Journal of Risk Research, Volume 10, Issue 1, January 2007, pages 85-104

Benchmarking risk management within the international water utility sector. Part I: design of a capability maturity methodology

B.H. MacGillivray, J.V. Sharp, J.E. Strutt, P.D. Hamilton and S.J.T. Pollard*

School of Water Sciences, Cranfield University, Cranfield, Bedfordshire, MK43 0AL, UK.

* Corresponding author

Email: s.pollard@cranfield.ac.uk

Telephone: +44 (0)1234 754101

ABSTRACT

Risk management in the water utility sector is becoming increasingly explicit. However, due to the novelty and complexity of the discipline, utilities are encountering difficulties in defining and institutionalising their risk management processes. In response, the authors have developed a sector specific capability maturity methodology for benchmarking and improving risk management. The research, conducted in consultation with water utility practitioners, has distilled risk management into a coherent, process-based framework. We identified eleven risk management processes, and eight key attributes with characterise the extent to which these processes are defined, controlled and institutionalised. Implementation of the model should enable utilities to more effectively employ their portfolio of risk analysis techniques for optimal, credible and defensible decision making.

KEYWORDS: maturity model, risk, analysis, management, water, sector

1. Introduction

Financial restrictions, regulatory pressures and sectoral restructuring are encouraging water utilities to move from technically inclined, risk-averse management approaches towards more commercial, business-oriented practices (MacGillivray *et al.*, 2006a). Many within the industry, spurred on by developments in international regulation and guidance, are promoting a business-wide approach to risk management as a means to ease and exploit this transition (*e.g.* Lifton and Smeaton, 2003; Miller, 2005; Lloyd and Abell, 2005). Whilst the sector has made good progress towards setting its stated goal (AWWA *et al.*, 2001) of providing wholesome, safe drinking water that has the trust of customers within a risk-based context (Pollard *et al.*, 2004), there remain barriers to the implementation of risk management. These can be categorised as business-related, the challenge of embedding risk management within organisational cultures and decision-making processes (*e.g.* Pollard *et al.*, 2004; Howard and Lourens, 2005); and technical, relating to the selection and application of risk analysis tools (*e.g.* MacGillivray *et al*., 2006a). Our research addresses the former; the premise being that the tools and techniques for risk analysis are sufficiently developed, yet lacking is the organisational capacity to employ these methodologies for more optimal, credible, and defensible decision-making.

The authors propose that the dominant cause of this capacity deficiency is the difficulty inherent in establishing, defining and controlling risk management processes. This is perhaps because the sector's approach to implementation has centred on adherence to risk management frameworks. These are essentially standards describing the fundamentals of the prior art and the interrelationships between its core elements (*e.g.* Hamilton *et al.*, 2006). Here, we are not concerned with frameworks for drinking water quality management (*e.g.* NHMRC, 2001; WHO, 2002), widely accepted and applied within the sector as a means of placing public health protection within a risk-based context, but with those corporate-level frameworks intended to foster an integrated approach to risk management (*e.g.* COSO, 2004; Canadian Standards Association, 1997; Council of Standards of Australia, 1999). These latter frameworks have been instrumental in transforming the discipline from the preserve of engineering and finance functions towards a business-wide paradigm. However, a number of criticisms may be offered. Critically, although they typically embrace the concept that risk management is comprised of processes, their treatment of the discipline focuses on organisational structures and procedures. They often fail to address how the core tasks and activities of risk management may be defined and controlled as processes. Furthermore, although they have evolved beyond prescribing static requirements towards embracing the concept of continuous improvement, too often this is addressed as an afterthought rather than as an explicit component of these frameworks. As such, the water sector has lacked methodologies on which to base risk management improvement initiatives, suggesting that enhancements may often be isolated and that their associated benefits can neither be replicated nor extended throughout organisations. Finally, whilst typically generic in nature, these frameworks are often representative of the large, financially-oriented firms where their application predominates.

To address these shortcomings, the authors have developed a sector-specific risk management capability maturity model (RM-CMM), a vehicle for benchmarking, implementing and improving the *processes* that comprise risk management. In this paper we review the field of capability maturity modelling. We then describe the research methodology adopted in the design of our model, before discussing its development, structure and practical definition. A companion manuscript (MacGillivray *et al.*, 2006b) describes the model's application in a benchmarking of eight utilities within the international water sector.

2. Risk management in the water sector

The water industry is undergoing a significant shift in its approach to risk management to one that is increasingly explicit and better integrated with other business processes. Risk management strategies and techniques traditionally applied to occupational health and safety and public health protection are now seeing broader application for asset management (Booth and Rogers, 2001; Lifton and Smeaton, 2003), watershed protection (IMPRESS Management, 2002; NHMRC, 2001; WHO, 2003) and network operation (Stahl and Elliott, 1999; Stevens and Lloyd, 2004). Beyond this operational context, utility managers are increasingly concerned with managing the risks inherent to corporate level decision making. Critical issues include decisions on outsourcing asset maintenance; billing and monitoring; the management of change; staff retention; the long-term viability of investment decisions; and the management of external interfaces with regulators and "competing" utilities (MacGillivray *et al.*, 2006a). Pollard *et al.* (2004) report that the organisational hierarchy that exists even within "flat" utilities requires that these risks are actively managed at strategic, programme and operational levels (Fig. 1). Typically, there are split accountabilities for these risks such that the chief financial officer / financial director and Board have overall responsibility, supported by an internal audit or control function for the management of strategic risks; executive and senior management address programme level risks (*e.g.* asset management, maintenance planning); and operational (*e.g.* site) managers bear responsibility for operational risks (*e.g.* treatment plant performance).

Water utilities must employ a range of techniques to evaluate and consider these aspects alongside one another, devising business and operating strategies that prioritise resources on the basis of risk. Here tensions may arise from the explicit risk trade-offs inherent to running a commercial water utility, such that the industry's overarching goal of public health protection is placed in conflict with narrower financial interests. Critically in this regard, the transition to an explicit risk management philosophy within the sector is reflected in recent revisions to the World Health Organisation's (WHO, 2003) Guidelines for Drinking Water Quality. It is this overall context that drives the need for an increased capability to manage risk.

3. Overview of capability maturity modelling

A capability maturity model (CMM) is a simplified representation of an organisational discipline (*e.g.* software engineering, risk management) that distils industry practices into a coherent, process-based framework. These models are constructed according to maturity levels, from learner to best practice, which are characterised by the extent to which the processes are defined, controlled and institutionalised. The field's origins can be traced to the "quality revolution" of the 1970s (*e.g.* Crosby, 1979) and to the field of management performance measurement. The CMM methodology was first articulated by the Software Engineering Institute (SEI), whose seminal model (Paulk *et al.*, 1993) explored the design capability of software development organisations. The capability maturity modelling concept is finding increasing acceptance in academia and industry. Notable applications include software and systems engineering (Paulk *et al.*, 1993; Software Engineering Institute, 2002a), workforce development and management (Software Engineering Institute, 2002b), offshore design safety (Sharp *et al.*, 2002), reliability engineering (Strutt, 2003), and construction (Sarshar *et al.*, 2000). Capability models enable organisations to establish their current level of process maturity and identify the steps necessary to progress to a higher level, building on their strengths and improving on their weaknesses. They may be used for benchmarking purposes, enabling organisations to compare themselves against other companies in their sector and beyond. This may be done at the corporate, functional or business unit level. Similarly, they may be used to assess the capabilities of key suppliers and partners.

Recently, a selection of risk management capability maturity models (*e.g.* IACCM, 2003; RMRDP, 2002) have been developed. We believe that these models insufficiently reflect the basic principles of capability maturity modelling. The most critical point is that they are not explicitly process-centred. Furthermore, they do not closely reflect the clear distinctions between maturity levels as set out by the SEI and developed further by subsequent researchers, instead characterising risk management maturity on a graded scale of good-to-bad practice. Of course, the CMM approach is not the sole means for improving risk management, and these critiqued models have found support within industry. Thus, we do not imply that the IACCM and RMRDP models are without value, indeed their simplicity and modest time demands may prove attractive to many organisations. However, our development of the RM-CMM is not an extension of these models, but rather a novel application of capability maturity modelling to risk management in the water utility sector.

4. Rationale of research methodology

The tailoring of existing maturity models to a new discipline and sector is not a simple mapping exercise (Sarshar *et al.*, 2000). Here, the core principles of maturity modelling were abstracted and recreated in a form specific to risk management within the water utility sector. Design of the research methodology (Fig. 2) was informed by the authors' previous experience in maturity modelling within similar utility sectors and drew upon the CMM literature, particularly Sarshar *et al.* (2000). The methodology is designated "testing-out research" (Starke, 1995). Here, the aim is to explore the limits of previously proposed generalisations and to specify, modify or clarify their content (Starke, 1995). This form of research must be conducted under real world conditions, where the kind of control present in laboratory conditions is neither feasible nor justifiable. The lead author, in concert with a steering group of four expert practitioners, designed the model in collaboration with partner water utilities. Key development inputs included literature reviews of risk management and capability maturity modelling, structured scoping interviews with eleven water utility professionals from five countries, prior knowledge of maturity modelling in similar utility sectors, and past experience within the water sector.

Given the qualitative nature of the research, verification and validation mechanisms were adopted. The purpose of the expert steering group was to verify that the model accurately codified risk management in line with the principles of maturity modelling. Furthermore, feedback was sought from three water utilities to ensure that the model reflected the practical realities of managing risk in the sector. This took the form of one workshop and two interviews conducted after sharing the pilot model. This piloting sought to validate the model's architecture (*e.g.* are the right processes included, are they adequately characterised, are the key attributes relevant, *etc.*) and to clarify its terminology. The model remains under research. The authors have recently tested the model through a benchmarking exercise and two industrial case studies. These applications will provide data of intrinsic value to both the industrial and academic communities, and will serve as a means for evolving the model towards a state compatible with industrial ownership.

5. Risk management capability maturity model

5.1 MODEL OVERVIEW

The RM-CMM is designed to measure and improve risk management processes. Hence it is process-based rather than focussing on specific outcomes or deliverables. It is increasingly accepted that continuous process improvement is based on a series of small, evolutionary steps, rather than revolutionary measures (Paulk *et al.*, 1993). The RM-CMM organises these steps within evolutionary plateaus, or maturity levels, which lay successive foundations for continual process improvement. Fig. 3 illustrates the model architecture.

5.2 RISK MANAGEMENT MATURITY LEVELS

Setting sensible goals for process improvement requires an understanding of the difference between mature and immature organisations (Paulk *et al.*, 1993). We have developed descriptions of five maturity levels that characterise organisational behaviours in both risk management overall and for each constituent process. These levels were derived by abstraction from existing CMMs describing different disciplines (Paulk *et al.*, 1993, Software Engineering Institute, 2002a / 2002b; Sharp *et al.*, 2002; Strutt, 2003; Sarshar *et* *al.*, 2000), contextualisation of which was supported by reviews (MacGillivray *et al.*, 2006a, Pollard *et al.*, 2004; Hamilton *et al.*, 2006) and scoping interviews. It is important to understand what these levels represent in practice, as they are central to assessing the maturity of an organisation. Below we describe the overarching maturity hierarchy. Note that at a given level of maturity, the positive characteristics from preceding levels remain.

Level 1 – Initial

L1 organisations practice a largely *ad hoc* approach to risk management, possessing no formal risk management processes and often exhibiting limited knowledge of relevant standards or regulatory guidelines. Thus, they are largely reliant upon individual heroics for the active management of risk. L1 organisations are likely to be small water providers based in isolated rural areas where resource constraints prevent the staffing of utilities with dedicated water professionals.

Level 2 – The repeatable organisation

L2 organisations understand that they have risks that require formal management, and have established basic risk management processes for this purpose. However, these processes are ill-defined and poorly institutionalised, limiting their capacity to influence organisational actions. Furthermore, the scope of risk management is narrow, generally restricted to addressing mission-critical risks and areas required by regulation (*e.g.* occupational health and safety, water quality). Hence, at L2 the active management of risk tends to be influenced less by explicit risk management processes than by the repetition of activities and practices that have worked for the organisation before. In a technical context, this places a premium on accepted standards of performance and codes of practice (*e.g.* engineering standards; accepted best practice) which, if adhered to, provide high degrees of control. This is a pragmatic approach in familiar and well-characterised situations where uncertainties and system vulnerabilities are well understood.

However, this mind set is vulnerable; when mistakes are made they do not learn – failures are repeated as well as success. Whilst L2 organisations often have a reputation for achieving reliable, cost-effective water supply, they are very vulnerable to change, whether organisational, technical or commercial. This, allied with deficient organisational learning, is a common theme across many recent water quality related outbreaks in affluent nations (Hrudey and Hrudey, 2004).

Level 3 – The defined organisation

The key characteristic of the L3 organisation is the definition and implementation of risk management processes across core business areas. This is achieved through establishing process "enablers". Enablers include the policies, procedures and frameworks that guide risk management activities (*i.e.* who does what and when), and the provision of adequate training, funding and tools in support of these activities. Several scoping interviewees described their recent definition of risk management processes. Drivers for this included: a desire to balance the role of "brainstorming" and "judgement" in risk management with more methodological, standardised and objective approaches; the need to "institutionalise" risk management; and obligations to exhibit good corporate governance to shareholders and regulators. In essence, definition seeks to formalise existing implicit approaches to risk management. This is most notably illustrated in the sector's increasing adoption of the "water safety plan" approach, which codifies good practice in the identification, assessment and control of hazards to water quality.

Definition creates an environment in which risks are methodically identified, analysed, responded to and monitored. In a technical context, L3 maturity is required where systems are characterised by greater levels of uncertainty and the potential to deviate from routine operation. This is increasingly common, as the trend towards utility self-sufficiency means that management can no longer seek to "over-engineer" facilities with the presumption of screening out technical risk (MacGillivray *et al.*, 2006a). Here, optimisation of plant, network and process design and operation requires a capacity to assess, understand and respond to what is driving the risk from or to the plant, process or network. However, at L3 the efficiency and quality of risk management processes are variable, stemming from limitations in their verification, validation and feedback mechanisms (the "evaluators"). These limitations restrict organisations' ability to track and therefore control their risk management processes, which are thus characterised as "open loop."

Level 4 – The controlled organisation

The key characteristic of the L4 organisation is a structure which not only enables their risk management processes but also evaluates and ensures their effective execution (closing the open loop of L3). The scope of these processes reach throughout the organisational hierarchy and across all functional boundaries. Evaluating refers to the implementation of verification and validation mechanisms to provide feedback on the status, quality, efficiency and expediency of risk management (*e.g.* ensuring procedural compliance, quality assurance, benchmarking *etc.*). The value of systematic verification was emphasised by one scoping interviewee, who noted that previously, free access to the corporate risk register was combined with an absence of peer review of risk assessments. This had allowed staff to "over-estimate their own pet concerns" and to assign risk reduction actions via the register to other staff "unbeknownst to them." These deficiencies were remedied through the introduction of formal procedures governing access and use of the register and the establishment of challenge procedures to provide quality assurance of risk assessments.

However, the L4 organisation tends to be hardwired and lacking in internal flexibility. This is reflected in that although a learning ethos exists, the manner in which L4 organisations learn is defined as single-loop (Argyris and Schön, 1978). This refers to learning where the emphasis is on improving techniques for executing processes, within the constraints of established process strategies. In other words, learning is directed towards making existing process strategies more effective. Single-loop learning tends to be present in organisations where goals, values, frameworks and strategies are taken for granted. This lack of capacity for deeper learning hampers their ability to make informed risk management decisions in rapidly changing and uncertain contexts. Additionally, L4 organisations are often unable to grasp the soft issues associated with human and organisational behaviour. This is a core weakness.

Level 5 – The optimised organisation

The key characteristics of the L5 organisation are its adaptability, flexibility and attention to human and organisational behaviour. The L5 mindset is one of deeper understanding, of an adaptive, learning organisation aiming to be best in class and always improving in the long term. Central to this is their capacity for both double (Argyris and

Schön, 1978) and triple-loop learning. Double-loop learning involves questioning the norms, values and assumptions underlying the design of risk management processes, and is typically found in organisations where risk information is continually developed through a broad range of channels (*e.g.* experience, R+D, benchmarking, analysis, simulation, *etc.*). This information is openly shared, communicated and used to publicly test assumptions and beliefs. We define triple-loop learning as questioning and revising *broader* organisational structures and practices to optimise the capability of risk management processes (*e.g.* changing incentive structures to encourage knowledge sharing and collaboration between traditionally competing departments, *etc.*). The core enablers of triple-loop learning are an understanding of how human and organisational behaviour influence process capability, and organisational flexibility. L5 organisations are also actively engaged in the innovation, development and piloting of new ideas and technologies to optimise risk management throughout the organisation. From these efforts, best practices are identified and transferred throughout the organisation. L5 processes are extremely efficient and there is a strong risk management culture, because of the long term investments made in developing processes and in training staff to participate in them.

5.3 RISK MANAGEMENT PROCESSES

Our research identified 11 risk management processes (Fig. 3). Strategic risk planning centres on developing the corporate framework for risk management. Hamilton *et al.* (2006) describe how these frameworks can introduce greater rigour, consistency and standardisation to the discipline. The researchers further note their potential for adaptation to suit "user needs." This final point is crucial, as our scoping interviews suggested that risk management frameworks were not simply shoehorned within utilities. Establishing risk acceptance criteria is perhaps the least understood aspect of risk management. Whilst our scoping interviews implied that internally developed criteria for evaluating the significance of risks were commonplace (risk ranking techniques), prior experience in similar sectors suggests that tolerability criteria are less prevalent and often externally imposed (*e.g.* ALARP criteria for dam safety). We address both of these aspects in the context of an internal process, as we propose that both are required to develop responses to risks in a consistent, objective and defensible manner. Risk analysis involves the identification and assessment of risk. We have previously reviewed (MacGillivray *et al.*, 2006a) its application in the sector at operational, programme and strategic levels. Here, our focus is not on the methodologies *per se*, but on their application. Supported by initiation criteria and formal procedures, using personnel with appropriate skills, experience, and resources, risk analysis techniques can provide utilities with benefits ranging from an improved understanding of treatment reliability to an explicit appreciation of project financial risks. Applied inappropriately, whether due to ill-defined procedures or deficient institutional capacities, risk analysis is not a subset of risk management but its panacea. Our inclusion of risk based decision making examines how organisations identify and evaluate solutions to manage individual risks. Clearly, risk analysis is of little use if the outputs are intended to placate regulators rather than inform decision making. Furthermore, one interviewee noted that an absence of criteria to evaluate decisions restricts objectivity (*i.e.* opinions dominate in decision making), and we further propose that it prevents the *ex ante* validation of decisions taken. Risk response is the implementation of risk based decisions. Although an argument may be forwarded that this lies outside the scope of our model as implementation processes are unlikely to be unique to risk based decisions (*i.e.* there will exist models for implementing capital or operational solutions, not models for implementing risk based decisions *per se*), it is included as decisions left unimplemented are hollow gestures. The model's treatment of these latter two processes is particularly relevant as risk management frameworks have historically focussed on the identification and assessment of risk, effectively marginalising guidance on their practical management. Risk monitoring involves tracking the evolution of identified risks, and is included in recognition of their dynamic nature. Integration is the current focus of the risk management community. From the literature and our scoping interviews, two aspects were identified: embedding risk management within organisations; and enterprise risk management, where risks are managed with reference to the organisation as a whole, rather than in isolation or in functional silos. Illustrating the latter aspect, Lam (2003) contends that the traditional, fragmented approach, where companies manage risk in organisational "silos," is ineffective because risks are highly interdependent and cannot be segmented and managed by entirely independent units. As one scoping interviewee stated, "one of the challenges is…when [staff] are all using discrete [risk] tools which may have different terminologies, scoring systems and ways of presenting the outputs, my role is [to ensure] is a shared understanding and an ability to interpret the results of tools in a business-wide context." We introduce a third element of integration by abstraction from the systems engineering CMM (Software Engineering Institute, 2002a): integration of the risk management process interfaces (*e.g.* between risk analysis and risk based decision making).

Supply chain risk management addresses two components: the sourcing of components required to develop a product (*e.g.* chemicals) and the management of services provided by organisations throughout the supply chain. The latter element is of particular significance to the sector owing to the increasing utilisation of outsourcing. However, one pilot interviewee challenged the inclusion of product risk, arguing it is effectively managed through adhering to quality accredited suppliers. However, it was maintained as the authors' prior research in the oil and gas industry indicates that many organisational failures can be traced back to minor and apparently insignificant services *and* components sourced from suppliers. Change risk management is abstracted from the reliability engineering CMM (Strutt, 2003), and involves identifying and managing the risk implications of organisational (*e.g.* business process re-engineering) and technical change. We justify its inclusion as a range of factors (*e.g.* globalisation, regulatory and market restructuring, novel technologies) are serving to fundamentally alter the context in which water utilities operate. Education and training – the development and maintenance of the competencies required to manage risk – is included as our scoping interviews suggested that risk management simply does not fit well into traditional company skill sets. Risk knowledge management may be considered as the collection, storage and access of the data underpinning *and* accumulated from the broader risk management processes, *i.e.* the input and output data. The latter aspect is drawn from our scoping interviews, which discussed various risk communication and reporting protocols and the use of databases for storing risk assessment outputs. We include the former aspect on the premise that in the absence of pre-defined data requirements, risk data collection is likely to be *ad hoc* and largely restricted to the needs of business as usual.

There was some discussion amongst the authors as to whether research and development in risk management merited inclusion as a process. However, the pilot interviewees were resistant to this, with one considering it ‘‘not directly relevant,’’ another stating that the tools and techniques of the discipline are sufficiently developed, rendering it a secondary issue. Although their experience within the sector confers validity to their arguments, they may nonetheless be considered somewhat short-sighted. A compromise was found through considering research and development not as a distinct process but as a defining characteristic of mature risk analysis, risk monitoring and risk knowledge management.

5.4 KEY ATTRIBUTES

We have identified eight key attributes (Fig. 3) which characterise process maturity. Scope is included as we propose maturity to be correlated with the scope of implementation (*i.e.* a well defined process restricted to engineering does not constitute high *organisational* maturity). Here, integration refers to the existence of initiation criteria and procedures for process execution. Although its treatment as both process and attribute constitutes double-coverage, this was felt appropriate given its prominence in the practitioner and academic literature. Verification mechanisms address procedural compliance and quality assurance of process execution, whilst validation determines whether the process itself is correct. Together, these mechanisms create process control, and provide the primary feedback inputs for organisational learning. The inclusion of organisational learning builds on prior research conducted by the authors in offshore design and safety (Sharp *et al.*, 2002) and reliability engineering (Strutt, 2003), although the underlying principle is drawn from ideas from the *theory of action* and the concept of *single and double loop learning* (Argyris and Schön, 1978). It is best illustrated by paraphrasing Dalrymple (2006), who notes that experience rarely provides lessons directly, but instead requires interpretation through the filter of preconceived theories, values and prejudices. Where these are impregnable, facts are weak things. The capacity to use experience to question and revise these preconceived notions constitutes double loop learning.

We include stakeholder engagement in deference to its prominent representation within risk management frameworks. However, our scoping interviews revealed a disconnect between academic and industrial perceptions of the appropriate role of *external* stakeholders within risk management, with the latter generally more resistant to their involvement. Explanations to support this stance included the need to preserve commercial confidentiality, concerns over possible conflicting objectives between stakeholders and organisations, and fears that stakeholder representatives may lack specialist knowledge and hence “slow down” risk management. One interviewee described that whilst they developed emergency response plans for water quality incidents in conjunction with the public health regulator, they were resistant to brining concerns about drinking water safety to the public domain owing to fears of press sensationalism. Another noted that they “don’t so much consult stakeholders as expose the [risk] governance process to them [*e.g.* regulators or shareholder representatives] – they form an opinion of [its] adequacy or otherwise.” That said, there was agreement on the importance of engaging internal stakeholders, on the premise that through engaging other departments, functions, and business units, organisations may avoid the silo mentality which has historically pervaded risk management, thus creating synergies through shared knowledge and expertise, the co-ordination of related work, *etc*. For example, one interviewee described the value of using “networks of participants” to provide input to capital investment decisions. Here, stakeholders have the opportunity to critique proposed options (*e.g.* for constructing a new treatment plant, staff involved in the design, operation and maintenance, costing, *etc.*). The inclusion of competency as an attribute recognises that risk management processes will prove ineffective if their execution lies outwith technical or managerial skill sets. Indeed, many of our interviewees discussed their desire to maintain in-house competencies to manage risk in preference to relying on consultants. Resourcing encompasses the use of monetary, human and technical (*e.g.* analysis methodologies) resources. As one interviewee noted, "funding, manpower, and specialists" are particular constraints to effective risk management in smaller utilities. Process documentation and reporting is the final attribute. Notably, Deloach (2000) reflects that there is often a lack of organisational consistency in reporting formats for risk management, which he perceives as a barrier to "enterprise wide" risk management. More practically, one interviewee argued that in what remains a conservative industry, if risk information is not properly documented and accessible then staff will use this ‘‘as an excuse to ignore risk management.’’

Consideration was afforded to the inclusion of culture as an attribute, given its extensive discussion in the literature and our scoping interviews. However, this was rejected for two reasons. Firstly, culture is a notoriously difficult concept to define, let alone measure. Secondly, overt attempts to change culture, which in this context may be thought of as the values and beliefs held by employees that guide their actions in managing risk, are not only Orwellian, but likely to be ineffectual. Ineffectual, as the authors consider that employee values and beliefs are not intrinsic properties, but rather are conditioned by the environment within which they manage risk (*i.e.* the risk management processes). Thus, culture change is a consequence of process improvement, not a prerequisite.

5.5 INTERNAL STRUCTURE OF PROCESS ASSESSMENT FRAMEWORK

At the framework's core are a series of guideline statements which describe how each process is conducted at each level of maturity with reference to the key attributes. In support of this are process descriptions which also outline the key practices required to satisfy the process goals. As the guideline statements are largely devolved from the principles contained in the overarching maturity hierarchy, we do not dwell on their detail. However, by way of illustration, Table 1 depicts the assessment framework at levels 3 and 4 for risk analysis.

5.6 INTERNAL STRUCTURE OF PROCESS IMPROVEMENT FRAMEWORK

This framework outlines the operational steps that utilities may take in order to implement their process improvement priorities as identified from application of the assessment framework. It was developed after receiving feedback that the assessment framework was at a layer of abstraction which restricted its ability to inform the development of improvement plans. The steps are grouped by process and maturity level, and are categorised according to actions to: perform base and advanced practices that satisfy the process goals (*i.e.* do the process); establish and define the process (*i.e.* structure the process); and enable and evaluate the process (*i.e.* institutionalise the process). Table 2 depicts the process improvement framework relating to progression from L3 to L4 in risk analysis.

6. Illustrating the RM-CMM

We have discussed the overarching maturity hierarchy, and introduced the risk management processes and those attributes which define their maturity. Here, we build on these foundations by illustrating what the model practically means within various organisational functions. Consider first risk analysis. The distinction between the *ad hoc* and the repeatable level is that in the latter, the application of basic techniques by experienced staff creates a degree of stability. In process engineering, this may entail the execution of hazard and operability studies (HAZOP) to identify and assess the potential for designs to deviate from specifications, whilst at L1 this potential would be addressed implicitly if at all. At L3, initiation points for analyses are defined (*e.g.* at the concept design stage), and formalised procedures detail the tasks, activities, roles and responsibilities for execution, creating a basic infrastructure that maintains the process beyond the tenure of experienced staff (who are depended upon at L2). At L4, verification extends beyond ensuring procedural compliance (L3) to address quality assurance of analyses, for example through technical peer reviews. Questions addressed may include: did the analysts work their way through the HAZOP study systematically, or did they overlook important scenarios, components and process flows; were all stages and operating modes of the process considered (*e.g.* startup, shutdown and transitioning to partial operation); and was adequate time spent on the analysis.

We now consider risk based decision making in the context of occupational health and safety. Here, the initiating point is the receipt of risk analysis outputs (*e.g.* job safety risk analyses, plant hazard evaluations, *etc.*). These outputs, together perhaps with a predefined hierarchy of health and safety risk controls (*e.g.* engineering; administrative; and protective personal equipment) serve as the framework for identifying solutions to manage individual risks. Once identified, these solutions may be evaluated with reference to criteria including: cost, feasibility and risk reduction achieved. In contrast, at L2 maturity, decisions to manage risks are taken in isolation of a clearly defined framework and perhaps even in the absence of risk analysis outputs, and are hence focus upon replicating historic good practice. Thus, health and safety is under pressure when circumstances change, whether through the introduction of new technical processes or modifications to work practices.

Finally, consider education and training in risk management. Here, a repeatable process may focus on workshops, where the concepts of risk management are introduced to staff on an as required basis, supported by on the job training. Further, there is an absence of clear criteria dictating when and to whom training should be delivered. An additional weakness is the inability to define the required competencies for effective risk management. Without these, on what basis are training programmes designed, how are the appropriate means of delivery selected (*e.g.* classroom training, workshop, on the job, *etc.*), and how can the efficacy of training be evaluated? These weaknesses are remedied at the defined state.

7. Model application

The RM-CMM has a range of potential applications, including:

- Self-assessment or external evaluation (voluntary or audit) of risk management maturity at the corporate, business unit, functional and project level;
- Use by management and technical staff as a reference model for designing and implementing a risk management improvement initiative;
- Evaluation of potential suppliers' / contractors' / partners' risk management maturity prior to selection.

The model can be implemented either as a self-assessment procedure or by external audit using independent verification authorities. It is felt that the latter, in most cases, gives greater credence to the results of an assessment. However, internal assessments are often more useful when using the model as an improvement tool rather than as a measurement tool. The companion paper (MacGillivray *et al.*, 2006b) describes in detail the self-assessment methodology.

8. Conclusions

We have described a risk management capability maturity model, a vehicle for benchmarking and improving risk management within the water sector. We have addressed the model's theoretical and empirical foundations, overviewed its architecture, and illustrated its practical definition. Implementation of the model should assist utilities to more effectively employ their portfolio of risk analysis techniques for optimal, credible, defensible decision making. A companion paper describes its application to benchmark eight utilities within the international water sector.

Acknowledgements

This work has been funded by the American Water Works Association Research Foundation (AwwaRF project RFP2939) and a consortium of international water utility companies. The comments and views herein are the authors' alone. BM is co-funded on a UK Engineering and Physical Sciences Research Council (EPSRC) Doctoral training account.

References

Argyris, C. and Schön, D. (1978) *Organizational learning: A theory of action perspective*, Reading, Mass: Addison Wesley.

AWWA, EUREAU, WSAA and DVGW (2001) *Bonn Workshop 2001 – Key principles in establishing a framework for assuring the quality of drinking water: a summary,* AWWA, Denver, CO., 2001.

Booth, R. and Rogers, J. (2001) Using GIS technology to manage infrastructure capital assets, *J. AWWA*, **93**(11), 62-68.

Canadian Standards Association (1997) *Risk management: guidelines for decision makers.* CAN/CSA-Q850-97.

COSO (2004) *Enterprise risk management framework - Executive Summary*. Available at www.otpp.com.

Council of Standards of Australia (1999) *Australian/New Zealand risk management standard No.4360: 1999.*

Crosby, P. B. (1979) *Quality is Free*, New York, McGraw-Hill.

Dalrymple, T. (2006) Less liberté means less egalité, *City Journal*, Winter 2006.

Deloach, J.W. (2000) *Enterprise-wide risk management - strategies for linking risk and opportunity,* Pearson Education Limited, London, 284pp.

Hamilton, P.D., Pollard, S.J.T., Hrudey, S.E. and MacGillivray, B.H (2006) Risk management frameworks for the water sector – a review, *at review*.

Howard, J. and Lourens, A. (2005) Engaging operational staff in risk management, *Proc. of Risk analysis strategies for better and more credible decision making*, 6-8th April, 2005, Banff, Canada.

Hrudey, S.E. and Hrudey E.J. (2004) *Safe drinking water: Lessons from recent outbreaks in affluent nations*, IWA Publishing.

IACCM (2003) *Organisational maturity in risk management: The IACCM business risk management maturity model (BRM3)*. Available at http://www.risk-doctor.com/pdf-files/brm1202.pdf.

IMPRESS Management (2002) *Guidance for the analysis of pressures and impacts in accordance with the water framework directive, Draft 5.2*, European Commission, Brussels.

Lam, J. (2003) *Enterprise risk management: from incentives to controls*, John Wiley & Sons, Hoboken, New Jersey.

Lifton, G. and Smeaton, P. (2003) Asset risk management in Scottish Water, *Proc. of the ICE/CIWEM Conference: Risk and reward in asset management delivery – who is best prepared for the challenges ahead?*, 14th November, 2003, London, UK.

Lloyd, R. and Abell, P. (2005) Capital maintenance in Yorkshire Water's water business unit, *Proc. of Risk analysis strategies for better and more credible decision making*, 6-8th April, 2005, Banff, Canada.

MacGillivray, B.H, Hamilton, P.D., Strutt, J.E., Pollard, S.J.T. (2006a) Risk analysis strategies in the water utility sector: an inventory of applications for better and more credible decision-making, *Critical Reviews in Environmental Science and Technology*, **36**, 85-139.

MacGillivray, B.H., Pollard, S.J.T., Hamilton, P.D. and Bradshaw, R.A. (2006b) Benchmarking risk management within the international water utility sector. Part II: A survey of eight water utilities, *J. Risk Research*, at review.

Miller, G.A. (2005) Risk governance in a water utility, *Proc. of Risk analysis strategies for better and more credible decision making*, 6-8th April, 2005, Banff, Canada.

NHMRC (2001) Framework for management of drinking water quality, NHMRC, New Zealand.

Paulk, M.C., Curtis, B., Chrissis, M.B. and Weber, C.V. (1993) Capability maturity model, version 1.1, *IEEE Software* **10**(4), 18-27.

Pollard, S.J.T., Strutt, J.E., MacGillivray, B.H., Hamilton, P.D. and Hrudey, S.E. (2004) Risk analysis and management in the water utility sector – a review of drivers, tools and techniques, *Trans. IChemE, Part B: Proc. Safety Environ.* **82**(B6): 1-10.

Prime Minister's Strategy Unit (2002), *Risk: improving Government's capability to handle risk and uncertainty*, The Strategy Unit, London. Available at: http://www.number-10.gov.uk/SU/RISK/risk/home.html.

RMRDP (2002) *Risk management maturity level development*. Available at http://www.risksig.com/Articles/rm%20report%20final%20version%2012.doc.

Sarshar, M., Haigh, R., Finnemore, M., Aouad, G., Barrett, P., Baldry, D. and Sexton, M. (2000) SPICE: a business process diagnostics tool for construction projects, *Engineering, Construction and Architectural Management*, **7**(3), 241-250.

Sharp, J.V., Strutt, J.E., Busby, J. and Terry, E. (2002) Measurement of organizational maturity in designing safe offshore installations, Proc*eedings of the International Conference on Offshore Mechanics and Arctic Engineering,* **2**: 383-390.

Software Engineering Institute (2002a) *CMMI for systems engineering / software engineering / integrated product development / supplier sourcing, version 1.1.* Available at http://www.sei.cmu.edu/.

Software Engineering Institute (2002b) *People capability maturity model, version 2.0.* Available at http://www.sei.cmu.edu/.

Stahl, G.R. and Elliott, J.C. (1999) 'New generation' computer models for risk-based planning and management, *Water Supply (Australia)*, **17**(3/4), 289-295.

Starke, R.E. (1995) *The art of case study research*, Sage, Thousand Oaks, CA and London.

Stevens, I.M. and Lloyd, R.I. (2004) *Water resources: Sustainable optimisation and security of supply, a proven example,* A paper presented to the 2004 Water sources conference and exposition, Jan 11-14th, 2004, Austin, Texas.

Strutt, J.E. (2003) *Reliability capability maturity briefing document*, Report No. R-03/2/1, Cranfield University.

WHO (2003), *Guidelines for drinking water quality, 3rd Edition* (draft), WHO. Available at: http://www.who.int/water_sanitation_health/dwq/guidelines3rd/en/.

WHO (2002) *Water safety plans (revised draft),* Report publication WHO/SDE/WSH/02.09, World Health Organisation.

Fig. 1. The risk hierarchy (adapted from Prime Minister's Strategy Unit, 2002)

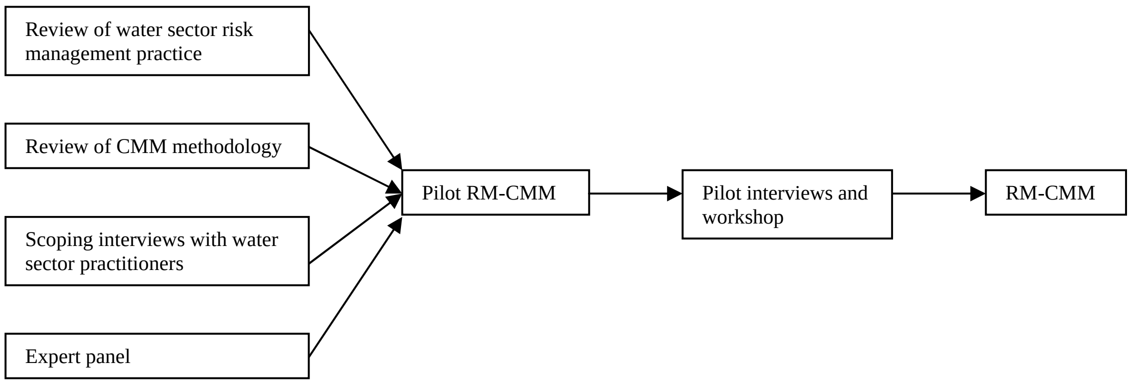
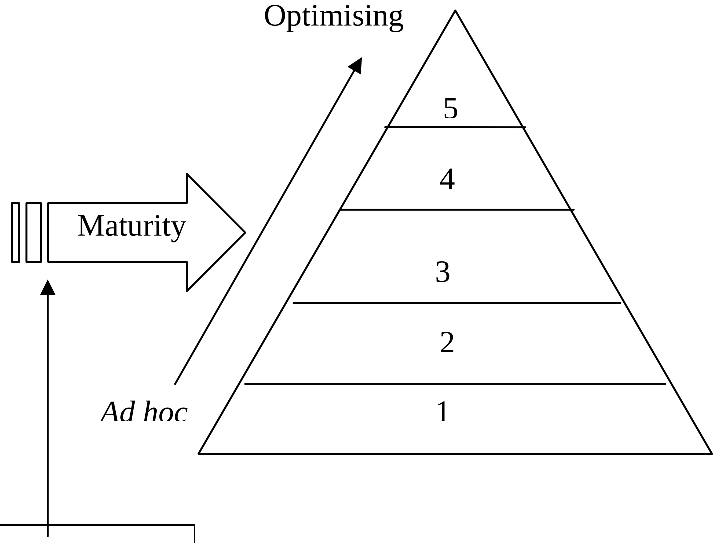


Fig. 2. Research methodology for design of RM-CMM.

	Processes
Core	Strategic risk planning (SRP)
	Establishing risk acceptance criteria (ERAC)
	Risk analysis (RA)
	Risk based decision making and review (RBDM)
	Risk response (RR)
	Risk monitoring (RM)
	Integrating risk management (IRM)
Supporting	Supply chain risk management (SCRM)
	Change risk management (CRM)
Long-term	Education and training in risk management (E&T)
	Risk knowledge management (RKM)



Attributes
Scope
Integration
Verification and validation
Feedback and organisational learning
Stakeholder engagement
Competence
Resources
Documentation and reporting

Fig. 3. Overview of the RM-CMM (after Strutt *et al.*, 2005).

Attribute	Attribute at level 3: Risk analysis	Attribute at level 4: Risk analysis
Scope	A defined, documented process is in place containing criteria, methods and guidelines for the identification, assessment and evaluation (with respect to acceptance criteria) of a broad range of risks across core business areas, guided by a risk register. The organisation is conversant with and goes beyond the regulatory requirements for risk analysis.	A controlled process is in place containing detailed criteria, methods and guidelines to manage the identification, assessment, evaluation (with respect to acceptance criteria), establishment of causality and linking (common cause and dependent) of risks at all levels of the company and across all functional boundaries of the business, guided by a company-specific risk register.
Integration	Procedures are in place to initiate risk analysis processes.	Risk analysis is initiated automatically as part of core business processes (*e.g.* periodic business risk assessments).
Verification and Validation	Basic mechanisms are in place to verify that risk analysis is performed as required, largely reliant on lagging indicators. The expertise for validation is generally lacking.	Verification and validation systems are in place to verify the efficiency of risk analysis activities and to validate their expediency (*e.g.* the organisation tracks that tools and techniques are being used correctly and that the correct tools and techniques are being used).
Feedback and Organisational Learning	The risk analysis tool suite is reviewed and modified on an event-driven basis.	Feedback is actively used to improve the execution of risk analysis (*e.g.* gaps identified and risk analysis tools and techniques improved in response).
Stakeholder Engagement	Risk analysis processes generally reside within the responsible unit, with limited cross-functional or external consultation.	Risk analysis processes generally reside within affected disciplines, and stakeholders work together to define and implement an integrated approach to risk analysis, capitalising on synergies and collective knowledge.
Competence	Detailed knowledge of risk analysis resides only within the responsible unit.	Most involved staff exhibit a good level of competence in the selection and application of risk analysis tools and techniques, and have access to support from internal or external expert risk practitioners.
Resources	Adequate resources are provided in support of risk analysis, with both qualitative and quantitative tools and techniques available.	Sufficient resources are provided in support of risk analysis, a portion of which is made available for R + D for risk assessment. A broad range of qualitative and quantitative tools and techniques are available and applied, including methodologies for aggregating and comparing risks.
Documentation and Reporting	Risk analysis outputs are compiled and disseminated in a format that supports decision making.	Risk analysis outputs are compiled and disseminated in a clear, concise and actionable format that supports real-time decision making, and their reporting is co-ordinated with other risk reporting mechanisms (*e.g.* risk status updates).

Table 1. L3 and L4 process maturity in risk analysis.

Domain	**Improvement step**
Process enablement	• Identify and allocate sufficient resources in support of risk analysis, updating them as necessary to reflect changing needs. • Identify key internal and external stakeholders (*e.g.* representatives of different functions or divisions of the business) and define their potential contributions (*e.g.* synergies from collective knowledge and advice, *etc.*) and requirements (*e.g.* involvement in assessing cross business impacts). • Establish mechanisms to involve identified stakeholders (*e.g.* cross-functional working groups).
Process evaluation	• Establish formal mechanisms (*e.g.* periodic reviews, audits, status reports, milestones, *etc.*) to verify that risk analysis adheres to its formal description, policies, and procedures, **and** is being performed efficiently. • Designate 'ownership' of verification to a responsible individual(s). The individual(s) is responsible for ensuring verification is performed, reviewing the findings, and recommending corrective action where necessary. Stakeholders should be involved as appropriate (*e.g.* staff not conforming to established procedures). • Define and collect measures to support verification of adherence **and** efficiency (*e.g.* task and activity checklists, cost of analyses, timeliness of analyses, *etc.*). • Establish formal mechanisms (*e.g.* periodic reviews, external advice, status reports, *etc.*) to validate the process of risk analysis. Candidates for validation include the methods and procedures for risk analysis (*e.g.* the tools and techniques applied) and the risk analysis outputs (*e.g.* do the analysis outputs inform decision making). • Designate 'ownership' of validation to a responsible individual(s). The individual(s) is responsible for ensuring validation is performed, reviewing the findings, and recommending corrective action where necessary. Stakeholders should be involved as appropriate (*e.g.* where changes to the tool suite or procedures are recommended, the process 'owners' would be involved). • Define and collect measures to support validation of risk analysis (*e.g.* internal assessments by decision makers of the value of risk analysis outputs, formal validation of risk analysis methodologies, *etc.*). • Establish mechanisms to compare in-house risk analysis with industry practice, making changes where appropriate (*e.g.* benchmarking initiatives, strategic information exchange, *etc.*).

Table 2. Steps for progressing between levels 3 and 4 in risk analysis.