignored by KRM researchers.

Methods and data

Method

The aims of the study were addressed through the case study method of empirical enquiry. The reasons for this are as follows. First, exploratory fieldwork is essential in ''new'' areas of research which lack an extant body of both theory and data (Eisenhardt, 1989). Second, qualitative studies are necessary where organizational processes, such as the relationship between risk and knowledge, are involved which do not lend themselves easily to quantitative measures (Van Maanen, 1979). The organisation used as the case study, which we call EngServ, is part of the Australian Department of Defence. It is primarily responsible for managing technical risk. EngServ had 33 staff at the time of survey. A total of 31 staff (94 percent) completed a survey which contained questions about the work done at EngServ, the risk factors involved, and their perception of the significance of these risks using a decision tree method (HRI) and the KRM method proposed in this paper. While this is a relatively small sample based on a single case study, the results offer a rich narrative that may be used to develop theory. Single case studies are often reliable sources of empirical data (Eisenhardt, 1989), and ''are likely to produce the best theory'' (Walton, 1992, p. 129). Recent research in managerial decision making has been based on a single case study (see Douglas, 2006). This paper is an exercise in theory development, which may be followed by further research to test the theories presented here.

Data context

As with any Defence Force, the RAN is involved in many activities that may be considered risky. The RAN controls a large and expensive physical infrastructure, e.g. ships, which play a crucial role in Australia's national security. The consequences if something goes wrong are significant. In managing these risks, the RAN has traditionally focused on the technical integrity of naval materiel during all aspects of the design and construction stages (acquisition) and the sustainment and maintenance stages (in-service support). Much of the management of technical risk has been outsourced to industry. EngServ represents the last remnants of the RAN's internal engineering capability for surface ships and, as such, plays a crucial role in ensuring the RAN is an intelligent customer of industry.

For many years, the Australian Government employed a capability to design, build, and maintain ships. However, policy changes have gradually eroded the RAN's engineering capability; including the privatization of Government owned factories and dockyards, and contracting out of in-house engineering, design, and maintenance services. RAN engineering and technical staff numbers have decreased dramatically. In the early 1990s, there were about 700 naval engineers working for the Department of Defence, and 15 years later there are less than 100. This has had significant implications for the RAN's risk management. First, there was a substantial decrease in the Navy's stock of technical knowledge. Second, there was a heavy dependence on contractors (private industry) to do the work that was previously done by the RAN. Third, there were concerns about the capability of industry to maintain technical integrity of RAN materiel. Fourth, the RAN's ability to be an intelligent customer of industry was declining to the point where some worried whether it could still ensure contractors were performing their role. The shift in technical responsibility from the public to the private sector raised alarm bells. Critics of the

outsourcing argued that contractors did not understand the operational requirements of naval vessels, which were very different from commercial vessels; and that contractors did not have sufficient depth of knowledge to understand the complexity of naval vessels and their operational environment.

Analysis

The analysis section has three purposes: first, to present the way the RAN manages technical risk using conventional decision tree methods; second, to develop an alternative method based on knowledge management constructs; and third, to test the method on EngServ respondents.

Decision tree method

The Technical Regulatory System. In 2001, the RAN responded to the need for improved risk management by introducing its Technical Regulatory System (TRS). The TRS aimed to provide assurance to the Chief of Navy that the technical integrity of naval materiel is maintained from design inception to disposal, i.e. the full life of the asset. EngServ were the RAN's only internal engineering resource. The corner-stone of the TRS was the concept of Competent Authorities (CAs). To gain accreditation as a CA, staff had to be authorised as having the qualifications, experience and demonstrated technical competence required for the work being performed. The RAN recognized that there is high staff turnover in the Defence industry. To counter this, accreditation was linked to positions rather than individuals. The RAN identified levels of technical decisions based on the level of risk involved. The decisions with the highest risk were allocated to the most senior positions. Staff in positions at lower levels were not allowed (i.e. accredited) to make the highest risk decisions. The structure adopted by the RAN articulated six levels of technical proficiency similar to that defined by the Australian Qualification Framework (AQF). These levels are applied to specific technical positions within each CA. Normally each position required a general level of competency and specific discipline requirements. This shows how the TRS used competency frameworks to manage risk through the technical decisions defined by position descriptions. It ensured that individuals only made decisions in areas where they had demonstrated competence. Importantly, the RAN process focuses risk assessment on the individual, and risk is rarely discussed as a group of experts, so we must use conventional decision tree theory to examine what is happening, rather than contemporary theories such as post-normal risk management and complexity theory.

Hazard Risk Index. The RAN introduced a Hazard Risk Index (HRI) which ranked technical decisions in terms of their risk levels. The HRI aimed to reduce the subjectivity of individual assessment by broadly categorizing risk into four levels of acceptability: intolerable, unacceptable, acceptable with continuous review and acceptable with periodical review. Risks are assessed based on the probability of the risk occurring and the consequence or impact on the activity if the risk occurs. The probability indicators are defined by Table I and the consequences indicators are defined by Table II.

These two dimensions were combined using a two dimensional matrix to allocate a Hazard Risk Severity Score (see Figure 1).

Table I Risk likelihood

Description	*Individual event*
Frequent	Likely to occur regularly
Probable	Will occur several times
Occasional	Unlikely but can be reasonably expected to occur
Remote	Unlikely but possible to occur
Improbable	So unlikely it may not be experienced

Table II Risk consequence

Description	*Definition*
Catastrophic	Failure would prevent the organization from meeting the primary operational requirements
Critical	Failure would significantly degrade the organization's ability to perform its primary mission
Major	Failure would result in temporary loss of one or more significant capabilities within the organization
Minor	Failure would result in temporary degradation or loss of one or more capabilities within the organization

Figure 1 Hazard Risk Severity Score (HRSS) level for the RAN

The Hazard Risk Severity Score (HRSS) were then classified in terms of the level of risk to produce a Hazard Risk Index (HRI) (see Figure 2).

The capacity to differentiate amongst the level of risk was an essential component of the TRS. In this way CAs can delegate technical decisions to others, using the HRI scale, making the process manageable. Second, staff training as part of the accreditation process meant that the Level 2 delegates in any CA would have similar interpretations of the various HRI categories. In this way, individuals had clear lines of demarcation, as illustrated by (see Table III). It is important to note that terms such as ''intolerable'' and ''unacceptable'' risk were defined by EngServ, are used as part of the normal language of risk assessment, and all staff trained in risk management develop a common understanding of these terms.

The new threat: high volume decision environments. In practice, problems were created by the sheer volume of work which RAN Competent Authorities (CAs) had to deal with and the process of delegated authority. A CA might receive hundreds of requests for technical decisions each year. If a request was considered a low priority, it would be placed at the bottom of an in-tray. It often took up to six months for a decision and in extreme cases some decisions had been delayed by three years or more. The problems were created because there was no adequate means for prioritising work. Managers would allocate work based on three principles: order of receipt (i.e. first-in-first-served), perceptions of risk levels (e.g. catastrophic), and customer urgency (i.e. who screams loudest). The result was a very

Figure 2 Hazard Risk Index (HRI) level for the RAN

Acceptability of risk by Hazard Risk Index (HRI)		
HRSS	**Risk Level**	**Risk Acceptability**
1 to 5	High	Intolerable
6 to 9	Medium	Unacceptable
10 to 20	Low	Acceptable with review

Table III Levels of authority by risk

Risk/hazard category	*Decision or authority level*	*Equivalent APS level*
Cat 1 – intolerable	Level 1	CNE
Cat 2 – unacceptable	Level 2	Director/Deputy Director
Cat 3 – acceptable (10-13)	Level 3 and 4	Senior Engineer/Engineer
Cat 4 – acceptable (14-16)	Level 4 and 5	TO4
Cat 5 – acceptable (17-20)	Level 6	TO4/TO3

Note: The numbers in parentheses in column 1 represent the risk rating (see the Figure 1 quadrants)

reactive organisational culture that created a sense of panic. This compounded the cognitive biases of managers through variable anxiety levels caused by feelings of stress, being overloaded, and customer pressure. Within this environment, it is easy to see how mistakes could be made and matters that were very serious could be overlooked or unnecessarily delayed. It also created a focus on operational issues at the expense of strategic activities. Staff constrained by time focused on doing technical work and often ignored activities seen as 'non-core', such as human resource management. Managers had no way to differentiate amongst technical work and also no idea how to compare technical versus management activities.

Conceptual development

This research aimed to examine the validity of decision tree methods for managing organisational risk; and to develop an alternative risk management method derived from knowledge management constructs. Previous research has argued that traditional methods are ineffective (Fischhoff *et al.*, 1984). Our aim was to understand more about why decision tree methods do not work, and to use this knowledge to develop an alternative method. Our alternative is grounded in an emerging field of research, knowledge risk management (KRM), which uses knowledge management constructs to help differentiate the nature of organisational risk and prioritise for action. Our conceptual model aimed to improve upon existing decision tree methods by addressing cognitive constraints. The knowledge management literature provides three constructs we can use in the development of our conceptual model: individual, knowledge, and organizational characteristics.

Individual characteristics

Our individual characteristic is grounded in the construct of intellectual capital (IC). Intellectual capital (IC) represents the collective knowledge that is embedded in the

personnel, organizational routines and network relationships of an organization (Bontis, 2002). The concept of IC encompasses three primary interrelated components: human capital (HC), structural capital (SC) and relational capital (RC) (Stewart, 1997). This research focuses on the risks associated with human capital.

There are two risks associated with the inputs to the firm's human capital: ineffective recruitment and inefficient training. Ineffective recruitment is determined by the organisation's ability to attract suitably qualified staff, which we define as Necessary Qualification Levels (NQL). NQL is measured by the levels of pre-requisite knowledge (i.e. qualifications) necessary to manage the risk factor (i.e. the unwanted event). The higher the qualification levels, the more difficult it will be to recruit, and vice versa. The higher the qualifications, the greater the risk that human capital cannot be bought. Inefficient training is determined by the length of time necessary to train staff, which we define as Time To Learn (TTL). TTL is measured by the time required to develop necessary human capital. The more time required to learn, the greater the risk that human capital cannot be developed. We derived codes for each activity on a scale of 1 to 5 (see Figure 3).

Knowledge characteristics

Our knowledge characteristic is grounded in the construct of knowledge transfer barriers. There is a large literature on this topic (see von Hippel, 1994; Szulanski, 1996) In discussing the transferability of knowledge resources, researchers typically distinguish between codified (explicit) or tacit (implicit) knowledge. Tacit knowledge is valuable, difficult to transfer, and highly context dependant (Nonaka, 1994). It explains the ''accumulated practical skill or expertise that allows one to do something smoothly and efficiently'' (Kogut and Zander, 1995). It is commonly referred to as the knowledge in people's heads. Researchers agree that the most important knowledge is tacit (Nonaka and Takeuchi, 1995) but that the transfer of tacit knowledge between organizational members is exceptionally difficult (Grant, 1996). Codified knowledge, on the other hand, is stored in databases, reports, and policies. It is easily captured and accessible. A second knowledge transfer barrier is complexity. This influences comprehension and whether the receiver can understand the knowledge being transferred. There are three levels of complexity (Schulz,

Figure 3 Individual characteristics risk matrix

Necessary Qualifications (NQL)

Length of time to learn (TTL)	1 = Postgraduate university	2 = Undergraduate university	3 = TAFE	4 = Technical	5 = None necessary
1 = Years of on-the-job experience	1	3	10	15	20
2 = Several months working with knowledgeable staff member	2	5	11	16	21
3 = A training course	4	7	12	17	22
4 = A short session with knowledgeable staff member	6	9	14	19	24
5 = No time at all (know what to do)	8	13	18	23	25

Intolerable
Unacceptable
Acceptable

2001). Some knowledge is simple. It is codified and easily transferred to others. Examples include market research data and firm policies. The next level of knowledge is re-combined with the firm's existing stock of knowledge. Examples include firm strategy, marketing, and technical knowledge involved with new product development. The process of combining the knowledge of staff from different functional areas can create a small incremental increase in knowledge for the firm. The most complex knowledge is idea creation and problem solving involving ill-structured and unknown cause and effect relationships. Examples include business process improvements, large scale investments, or new business initiatives. These activities are often non-routine and require an iterative process of learning at multiple levels within the organization.

There are two risks associated with knowledge resources: tacitness and complexity. For this study, tacitness is determined by the location of the knowledge necessary to manage the risk factor, which we define as Receiver Transfer Access (RTA). RTA is measured by the degree to which individuals who need knowledge can access it. If the knowledge necessary to manage the risk is only found in people's heads, i.e. tacit knowledge, then the organisation is vulnerable if they are unavailable. Alternatively, if the necessary knowledge is codified and readily accessible, the risk of not knowing what to do if something goes wrong is much lower. RTA may be identified by asking respondents the following question: Where is the knowledge necessary for managing the risk factor? This measures the possibility that knowledge will become ''stuck'' with an individual and, therefore, somewhat inaccessible to others. We derived codes for each activity on a scale of 1 to 5 (see Figure 4).

Complexity is determined by the amount of new knowledge that must be created to manage the risk factor, which we define as Degree of Creativity (DoC). DoC is measured by levels of knowledge. If the knowledge necessary to manage the risk is highly complex, then the organisation is vulnerable because if it is lost or otherwise unavailable it must be recreated. Alternatively, if the necessary knowledge required is simple, it is likely to be more easily replaced. Deeper levels of knowledge require more time to learn and, therefore, increase the possibility of inaction, i.e. when no-one knows what to do. DoC may be identified by asking respondents the following question: How much new knowledge would typically be required

Figure 4 Knowledge characteristics risk matrix

Complexity (DoC)

Type of knowledge (RTA)	1 = True innovation i.e. complex problem solving	2 = New knowledge is created	3 = Recombined with person's current stock of knowledge	4 = Added to person's current stock of knowledge	5 = No knowledge creation
1 = Stays in people's heads	1	3	10	15	20
2 = Discussed by social networks	2	5	11	16	21
3 = Shared in formal discussions	4	7	12	17	22
4 = Written in operating procedures	6	9	14	19	24
5 = Part of routine training courses	8	13	18	23	25

Intolerable
Unacceptable
Acceptable

for an individual to learn how to manage that risk factor? We derived codes for each activity on a scale of 1 to 5 (see Figure 4).

Organisational characteristics

Our organisational characteristic is grounded in the construct of absorptive capacity. In their review of the literature on absorptive capacity, Zahra and George (2002) found there were three key definitions. First, Cohen and Levinthal (1990) introduced the concept of absorptive capacity as ''the firm's ability to value, assimilate and apply new knowledge''. Second, Mowery and Oxley (1995) defined it as a broad set of skills needed to deal with the tacit component of transferred knowledge and the need to modify this imported knowledge. Third, Kim (1998) defines it as the capacity to learn and solve problems. Zahra and George (2002) build on this earlier research by proposing an input-output model based on potential and realized absorptive capacities. They argue that absorptive capacity begins with ''potential capacity''. This comprises knowledge acquisition and assimilation capabilities. It ends with ''realized capacity'' which focuses on knowledge transformation and exploitation. In this framework, the ''input'' is the firm's ability to learn from knowledge transfer and the ''output'' is the capacity to use the knowledge.

There are two risks associated with the firm's absorptive capacity: insufficient potential capacity and inadequate realised capacity. Insufficient potential capacity is determined by the organisation's stock of knowledge, which we define as Risk Management Capability (RMC). RMC is measured by the proportion of staff with the necessary knowledge to manage the risk factor (i.e. the unwanted event). If only one or a relatively few staff have sufficient knowledge, the organisation has low RMC. It is vulnerable if these staff leave the organisation or are unavailable for any reason. RMC may be identified by asking respondents the following questions: What does the organisation do to manage the risk? What do you need to know to do this? Who does this? Who else knows how to do this? The final question measures the possibility of someone else replacing the person responsible for managing the risk. The more staff with relevant knowledge, the more likely that someone may be found to anticipate or respond to the risk factor. Codes were derived for each activity on a scale of 1 to 5 where 1 = less than 5 percent of staff have necessary knowledge, and 5 = more than 50 percent of staff have necessary knowledge (see Figure 5).

Inadequate realised capacity is determined by the organisation's willingness to allocate staff resources, which we define as risk management motivation (RMM). RMM is measured by the degree to which the organisation replaces staff required to manage the risk factor. Knowledge is about action and it must be put to some use in order to create value (cited in Nonaka and Takeuchi, 1995). The organisation might have many staff who know what to do to manage the risk factor (i.e. high RMC), but not release them to perform this role or the staff themselves may be unwilling to take on this role. RMM may be identified by asking respondents the following question: What will happen if the individual(s) normally responsible for managing the risk factor becomes unavailable? This measures the likelihood of the organisation taking action. We derived codes for each activity on a scale of 1 to 5 (see Figure 5).

Conceptual model

The conceptual model presented by this paper has three steps. The first step is to calculate the level of risk associated with each of the organization's main activities. This follows a conventional decision tree method, i.e. the likelihood and consequences of an unwanted event occurring (HRI), with the addition of a weighting based on the relative importance of each activity. The second step is to calculate the level of risk associated with the knowledge necessary to manage the risk factors for each activity. The third step is to prioritise risks for action by considering the outcomes of step one and step two in isolation and then in combination. Figure 6 presents the conceptual model. The letters in brackets represent the columns outlined later in Table IV.

Figure 5 Organisation characteristics risk matrix

What happens if knowledge is lost? (RMM)

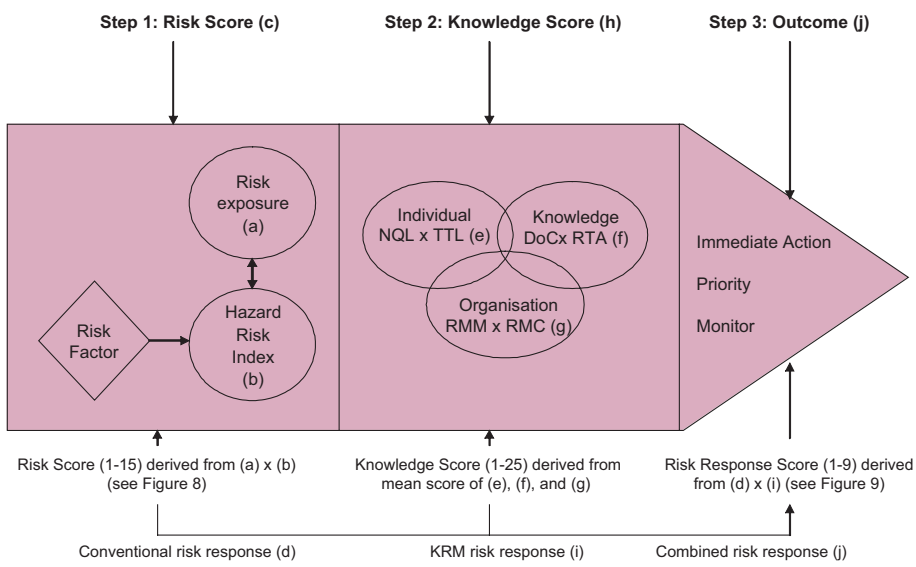
Proportion of staff with knowledge (RMC)	1 = Person would not be replaced & the work would not get done	2 = Person is replaced & work is done poorly	3 = Person is replaced & work is done satisfactorily	4 = Person is replaced & work is done well	5 = Person is replaced & work is done very well
1 = < 5%	1	3	10	15	20
2 = 5-10%	2	5	11	16	21
3 = 11-20%	4	7	12	17	22
4 = 21-50%	6	9	14	19	24
5 = > 50%	8	13	18	23	25

Intolerable

Unacceptable

Acceptable

Figure 6 Knowledge risk management: a conceptual model



Research findings

The research findings are presented in the following way. First, we calculate a risk score for each EngServ activity based on traditional decision tree methods (Step 1 in Figure 6). This analysis reveals a ''clustering'' effect, which exposes the weaknesses of the RAN's existing

Table IV RAN case study summary

Activity	Risk score: Risk exposure (a)	Hazard risk index (b) (Figure 7)	Combined score (c) (Figure 8)	Risk response (d) (Figure 9)	Knowledge score: Individual characteristics (e) (Figure 3)	Knowledge characteristics (f) (Figure 4)	Organization characteristics (g) (Figure 5)	Mean score (h)	Risk response (i)	Overall response (j) (Figure 9)
12. Engineering policy and requirements management	5	6	3	Intolerable	10	12	12	11	Unacceptable	Immediate action
14. Engineering advice	5	6	3	Intolerable	3	4	18	8	Unacceptable	Immediate action
15. Defence record management	4	11	9	Unacceptable	17	17	18	17	Acceptable	Monitor
10. Design of certification basis and validation processes	3	6	6	Unacceptable	5	17	18	13	Unacceptable	Priority
13. Technical support network management	3	11	11	Acceptable	11	17	12	13	Unacceptable	Monitor
1. Customer management	3	11	11	Acceptable	16	5	12	11	Unacceptable	Monitor
3. Professional development program	3	11	11	Acceptable	11	12	14	12	Unacceptable	Monitor
7. Facilities, equipment management	3	11	11	Acceptable	17	17	11	15	Acceptable	Monitor
2. Supplier management	2	11	13	Acceptable	16	7	12	12	Unacceptable	Monitor
16. Investigation assistance	2	11	13	Acceptable	11	17	14	14	Acceptable	Monitor
4. Managing staff	2	11	13	Acceptable	11	7	11	10	Unacceptable	Monitor
9. Design of maritime systems	1	6	14	Acceptable	3	2	12	6	Unacceptable	Monitor
18. Engineering product reviews & process improvement	1	11	15	Acceptable	10	7	18	12	Acceptable	Monitor
5. Strategic planning & direction	1	6	14	Acceptable	3	4	11	6	Unacceptable	Monitor
11. Certification of material	1	6	14	Acceptable	3	12	18	11	Unacceptable	Monitor
8. Promote Navy engineering	1	11	15	Acceptable	17	17	12	15	Acceptable	Monitor
6. Financial management	1	9	14	Acceptable	11	17	14	14	Acceptable	Monitor
17. Audit assistance	1	11	15	Acceptable	16	17	14	16	Acceptable	Monitor

approach to risk management. Second, we calculate a knowledge score for each EngServ activity based on aggregating scores for three KRM constructs: individual characteristics, knowledge characteristics, and organisational characteristics (Step 2 in Figure 6). Third, the risk score and the knowledge score are combined using a two dimensional matrix to derive an overall risk response score (Step 3 in Figure 6). This is used to prioritise risks in terms of their urgency. The results illustrate managers' cognitive processes when evaluating risk. In doing so, the case study discussion exposes the weaknesses in traditional decision tree methods (Step 1). It also demonstrates the power of the conceptual model by identifying the objective criteria necessary to prioritise risks for action.

The risk score

Activity importance

The first step in the KRM method proposed in this paper is to differentiate amongst the importance of the firm's activities. This approach is grounded in the knowledge-based view of the firm (KBV) (cited in Grant, 1996) where the value of knowledge is derived from its combination with other resources to perform activities. Activities vary in their capacity to create value for the firm (Barney, 2001) and, therefore, some are more important than others. It is reasonable to accept that the risks associated with the most important activities, i.e. those that create most value for the firm, are more significant then those associated with less important activities. We call this concept ''Risk Exposure'', i.e. the level of risk associated with the importance of the activity. The level of risk exposure was calculated in the following way. Eighteen activities were identified from EngServ's strategic plan and were verified by senior management. Respondents were then asked to rate the importance of each activity on a scale from 1 to 5, where 1 = not at all important and 5 = extremely important. Each activity was then allocated an overall Risk Exposure score based on the mean score ranking from respondents (see (a) in Figure 6).

Hazard Risk Index

The second step is to identify the Hazard Risk Index (HRI) for the main Risk Factor associated with each activity (see (b) in Figure 6). With this in mind, we wanted to test the way individuals think when assessing risk using the HRI. We did this in the following way. First, we identified the main activities performed by the case study organization – EngServ. Second, we asked respondents to indicate the main risks associated with each activity, i.e. what is the worst thing that can go wrong with this activity. Third, we then asked respondents to rate the probability of this event occurring and the consequences using the HRI. The results are presented in the Tables V and VI.

These tables highlight the problem of clustering when using the decision tree approach to risk management. Clustering occurs when all risk factors are rated similarly. This is problematic because managers cannot differentiate between risks and then priorities for action. A quick glance at the table shows that every risk was rated 3 for probability, i.e. happens occasionally, except for poor financial decisions which is rated a 2 – probable.

Table V Probability and consequence – management activities

Management activity (order of importance)	*Risk factor*	*Prob.*	*Cons.*
7. Facility/equipment management	Reliability and capability failure	3	3
1. Customer management	Unhappy customers	3	3
3. Professional development program	Unskilled workforce and poor career development	3	3
2. Supplier management	Poor communication and teamwork	3	3
4. Managing staff	Do not manage poor performance	3	3
5. Strategic planning and directing	Lack of direction and strategy	3	2
8. Promote navy engineering	Requirements unworkable	3	3
6. Financial management	Changes and poor decisions	2	3

Table VI Probability and consequence – technical activities

Technical activity (order of importance)	*Risk factor*	*Prob.*	*Cons.*
12. Engineering policy and requirements management	Incorrect or inadequate advice	3	2
14. Engineering advice	Wrong advice	3	2
15. Defence record management	Loss of records	3	3
10. Design of certification basis and validation process	Not fit for purpose	3	2
13. Technical support network management	Loss of knowledge and experience	3	3
16. Investigation assistance	Lack of knowledge, skill and experience	3	3
9. Design of maritime systems	Failure of system	3	2
18. Engineering product reviews and process improvement	Product not fit for purpose	3	3
11. Certification of material	Failure of operation and systems	3	2
17. Audit assistance	Insufficient knowledge and experience	3	3

There is more variability in the consequences but all risks were rated either a 2 or 3. The consequences of the clustering effect are illustrated when we look at the way the RAN prioritized the HRI results. After a HRI assessment was made, staff were required to classify the risk as either intolerable, unacceptable, or acceptable. Figure 7 maps respondents' risk rating of EngServ's main activities, using the probability and consequences levels (Tables V and VI), to the Hazard Risk Severity Score (HRSS) indicator (Figure 1). Please note: the activity numbers refer to the tables above, e.g. activity 6 is Financial Management:

Figure 7 shows how seven risks are unacceptable, and the other eleven risks are acceptable. A closer look at the figures shows that there is more risk associated with technical activities compared with management activities because the consequences are generally more serious. For example, a greater proportion of risk factors associated with technical activities are rated unacceptable. However, the risks are plotted in only three of the 20 quadrants – 6, 9 and 11 – and are clustered together in the middle, which is not particularly helpful. The sameness in the risk ratings make it difficult for managers to differentiate between the risks and priorities for action.

Combining activity importance and HRI

By combining the activity importance and the HRI ratings, we can ''weight'' the Risk Factors in a way that is meaningful to the organization. Figure 8 plots the activities in terms of their Risk Exposure and their overall HRI rating. The results show that adding a weighting factor, such as Activity Importance, does make a difference to the overall risk assessment. The Risk Exposure dimension differentiates the activities in terms of the three risk categories. Figure 8 shows that there are two activities – 12 and 14 – which now have intolerable levels of risk, whereas the HRI on its own did not identify any intolerable risks. The combination of Risk Exposure and HRI has also differentiated sub-levels of risk. The activities are now scattered across the risk map (see Figure 8) and are found in seven of the 15 quadrants (compared to three of 20 in Figure 7). The result is that EngServ managers can better rank the Risk Factors in priority order (see the quadrant scores).

The knowledge score

The second step in the conceptual model presented in this paper was to derive a knowledge score (see Figure 6). Respondents were asked to assess the risks associated with the knowledge necessary to manage the main risk factors for each of EngServ's activities (see Tables V and VI) using the guidelines explained in the earlier section: Conceptual Development (see Figures 3, 4 and 5). In this way, each Risk Factor was allocated three scores between 1 and 25. We calculated the mean to derive an overall knowledge score. The results are summarised in Table IV.

Figure 7 Hazard Severity Index (HSI) ratings for EngServ

	Hazard Severity			
Hazard Likelihood	Catastrophic (1)	Critical (2)	Major (3)	Minor (4)
Frequent (1)	1	3	7	13
Probable (2)	2	5	9 6	16
Occasional (3)	4	12 14 6 5 10 9 11	17 15 18 11 1 8 4 16 13 7 2 3	18
Remote (4)	8	10	14	19
Improbable (5)	12	15	17	20

Intolerable
Unacceptable
Acceptable

Figure 8 Risk exposure and Hazard Severity Index (HSI) matrix for EngServ

Hazard Severity Index (HSI)

Risk Exposure	Intolerable (1)	Unacceptable (2)	Acceptable (3)
Critically Important (1)	1	3 12 14	7
Very important (2)	2	5	15 9
Important (3)	4	10 6	13 11 3 1 7
Not important (4)	8	10	2 13 4 16
Least important (5)	12	9 14 5 6 11	18 15 8 17

Intolerable
Unacceptable
Acceptable

Discussion

The discussion of the research findings is presented in three sections: the value of the conceptual model, the implications for managers or practitioners, and the research contribution for academics.

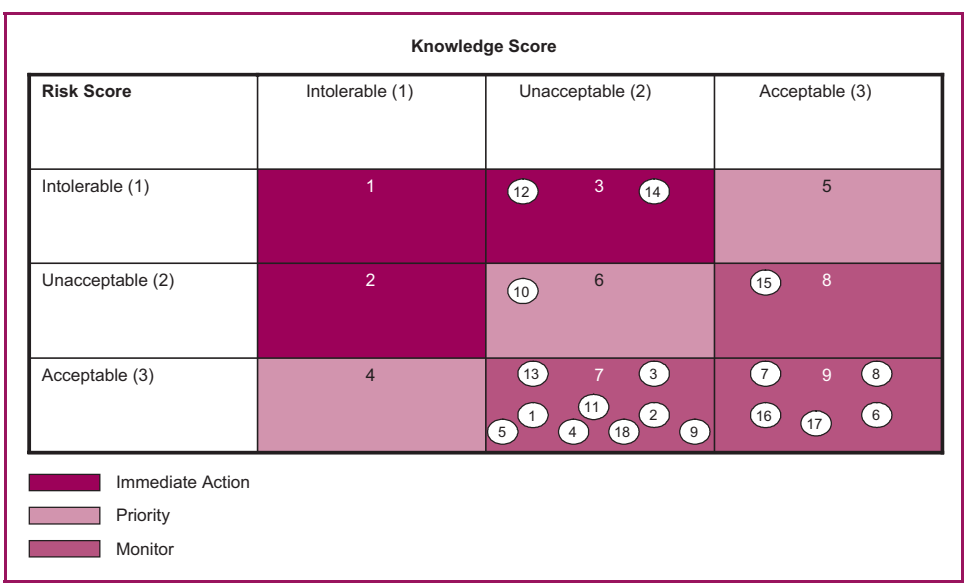
The value of the conceptual model

Has the addition of the Knowledge Score added any value to the conventional decision tree approach, i.e. the Risk Score? We answered this question in several ways. First, is there any difference in the risk response provided by the Risk Score (column (d) in Table IV) compared with the Knowledge Score (column (i) in Table IV)? Second, does the Knowledge Score risk response further differentiate the activities? Third, does the overall response, i.e. the combination of the Risk Score and the Knowledge Score (column (j) in Table IV), provide better managerial guidance on how to manage the risks at EngServ? Figure 9 presents the combination of the two scores.

In terms of the first point, 11 of the 18 activities (61 percent) had different risk responses, when we compared the Risk Scores with the Knowledge Scores. In the majority of these activities (8 of 11), the risk response was upgraded – from acceptable to unacceptable – by the inclusion of the Knowledge Score. On the second point, the Knowledge Score certainly removed the clustering effect of the Risk Score. The Knowledge Score had a much better split across risk category; reducing the number of activities rated acceptable risk from 78 percent (Risk Score) to 39 percent (Knowledge Score). The value of the Knowledge Score is perhaps best illustrated by the dramatic increase in risk rating, i.e. the quadrant scores (see columns (a), (b), (c), (e), (f), and (g) in Table IV), in some activities. It is important to remember when reading Table IV, that the column (c) Risk Score (i.e. Figure 8), is based on a scale of 1 to 15; where the column (e), (f), and (g) Knowledge Scores are based on a scale of 1 to 25 (e.g. see Figure 4).

The impact of the Knowledge Score is illustrated by comparing the most significant ratings changes. Using traditional decision tree methods, i.e. the Risk Score, the two highest risk activities are technical activities: engineering policy and requirements management (no. 12) and engineering advice (no. 14). These are EngServ's core business activities and commonly considered the most important work performed by the organization. It is, therefore, not surprising that these activities are considered to represent EngServ's greatest risk (see column (c) in Table IV). However, when we look at the Knowledge Score, the risk associated with these two activities is downgraded from intolerable to unacceptable. The conceptual model presented in this paper helps us understand why this has happened. If we look at the risk ratings provided by columns (e, (f), and (g), we see that engineering advice is still rated a very high risk activity (i.e. intolerable) in terms of individual characteristics and knowledge characteristics, but has a very low risk score for organizational characteristics

Figure 9 Overall risk response for EngServ activities



which lowers its overall Knowledge Score. The column (g) score tells us that the risk factor – wrong advice (see Table VI) – is not as worrying as it might seem at first glance (i.e. the Risk Score method) because the organization has an abundance of necessary knowledge. In other words, if someone makes a mistake, someone else will pick it up; or if someone is unavailable, someone else will fill in for them and so on. In a similar vein, the engineering policy and requirements management activity has a 'mid-range' risk rating for all three knowledge score indicators. While still rated unacceptable, and therefore requiring action from the RAN, it is not as urgent as the Risk Score would indicate. The findings show that cognitive bias has influenced the risk score and caused individuals' to over-estimate the risk associated with activities that they work on. We argue that the Knowledge Score is a more accurate indicator of risk because it removes this cognitive bias.

The capacity of the Knowledge Score to remove cognitive bias is shown when we look at some of the management activities. EngServ is an engineering organization. Its employees consider technical work to be much more important then 'managerial' work. This is illustrated by the Risk Exposure ratings (see column (a) in Table IV). However, this attitude has a dysfunctional influence on risk assessment. Individuals tend to correlate risk with their perception of the value of work. The more important the work, the higher the risks involved. This is not necessarily true and it is also dangerous from a risk management perspective. Two activities illustrate these points. Strategic planning and direction (no. 5) and design of maritime systems (no. 9) are rated a very low risk using conventional decision tree methods (see column (c) in Table IV). However, they are rated the equal highest risk activity by the Knowledge Score (see column (h) in Table IV), even higher then the two most important technical activities. The conceptual model explains why this has occurred. For example, the design of maritime systems has a very high risk knowledge characteristics score because it requires the highest levels of knowledge creation (i.e. complex problem solving) and this knowledge is a social capital. It is highly complex and inaccessible for many. Individual characteristics show us that this knowledge requires high qualifications and several years of on-the-job experience. It is difficult to buy (recruit) or develop (train). EngServ's competence in this activity is highly vulnerable if the few staff with this knowledge exit the organization or are otherwise unavailable to manage the risk. Why is this activity ignored by conventional risk management methods? The answer lies in cognitive bias or subjectivity. Design of maritime systems has largely been outsourced by the RAN to industry and, therefore, EngServ staff no longer spend much time doing it. Therefore, it has become one of the RAN's highest risk activities in terms of being an intelligent customer of industry and in ensuring the technical integrity of maritime materiel. However, the EngServ staff do not see this due to their cognitive bias.

On the third point, the combination of the Risk Score and the Knowledge Score (see column (j) in Table IV) does not appear to have added much value. The majority of activities resulted in the same response profile as provided by the Risk Score (see column (c) in Table IV). The combination of the Risk Score and the Knowledge Score appears to have diluted the impact of the Knowledge Score, meaning that the majority of activities (83 percent) had a low risk rating, i.e. monitor, which was similar to the high proportion of acceptable ratings (78 percent) generated by the Risk Score. There may be some value in prioritizing by quadrant scores (i.e. 1 to 9, see Figure 9), rather than the overall response category. The most value in the conceptual model for managers is to be gained from comparing the Risk Score and Knowledge Scores in isolation, as opposed to combining them, to remove the danger of subjectivity and to identify areas of cognitive bias.

Implications for managers/practitioners

Organizational risk management is a complex and important task for managers; particularly as the consequences of poor risk management is becomingly increasingly visible through financial loss, unethical behavior, and personnel injury and death. Stakeholders, such as institutional investors, are no longer willing to accept ignorance as an excuse. Managers must be aware of the risks associated with their organization's activities and have in place ways to manage unwanted events. The new field of knowledge risk management (KRM) offers managers ways to use knowledge to ensure decision makers are informed and can anticipate and respond to risk events. However, our analysis of EngServ identified a new

organizational risk – the high volume of decisions necessary to manage risk – which undermines the integrity of conventional risk management approaches, i.e. decision tree methods. Knowledge may help managers better identify risk factors and assess their risk levels (e.g. the HRI) but it also results in cognitive confusion resulting in a ''clustering effect'' (see Figure 7). It is not helpful if all risks are rated the same, particularly in high volume risk decision environments such as EngServ. The consequences could be that significant risks are ignored simply because decision makers are too busy. The addition of a weighting based on activity importance (column (a) in Table IV) was helpful in differentiating the risk scores (see Figure 8) but still resulted in an unacceptable degree of clustering or sameness about the risk response rating, i.e. intolerable, unacceptable or acceptable (see column (d) in Table IV).

Managers may use the conceptual model presented in this paper in the following way. Step 1 (see Figure 6) will identify the importance of the risk (risk exposure) and its threat (e.g. hazard risk index). The use of a weighting based on the importance of the activity reduces the clustering effect of traditional decision tree methods and also provides decision makers with organizational context. Step 2 (see Figure 6) provides deeper insight by assessing the organization's capacity to manage the risk. While Step 1 simply highlights what might go wrong, i.e. the unwanted event, Step 2 highlights the nature of the problem and the solution.

In further work with the case study organization, we have developed managerial guidelines for interpreting the risk ratings by activity and prioritising for action. Activities were color coded where red is intolerable risk, orange is unacceptable risk, and green is acceptable risk. The Knowledge and Risk Scores may then be interpreted by looking at the dimensions of the model that led to this rating. The dimensions help identify why each activity is a risk and, in this way, provide a platform for action from management. Management could target specific activities by addressing the issues underlying the risk rating. They can do this by looking at the scores for each dimension. Which dimension(s) is the lowest? That will identify the underlying problem. The following guideline is provided.

Activities with low knowledge scores (i.e. red colors)

1. *Low training score* (TTL – Figure 3) means it is difficult and time consuming to train people to do this activity. Can training be accelerated or otherwise improved?
2. *Low recruitment scores* (NQL – Figure 3) means it is difficult to find people to do this activity. Can the job requirement be lowered or recruitment otherwise improved? Or the job redesigned?
3. *Low accessibility scores* (RTA – Figure 4) means the knowledge involved is tacit (implicit) rather than codified (explicit). Can this knowledge be captured so that it is more easily shared or is there a way to improve knowledge sharing of people with this knowledge?
4. *Low complexity scores* (DoC – Figure 4) means the knowledge is difficult to learn. Can this knowledge be simplified or taught in a different way which makes it easier to learn? Alternatively is there pre-requisite (background) knowledge that can be taught to help people understand the topic?
5. *Low breadth of knowledge scores* (RMC – Figure 5) means only a relatively small number of staff know how to do this activity. Can we share this by identifying 'apprentices', 'successors', or even a community of practice?
6. *Low contingency scores* (RMM – Figure 5) means that there is little or no planning about what to do if people with the knowledge to manage this activity are unavailable. Can we write this into job descriptions, redesign jobs, or revise procedures to ensure that a back-up is in place?

Activities with low risk scores (i.e. red colors)

- *Low importance matrix codes* ((a) in Table IV) means the activity is very important and people feel they will be affected if things go wrong (i.e. the risk factor occurs). Is this true? If so, move onto the other dimensions. If not, provide a reality check to staff.

- *Low likelihood scores* ((b) in Table IV) means this risk factor is very probable. Is there any way to reduce the frequency of this unwanted event happening?
- *Low consequence scores* ((c) in Table IV) means the risk factor will have a serious negative impact. Is there any way to minimise the damage if this unwanted event occurs?

As a final guide, management could go through their list of activities and look for low scores. In some cases, there may be activities with only one low dimension. Addressing this dimension may be a quick way to increase the activity's overall risk rating.

The contribution to KRM theory

The paper has extended previous research on knowledge risk management by proposing a conceptual model that addresses the main problems associated with conventional decision tree methods of risk management. In doing so, it proposes several ideas which might the subject of further research. The first topic for investigation could be that an assessment of the risks associated with the knowledge necessary to manage the risk is a better indicator of organizational risk than conventional methods. There are several reasons for this: reduced clustering effect, better differentiation, and reduced cognitive bias. The research findings presented in this paper suggests a main cognitive constraint posed by decision tree methods is that individuals are biased towards work that they do when assessing risk levels. Conventional decision tree approaches request individuals to consider the main ''unwanted event'', i.e. the worst thing that can happen. The main risk factors at Eng Serv (see Tables V and VI) show that individuals tend to think of work being performed unsatisfactorily, i.e. they focus on the most negative outcome. In knowledge management terms, this is an output measure or realized capacity (cited in Zahra and George, 2002). In this way, the second topic for further investigation is our argument that inputs or potential capacity is a more accurate indicator of risk because it removes cognitive bias. This is shown when we compare the risk responses generated by the Risk Score compared with the Knowledge Score. At EngServ this was shown by the overestimation of risk associated with the two core engineering activities and the underestimation of risk associated with an outsourced engineering activity and a management activity. The third topic for further investigation is the six new constructs we advanced to measure potential capacity: necessary qualifications level (NQL), length of time to learn (TTL), degree of complexity (DoC), receiver's transfer capacity (RTA), risk management motivation (RMM), and risk management capability (RMC).

The paper has focused on resolving weaknesses associated with conventional decision tree methods of risk management, namely environmental complexity and cognitive constraints. The main focus was to reduce cognitive bias caused by subjectivity in risk assessment, manifested in our case study firm by individuals over-estimated the significance of risk associated with the work they do. We had to use conventional decision tree theory to evaluate the RAN process to risk management because that was how EngServ manages risk. We proposed a method using knowledge management theory as a way of improving conventional decision tree approaches to risk management, still being used in organizations as large as the Department of Defence. Would contemporary theories such as post-normal risk management and complexity theory help? In many ways, the KRM method proposed in this paper fits nicely with these contemporary theories. Post-normal risk management theory requires social interaction via discussion amongst groups of subject matter experts in the risk activity, while complexity theory sets appropriate boundaries around the social group (who should be involved) and the cognitive processes (what do we know). Our KRM method aims to increase objectivity in risk assessment, thereby reducing cognitive bias, by focusing individuals on the bigger picture of the knowledge necessary to manage the risk event (cognitive limits), and how well the organization can manage this knowledge (social setting limits). The KRM method addresses the cognitive bias of traditional risk assessment by ensuring the organization does not rely on individual experts who tend to focus on the risk event itself. By encouraging group reflection of the broader organizational issues introduced by our three dimensions of knowledge management – individual, knowledge, and organizational characteristics – we reduce a false sense of readiness that can be created by individual cognitive bias. Further research might test the KRM method within the context of these contemporary theories, for example, whether group discussion of the knowledge parameters on our model would further reduce cognitive bias.

Conclusions

The paper had two objectives. The first was to examine the effectiveness of conventional decision tree methods for managing organizational risk. The second was to develop an alternative model based on knowledge management constructs. The Royal Australian Navy's (RAN) Technical Regulatory System (TRS) follows a traditional decision tree approach to managing risk. The research findings showed that the TRS has addressed a main criticism of decision tree methods, individuals' cognitive constraints, by connecting risk levels (see Figures 1 and 2) with competency levels and positions (Table III). This ensured only suitably qualified staff (CAs) made decisions necessary to manage the RAN's risk. The process of delegated authority was effective because it fixed risk levels with competency levels. However, the RAN's risk management approach had two fundamental weaknesses. The first was related to environmental complexity, which was manifested at the RAN by the sheer volume of technical decisions required to manage organizational risk. This created a need for a model which helps manager's priorities risk factors for action. The second weakness was cognitive bias inherent in individual perception of the importance of the risk activity. EngServ respondents tended to have higher risk ratings for core as opposed to non-core activities, which suggests they are thinking about the consequences of the activity not being done, rather than the risk factor itself.

This paper has argued that the inclusion of knowledge management constructs would offer managers deeper insight into the real nature of organizational risk. The knowledge score was offered as a better alternative than the risk score because it better differentiates amongst the risk factors. This would address the cognitive constraints posed by conventional methods by reducing the clustering effect and offering more objectivity. This would be particularly helpful in high volume decision environments where individuals need to prioritise risk for action. This might also help reduce environmental complexity by clarifying risks that matter. It also fits nicely with more contemporary risk management theories and complexity theory by changing the boundaries from the risk event to the knowledge necessary to manage the risk event (see Midgley, 2008), and by expanding the social setting to include experts on the impact across the organization (see Seidl, 2007). In this way the KRM model presented in this paper provides a context for social dialogue amongst experts which takes them away from the cognitive bias of the risk event itself, and introduces a more objective assessment of the organizational-wide issues.

Knowledge risk management (KRM) appears to be a promising area for empirical research. It sits at the intersection of two exciting fields – risk management and knowledge – and has practical utility for managers and practitioners. The conceptual model presented in this paper (see Figure 6) uses knowledge management (KM) constructs to differentiate risks. Previous research on this topic argues that knowledge makes risk 'learnable' by moving decision makers from the unknown to the known; while knowledge management mobilizes the knowledge and expertise of employees (cited in Neef, 2005), by transferring knowledge to decision makers, improving knowledge accessibility, embedding knowledge in controls and processes, and generating new knowledge (cited in Marshall *et al.*, 1996). Our contribution to KRM is to use three KM constructs – individual, knowledge, and organizational characteristics – to identify a deeper level of insight about the nature of risk then is provided by conventional decision tree methods. This insight allows us to address both of the main weaknesses illustrated by the RAN's risk management approach. This paper is an exercise in theory development which, naturally, should be followed by further research in theory testing to empirically validate the model presented.

References

Adams, J. (1995), *Risk*, UCL Press Limited, London.

Apgar, D. (2006), *Risk Intelligence: Learning to Manage What We Don't Know*, Harvard University Press, Boston, MA.

Barney, J. (2001), ''Is the resource-based 'view' a useful perspective for strategic management research? Yes'', *Academy of Management Review*, Vol. 26 No. 1, pp. 41-57.

Bernstein, P.L. (1996), *Against the Gods: The Remarkable Story of Risk*, John Wiley & Sons, New York, NY, p. 383.

Bontis, N. (2002), ''Managing organisational knowledge by diagnosing intellectual capital: framing and advancing the state of the field'', in Choo, C.W. and Bontis, N. (Eds), *The Strategic Management of Intellectual Capital and Organizational Knowledge*, Oxford University Press, Oxford, pp. 621-42.

Choo, C.W. (1998), *The Knowing Organization: How Organizations Use Information to Construct Meaning, Create Knowledge, and Make Decisions*, Oxford University Press, New York, NY.

Cohen, W.M. and Levinthal, D.A. (1990), ''Absorptive capacity: a new perspective on learning and innovation'', *Administrative Science Quarterly*, Vol. 35 No. 1, pp. 128-52.

De Zoysa, S. and Russell, A.D. (2003), ''Knowledge-based risk identification in infrastructure projects'', *Canadian Journal of Civil Engineering*, Vol. 30 No. 3, pp. 511-22.

Douglas, D. (2006), ''Intransitivities of managerial decisions: a grounded theory case'', *Management Decision*, Vol. 44 No. 2, pp. 259-75.

Eisenhardt, K.M. (1989), ''Building theories from case study research'', *Academy of Management Review*, Vol. 14 No. 4, pp. 532-50.

Emblemsvag, J. and Kjolstad, L.E. (2002), ''Strategic risk analysis – a field version'', *Management Decision*, Vol. 40 No. 9, pp. 842-53.

Fischhoff, B., Watson, S. and Hope, C. (1984), ''Defining risk'', *Policy Sciences*, Vol. 17, pp. 123-39.

Grant, R.M. (1996), ''Toward a knowledge-based theory of the firm'', *Strategic Management Journal*, Vol. 17, pp. 109-22.

Kim, L. (1998), ''Crisis construction and organizational learning: capability building in catching-up at Hyundai Motors'', *Organization Science*, Vol. 9 No. 4, pp. 506-22.

Kogut, B. and Zander, U. (1995), ''Knowledge of the firm and the evolutionary theory of the multinational corporation'', *Journal of International Business Studies.*, Vol. 26 No. 4, pp. 625-44.

Liesch, P., Steen, J., Knight, G. and Czinkota, M.R. (2006), ''Problematizing the internationalization decision: terrorism-induced risk'', *Management Decision*, Vol. 44 No. 6, pp. 809-26.

McElroy, M.W. (2003), *The New Knowledge Management: Complexity, Learning and Sustainable Innovation*, KCMI Press, Amsterdam.

MacGillivray, A. (2007), ''Learning at the edge – Part 2: Scholar-practitioner reflections on boundaries'', *Emergence: Complexity and Organization;*, Vol. 9 No. 4, pp. 44-55.

March, J.G. and Shapira, Z. (1987), ''Managerial perspectives on risk and risk taking'', *Management Science*, Vol. 22 No. 11, pp. 1404-18.

Marshall, C., Prusak, L. and Shpilberg, D. (1996), ''Financial risk and the need for superior knowledge management'', *California Management Review*, Vol. 38 No. 3, pp. 77-102.

Mercer, D., Leschine, T., Drew, C.H., Griffith, W. and Nyerges, T. (2005), ''Public agencies and environmental risk: organizing knowledge in a democratic context'', *Journal of Knowledge Management*, Vol. 9 No. 2, pp. 129-48.

Midgley, G. (2008), ''Systems thinking, complexity and the philosophy of science'', *Emergence: Complexity and Organization*, Vol. 10 No. 4, pp. 55-74.

Mischen, P.A. and Jackson, S.K. (2008), ''Connecting the dots: applying complexity theory, knowledge management and social network analysis to policy implementation'', *Public Administration Quarterly*, Vol. 32 No. 3, pp. 314-39.

Mowery, D.C. and Oxley, J.E. (1995), ''Inward technology transfer and competitiveness: the role of national innovation systems'', *Cambridge Journal of Economics*, Vol. 19 No. 1, pp. 67-84.

Neef, D. (2005), ''Managing corporate risk through better knowledge management'', *The Learning Organization*, Vol. 12 No. 2, pp. 112-24.

Nonaka, I. and Takeuchi, H. (1995), *The Knowledge-creating Company*, Oxford University Press, New York, NY.

Nonaka, W. (1994), ''A dynamic theory of organizational knowledge creation'', *Organization Science*, Vol. 5, pp. 14-37.

Otterson, S. (2005), ''Transferring catastrophe risk management knowledge'', *Risk Management*, Vol. 52 No. 5, p. 46.

Schulz, M. (2001), ''The uncertain relevance of newness: organizational learning and knowledge flows'', *Academy of Management Journal*, Vol. 44 No. 4, pp. 661-81.

Schumpeter, J.A. (1934), *The Theory of Economic Development*, Harvard University Press, Cambridge, MA (Oxford University Press, New York, NY, 1961) (first published in German, 1912).

Seidl, D. (2007), ''The dark side of knowledge'', *Emergence: Complexity and Organization*, Vol. 9 No. 3, pp. 16-29.

Sherif, K. (2006), ''An adaptive strategy for managing knowledge in organizations'', *Journal of Knowledge Management*, Vol. 10 No. 4, pp. 72-80.

(The) Stanford Encyclopaedia of Philosophy (2007), *The Stanford Encyclopedia of Philosophy*, Metaphysics Research Lab, CSLI, Stanford University, Palo Alto, CA, available at: http://plato.stanford.edu/entries/risk/

Stewart, T.A. (1997), *Intellectual Capital: The New Wealth of Organisations*, Currency Doubleday, New York, NY.

Szulanski, G. (1996), ''Exploring internal stickiness: impediments to the transfer of best practice within the firm'', *Strategic Management Journal*, Vol. 17, Summer, special issue, pp. 27-43.

Taub, S. (2002), ''More corporate crimes and misdemeanors'', *CFO.com*, September 16, available at: www.cfo.com

Van Maanen, J. (1979), ''Reclaiming qualitative methods for organizational research: a preface'', *Administrative Science Quarterly*, Vol. 24, pp. 520-6.

Verhaegen, T. (2005), ''Knowledge makes risks manageable'', *Business Insurance: Industry Focus*, Vol. 3, pp. 16-17.

von Hippel, E. (1994), '''Sticky information' and the locus of problem solving: implications for innovation'', *Management Science*, Vol. 40 No. 4, pp. 429-40.

Walton, J. (1992), ''Making the theoretical case'', in Ragin, C. and Becker, H. (Eds), *What Is a Case? Exploring the Foundations of Social Inquiry*, Cambridge University Press, Cambridge, pp. 121-38.

Zahra, S.A. and George, G. (2002), ''Absorptive capacity: a review, reconceptualization, and extension'', *Academy of Management Review*, Vol. 27 No. 2, pp. 185-203.

About the author

Peter Massingham is from the University of Wollongong's School of Management and Marketing. He is currently the Director of the Centre for Knowledge Management. Before joining the University in 1998, he was a management consultant, most recently with KPMG. He is currently the Chief Investigator of an Australian Research Council Linkage Project Grant (2008-2011): measuring and managing the impact of knowledge loss (industry partner: Department of Defence). Peter Massingham can be contacted at: peterm@uow.edu.au