Appendix A

Poster presentation of performance measurement framework for risk management

Performance Measurement for Risk Management

B. H. MacGillivray[1], S.J.T. Pollard[1], P.D. Hamilton[2] and J.E. Strutt[3]

[1]Integrated Waste Management Centre, [2] School of Water Sciences and [3]Reliability Engineering and Risk Management Centre,
Cranfield University, Cranfield, Bedfordshire, MK43 0AL, UK

Introduction

Financial restrictions, regulatory pressures and sectoral restructuring are encouraging water utilities to move from technically biased, risk-averse management approaches towards more commercial, business-oriented practices. To manage and indeed exploit this transition, many within the sector are in the process of formalising and making explicit approaches to risk management that have formerly been implicit. Whilst the sector has made excellent progress towards setting its goal of providing wholesome, safe drinking water that has the trust of customers within a risk management context, there are practical issues of implementation to be addressed. One of the key difficulties utilities are facing is managing the interfaces between high level corporate objectives, business plans and operational reality - in other words, translating strategy into action. In response, we are currently developing a performance measurement framework for risk management, an action predicated on the belief that the placing of risk exposure metrics within a structured framework can provide the catalyst for operationalising risk management strategy.

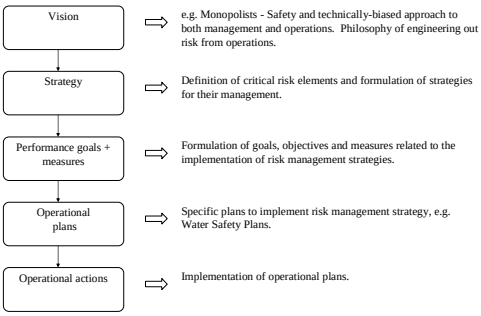

Figure 1. The hierarchy of risk management strategy (after Mintzberg, Simons)

Model Fundamentals

The core intention of this work is to provide a means for operationalising risk management strategy, the principle being that through measurement, management actions are stimulated, and it is through these management actions that organisational strategies are realised (Figure 1). Additionally, early findings of our related research suggest that a core barrier to effective risk management in utilities is that managers are struggling to define their data requirements, let alone their data collection and analysis processes. It is proposed that the placement of risk exposure indicators within a structured framework will go some way to countering this, by simplifying and clarifying data for decision-makers, highlighting core issues, and drawing attention to trends – in other words, collecting data and turning it into information.

The model structure (Figure 2) is an adaptation of the OECD's Pressure-State-Response indicator framework commonly applied to environmental problems. In essence, the adapted model represents the causal chain that links the drivers of core risk elements to their ultimate business impacts. The fundamental components of the model are outlined below:

Risk drivers – the core indicators and associated variables (metrics) that can induce changes in the state of the risk element;
Risk state – the core metrics that describe the state of the risk element, which in turn drives the business impact;
Risk impact – the core metrics that describe the **risk of** business impact, commonly defined in operational and financial terms.
Risk response – management responses to risk, according to the following hierarchy: risk reduction (e.g. redesigning the treatment process), risk control (e.g.process monitoring and control), and contingency planning (e.g. outbreak protocols). These responses are informed by and explicitly linked to the metrics at the driver, state and impact level.

The risk causality model is applied to the core risk elements specific to the water utility sector. Thus, a series of models exist, each of which is comprised of a set of metrics which represent the current condition of each constituent of the causal chain (Table 1). Taken together, these models represent a performance measurement framework for risk management.

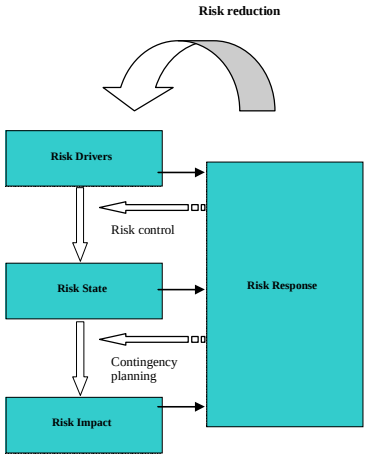

Figure 2. DSIR causality model for risk management (black arrows denote information flows)

Risk Element	Risk Driver	Risk State	Risk Impact
Catchment	Variability in diffuse pollution (from statistical aggregates and conceptual models); Variability in point source pollution (monitoring data);	Variability in catchment water quality (key indicators);	Operational costs (e.g. remediation costs); Financial costs (e.g. regulatory fines and penalties);
Network	Variability in supply; Variability in demand; Variability in network capability;	Network reliability; Network resiliency; Network vulnerability;	Operational costs (e.g. repair and work around costs); Financial costs (e.g. regulatory fines and penalties);
Treatment	Variability in process capability; Variability in source water quality;	Treatment reliability; Treatment resiliency; Treatment vulnerability;	Operational costs (e.g. repair and work around costs); Financial costs (e.g. regulatory fines and penalties);
Employee Retention	Employee development; Employee empowerment; Employee remuneration; Industry and profession-specific retention trends;	Turnover ratio; Average years service; Downtime;	Costs of recruitment; Costs of retraining; Costs of disruption;
Occupational Health and Safety	Education and training in H+S; Inherent hazard level; Safety culture;	Accident rates; Illness and injury rates; Work days lost; Near misses;	Operational costs (e.g. costs of disruption); Financial costs (e.g. penalties, fines and court costs);
Cash flow	Variability in outgoing cash flow components (e.g. taxes, labour, materials and energy); Variability in incoming cash flow components (e.g. commercial and domestic, or by product offering);	Variability in net post tax and operating cash flow;	Risk of deficit in operational cash requirements; Risk of financial default; Risk of shareholder default;
Supply Chain	Supply chain capability; Supply chain flexibility; Supply chain criticality;	Supply chain reliability; Supply chain resiliency; Supply chain vulnerability; (all in terms of cost, quality and timeliness)	Direct operational costs; Indirect operational costs (e.g. impact of variations in quality and timeliness of products or services on the business);

Table 1. Basic outline of key indicators associated with each risk element, by reference to each constituent of the causal chain

Conclusions

We are currently developing pilot versions of the model specific to the core risk elements inherent to the water sector. These include catchment management, network and treatment operations, supply chain management, employee retention, occupational health and safety, and cash flow management. Upon completion of this process, the next step is to test the value and pragmatism of our approach by refining and applying the pilot models within the sector.

Acknowledgements

Brian MacGillivray is part supported by a research grant awarded by the American Water Works Association (AwwaRF RFP 2939), and co-funded by an Engineering and Physical Sciences Research Award. His attendance at this workshop has been generously funded by the Royal Academy of Engineering. The opinions expressed herein are the authors' alone.

Appendix B

Descriptions of the maturity hierarchy for each process included in the RM-CMM

Strategic risk planning maturity hierarchy	
LEVEL 5 Optimised	**Scope** - Strategic risk planning and the associated risk framework (detailing core roles, responsibilities, accountabilities and mechanisms for risk management) address all types of risks across all areas of the organisation, with procedures in place for the management of opportunities as well as adverse consequences. Risk policies and guidelines enable the alignment of operational procedures with long-term risk strategy.
	Integration - Strategic risk planning is fully aligned with broader business planning, with explicit links established between risk management objectives and corporate objectives (*e.g.* supply / demand objectives incorporate measures of uncertainty).
	V + V - Management continually establishes measurable targets for improving risk management, with systems in place to verify their achievement and to validate the expediency of their enabling strategies.
	FB / OL - Feedback is actively used to improve risk planning and the development of strategies and policies, enabling changes to organisational structures and practices to optimise conditions for implementing the risk management strategy.
	FB / OL - Risk management goals and objectives and related plans are proactively modified in light of internal and external changes and influences on the business.
	Competence - The organisation is conversant with international practice in strategic risk planning and is active in improving this, with all involved staff, including executive management, fully cognisant of the methods and implications of strategic risk planning.
	Resources - Resources for implementing risk strategy are sufficient and allocated optimally and flexibly in response to need, and the organisation applies formal cost-benefit analysis in support of resource allocation (*i.e.* can quantify the 'value' of different strategies, and resources their implementation accordingly).
LEVEL 4 Managed	**Scope** - Strategic risk planning and the associated risk framework (detailing core roles, responsibilities, accountabilities and mechanisms for risk management) address risks at all levels of the company and across all functional boundaries of the business. Established policies and guidelines guide the implementation of risk strategy at the operational level.
	Integration - Strategic risk planning is automatically initiated as part of routine business planning and is co-ordinated with broader business planning (*e.g.* risk planning and broader business planning cycles are aligned).
	V + V - Risk management goals and objectives have measurable performance indicators, with systems in place to track progress in their achievement and to validate the expediency of their enabling strategies.
	FB / OL - Senior management review the validity of risk strategies and policies on a periodic and event-driven basis, making modifications based on feedback from the risk management committee, corporate experiences, regulatory input, *etc.*
	SE - Cross-functional teams and key external stakeholders work together to define and implement an integrated approach to risk planning, and core plans and strategies are endorsed across individual business units and by key external stakeholders (*e.g.* shareholders, regulators).
	Competence - The organisation is conversant with sectoral practice in strategic risk planning and makes efforts to exceed this, with most involved staff aware of the methods and implications of strategic risk planning.
	Resources - Sufficient resources are provided to implement risk management strategy.
LEVEL 3 Defined	**Scope** - Strategic risk planning is defined and documented, resulting in a tailored risk framework (detailing core roles, responsibilities, accountabilities and mechanisms for risk management) addressing a broad range of risks which is applied across core business areas. Policies and guidelines are established for risk management.
	Integration - Procedures are in place to initiate strategic risk planning.
	V + V - Basic mechanisms are in place to verify progress in the achievement of risk management goals and objectives, largely reliant on lagging indicators. The expertise for validation is generally lacking.
	FB / OL - Risk strategies and policies are reviewed on an event-driven basis and streamlined.
	SE - Strategic risk planning responsibilities generally reside within one group (*e.g.* executive management), with limited cross-functional or external consultation.
	Competence - The organisation is conversant with regulatory requirements for risk management and their planning exceeds these boundaries, with detailed knowledge of the methods and implications of strategic risk planning resident with senior (*i.e.* experienced) responsible staff.
	Resources - Adequate resources are provided to implement risk management strategy.
LEVEL 2 Repeatable	**Scope** - Basic process established for strategic risk planning, focused on meeting basic regulatory requirements and addressing 'mission-critical' risks.
	Integration - Strategic risk planning is reactive, often initiated in response to an event or situation.
	FB / OL - Strategic risk planning is based on regulatory guidance and previous experience, regardless of applicability or currency.
LEVEL 1 Initial	No formal process in place for strategic risk planning. *Ad-hoc* approach. Limited awareness of regulatory requirements for risk management.

Establishing risk acceptance criteria maturity hierarchy	
LEVEL 5 Optimised	**Scope** - Risk acceptance criteria are developed for all types of risk across all areas of the organisation, and their establishment is often (*e.g.* for key assets) informed by formal cost-benefit analysis.
	Scope - Criteria are in place to guide the balancing of business opportunities with adverse consequences (*e.g.* detailing whether international expansion is acceptable in risk terms).
	Integration -The development of risk acceptance criteria is a continual, explicit component of all business processes, forming part of the organisational culture.
	FB / OL - Feedback provides the organisation with an understanding of the relationship between its set levels of risk acceptance and business performance (*i.e.* the relationship between risk and reward), and risk acceptance criteria evolve based on this knowledge to provide a more effective balance of risk and reward.
	FB / OL - Risk acceptance criteria are proactively modified in light of internal and external changes and influences on the business.
	Competence - The organisation is active in developing international risk acceptance criteria, to form best practice, with all involved staff, including management, fully cognisant of the methods and implications of developing risk acceptance criteria.
LEVEL 4 Managed	**Scope** - Risk acceptance criteria are developed, with an appropriate degree of quantification (*e.g.* for key assets) and consistency, for risks at all levels of the company and across all functional boundaries of the business.
	Scope - Risk acceptance criteria are allocated at the asset and business unit level.
	Integration - Risk acceptance criteria are automatically developed as part of core business processes.
	V + V - Systems are in place to verify that risk acceptance criteria are uniformly adhered to and to validate the expediency of established criteria.
	FB / OL - Feedback is actively used to revise the process through which risk acceptance criteria are developed.
	SE - Cross-functional staff and key external stakeholders (*e.g.* regulators) provide input to the process of developing risk acceptance criteria.
	Competence - The organisation is conversant with sectoral practice in developing risk acceptance criteria and makes efforts to exceed this, with most involved staff aware of the methods and implications of developing risk acceptance criteria.
LEVEL 3 Defined	**Scope** - A defined, documented process is in place to develop risk acceptance criteria for a broad range of risks across core business areas.
	Scope - Risk acceptance criteria are allocated at the asset level.
	Integration - Procedures are in place to initiate the development of risk acceptance criteria.
	V + V - Basic mechanisms are in place to verify adherence to risk acceptance criteria, largely reliant on lagging indicators. The expertise for validation is generally lacking.
	FB/ OL - The organisation reviews and modifies risk acceptance criteria on an event-driven basis.
	SE - The responsibility for developing risk acceptance criteria generally resides within one group (*e.g.* risk management committee or executive management), with limited cross-functional or external consultation.
	Competence - The organisation is conversant with regulatory requirements for risk acceptance (*e.g.* risk based water quality standards) and makes efforts to exceed these, with detailed knowledge of the methods and implications of developing risk acceptance criteria resident with senior (*i.e.* experienced) responsible staff.
LEVEL 2 Repeatable	**Scope** - Basic process in place to develop risk acceptance criteria, generally through regulation and standards. The organisation may define its own acceptance criteria for 'mission-critical' risks.
	FB / OL - Risk acceptance criteria are retrospective and historical, regardless of applicability or currency, with limited organisational ability to plan ahead or learn from experience.
LEVEL 1 Initial	No formal process in place to develop risk acceptance criteria. *Ad-hoc* approach. Inappropriate use of standards.

Risk analysis maturity hierarchy	
LEVEL 5 – Optimised	**Scope** - Organisation is regarded as 'best practice' in risk analysis both nationally and internationally, with comprehensive and proactive identification, assessment, evaluation (with respect to acceptance criteria), establishment of causality and linking (common cause and dependent) all types of risk across all areas of the organisation, using a 'fit-for-purpose' range of tools and techniques.
	Scope - Risk analysis extends to include the risk based evaluation of business opportunities.
	Integration - Risk analysis is a continual, explicit component of all business processes, forming part of the organisational culture.
	V + V - Management continually establishes measurable targets for improving the risk analysis process, with systems in place to verify their achievement and to validate the means through which they are pursued.
	FB / OL - Feedback is actively used to improve both the execution and philosophy of risk analysis, and further enables the adaptation of organisational structures and practices to optimise its ability to perform risk analysis.
	Competence - High level of competence among all staff, including management, involved in risk analysis, with extensive experience / expert advice used to assist the selection and application of the most appropriate tools and techniques for risk analysis (*e.g.* the organisation knows where and when to source expert assistance, worldwide).
	Resources - Resources for risk analysis are sufficient and allocated optimally and flexibly in response to need.
	Resources - The organisation is active in researching and developing improved tools and techniques for risk analysis, with appropriate resources made available.
LEVEL 4 – Managed	**Scope** - 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 - Risk analysis is initiated automatically as part of core business processes (*e.g.* periodic business risk assessments).
	V + V - 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).
	FB / OL - Feedback is actively used to improve the execution of risk analysis (*e.g.* gaps identified and risk analysis tools and techniques improved in response).
	SE - 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 - 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 - 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.
	D + R - 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).
LEVEL 3 – Defined	**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.
	Integration - Procedures are in place to initiate risk analysis processes.
	V + V - 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.
	FB / OL - The risk analysis tool suite is reviewed and modified on an event-driven basis.
	SE - Risk analysis processes generally reside within the responsible unit, with limited cross-functional or external consultation.
	Competence - Detailed knowledge of risk analysis resides only within the responsible unit.
	Resources - Adequate resources are provided in support of risk analysis, with both qualitative and quantitative tools and techniques available.
	D + R - Risk analysis outputs are compiled and disseminated in a format that supports decision-making.
LEVEL 2 – Repeatable	**Scope** - Basic risk analysis process is in place, following basic regulatory requirements and addressing 'mission-critical' risks, but with no internal requirement and no appetite to go beyond what is required by regulation.
	Integration - Risk analysis is reactive, often initiated in response to an event or situation, or even to justify decisions.
	FB / OL - Risk analysis is largely rule-based, regardless of context; or mirrors past projects, with limited organisational ability to plan ahead or learn from experience.
	Resources - Limited range of tools and techniques available and applied for risk analysis.
LEVEL 1 – Initial	No formal process in place for risk analysis. *Ad-hoc* approach. Limited awareness of regulatory requirements for risk analysis.

	Risk based decision making and review maturity hierarchy
LEVEL 5 Optimised	**Scope** - Risk based decision-making proactively addresses all types of risk across all areas of the organisation and extends to include the risk based consideration of business opportunities, and is often informed by formal cost-benefit analysis (*e.g.* for critical decisions).
	Scope - The organisation understands how decisions on risk will influence organisational performance (*e.g.* can link the organisational risk profile to corporate performance), and develops risk response strategies with reference to broader organisational objectives.
	Integration - Risk based decision-making is a continual, explicit component of all business processes, forming part of the organisational culture.
	FB / OL - Feedback (from the risk monitoring process) on the evolution of risks is actively used to revise and adapt decision-making, and to explicitly question the principles and values that underlay 'problem' decisions.
	FB / OL - Risk response strategies / risk based decisions are proactively modified to adapt to internal and external changes and influences on the business.
	Competence - The organisation is able to go beyond the use of risk analysis outputs for answers (*e.g.* can intuitively develop risk response strategies where data is deficient), and considers the adaptation of organisational structures and practices to address the root causes of risk (*i.e.* changing the nature of its operations as part of its response to risk).
LEVEL 4 Managed	**Scope** - Risk based decision-making is actively practised in accordance with risk policies and guidelines at all levels of the company and across all functional boundaries of the business.
	Scope - Risk based decisions are made with reference to the business unit and organisational risk profile, but without subverting functional priorities.
	Integration - Risk based decision-making is automatically initiated as part of core business processes.
	V + V - Risk response strategies have measurable performance indicators (*e.g.* triggers and indicators established to highlight the need for revision), with systems in place to track progress and to validate their expediency (these mechanisms are informed by the risk monitoring process).
	FB / OL - Feedback (from the risk monitoring process) on the evolution of risks is actively used to revise and adapt decision-making.
	SE - Risk based decision-making responsibilities generally reside within affected disciplines, and cross-functional stakeholders work together to define and implement an integrated approach to risk based decision-making, with input from key external stakeholders (*e.g.* regulatory bodies) where appropriate.
	Competence - Risk analysis outputs are integral to risk based decision-making, and the organisation can develop an extended range of effective risk response strategies with reference to the life-cycle implications of risks.
LEVEL 3 Defined	**Scope** - Risk based decision-making is defined, documented and practised with reference to risk policies and guidelines, addressing a broad range of risks across core business areas.
	Scope - Risk based decisions are made with reference to traditional functional priorities (*e.g.* in engineering, finance).
	Integration - Procedures are in place to initiate risk based decision-making.
	V + V - Basic mechanisms are in place to track whether risk response strategies are meeting their objectives, largely reliant on lagging indicators (informed by the risk monitoring process). The expertise for validation is generally lacking.
	FB / OL - Risk based decisions / risk response strategies are reviewed and modified on an event-driven basis.
	SE - Risk based decision-making responsibilities generally reside within one group (*e.g.* risk management committee), with limited cross-functional or external consultation.
	Competence - The organisation understands how to use risk analysis outputs to inform risk based decision-making, and selects from a broad range of risk response strategies.
LEVEL 2 Repeatable	**Scope** - A basic process is in place for risk based decision-making, focused on repeating previously successful activities in order to manage critical risks, rather than on the explicit consideration of risk analysis outputs.
	Scope - Risk based decisions are largely made with reference to regulatory requirements, often in isolation of business considerations and context.
	Integration - Risk based decision-making is reactive, often initiated in response to an event or situation.
	FB / OL - Risk based decision-making is largely rule-based, regardless of context; or mirrors past projects, with limited organisational ability to plan ahead or learn from experience.
LEVEL 1 Initial	No structured approach established for risk based decision-making, with decisions taken on an *ad-hoc* basis. Limited cognisance of risk analysis outputs.

Risk response maturity hierarchy	
LEVEL 5 Optimised	**Scope** - Organisation is regarded as 'best practice' in risk response at both the national and international level, with comprehensive and proactive response to all types of risk across all areas of the organisation.
	Integration - Risk response is a continual, explicit component of all business processes, forming part of the organisational culture.
	V + V - Management continually establishes measurable targets for improving risk responsiveness, with systems in place to verify their achievement and to validate the means through which they are pursued.
	FB / OL - The organisation uses feedback to link the efficacy of its risk response efforts to business unit / organisational performance (*e.g.* by linking measures of residual risk to performance), acting as a spur for continual improvements in risk response.
	FB / OL - Feedback is actively used to improve the implementation of risk response strategies, and further enables the adaptation of organisational structures and practices to optimise its ability to respond to risk.
	FB / OL - The methods and techniques used in implementing risk response strategies are proactively modified to adapt to internal and external changes and influences on the business.
	Competence - High level of competence among all staff, including management, involved in implementing risk response strategies.
	Resources - Resources for implementing risk response strategies are sufficient and allocated optimally and flexibly in response to need.
LEVEL 4 Managed	**Scope** - A controlled process is in place containing detailed criteria, methods and guidelines to manage the implementation of risk response strategies at all levels of the company and across all functional boundaries of the business.
	Integration - Risk response processes are automatically initiated as part of core business processes.
	V + V - Systems are in place to verify that risk response strategies are implemented efficiently, and to validate the expediency of implementation techniques.
	FB / OL - Feedback is actively applied to improve the implementation of risk response strategies (*e.g.* gaps identified and risk response techniques improved in response).
	SE - Risk response processes generally reside within affected disciplines, and internal and external stakeholders work together to define and implement an integrated approach to risk response, capitalising on synergies and collective knowledge (*e.g.* common cause risks are addressed in a co-ordinated fashion, local industry and agriculture play their part in risk response, *etc.*).
	Competence - Most involved staff exhibit a good level of competence in the implementation of risk response strategies, and have access to support from internal or external expert risk practitioners.
	Resources - Sufficient resources are provided in support of risk response.
LEVEL 3 Defined	**Scope** - A defined, documented process is in place containing criteria, methods and guidelines for implementing risk response strategies, addressing a broad range of risks across core business areas.
	Integration - Procedures are in place to initiate risk response processes.
	V+ V - Basic mechanisms are in place to verify that risk response strategies are implemented as required, largely reliant on lagging indicators. The expertise for validation is generally lacking.
	FB / OL - The implementation of risk response strategies are reviewed and modified on an event-driven basis (*e.g.* in response to failures).
	SE - Risk response processes generally reside within the responsible unit, with limited cross-functional or external consultation.
	Competence - Competency in the implementation of risk response strategies resides only within the responsible unit.
	Resources - Adequate resources are provided for the implementation of risk response strategies.
LEVEL 2 Repeatable	**Scope** - Basic process in place for the implementation of risk response strategies, following basic regulatory requirements and addressing 'mission-critical' risks, but with no internal requirement and no appetite to go beyond what is required by regulation.
	Integration - Risk response is reactive, often initiated in response to an event or situation.
	FB / OL - Risk response is largely rule-based, regardless of context; or mirrors past projects, with limited organisational ability to plan ahead or learn from experience.
LEVEL 1 Initial	No formal process in place for implementing risk response strategies. *Ad-hoc* approach. Dependence on individual heroics.

Risk monitoring maturity hierarchy	
LEVEL 5 Optimised	**Scope** - Organisation is regarded as 'best practice' at both the national and international level in risk monitoring, with comprehensive and proactive monitoring of all types of watched and mitigated risks across all areas of the organisation, using a 'fit-for-purpose' range of tools and techniques.
	Scope - The process extends to include the risk based monitoring of business opportunities (*e.g.* tracking changes in the Net Present Value of investment opportunities).
	Integration - Risk monitoring is a continual, explicit component of all business processes, forming part of the organisational culture.
	V + V - Management continually establishes measurable targets for improving the risk monitoring process, with systems in place to verify their achievement and to validate the means through which they are pursued.
	FB / OL - The organisation uses feedback to link trends in the evolution of the (aggregate) organisational risk profile to both organisational behaviour (*i.e.* can source organisational practices that are influencing the risk profile) and organisational performance (*i.e.* can show how variations in the aggregate risk profile influence performance).
	FB / OL - Feedback is actively used to improve both the philosophy and execution of risk monitoring, and further enables the adaptation of organisational structures and practices to optimise its ability to perform risk monitoring.
	Competence - High level of competence among all staff, including management, involved in risk monitoring.
	Resources - Resources for risk monitoring are sufficient and allocated optimally and flexibly in response to need.
	Resources - The organisation is active in researching and developing improved tools and techniques to enhance risk monitoring, with appropriate resources available.
LEVEL 4 Managed	**Scope** - A controlled process is in place containing detailed criteria, methods and guidelines to manage the monitoring of watched and mitigated risks at all levels of the company and across all functional boundaries of the business.
	Scope - The organisation monitors changes in the (aggregate) risk profile at the organisational and business unit level.
	Integration - Risk monitoring processes are automatically initiated as part of core business processes.
	V + V - Systems are in place to verify the efficiency of risk monitoring activities (*i.e.* the organisation tracks that monitoring activities are performed and to the required standard) and to validate their expediency.
	FB / OL - Feedback is actively used to improve the execution of risk monitoring processes (*e.g.* gaps identified and risk monitoring techniques improved in response).
	SE - Risk monitoring processes generally reside within affected disciplines, and stakeholders work together to define and implement an integrated approach to risk monitoring, capitalising on synergies and collective knowledge (*e.g.* related risks are addressed in a co-ordinated fashion, water quality regulators provide input, *etc.*).
	Competence - Most involved staff exhibit a good level of competence in applying risk monitoring techniques, and have access to support from internal or external expert risk practitioners.
	Resources - Sufficient resources are provided in support of risk monitoring, a portion of which is made available for R + D in risk monitoring.
	D + R - Risk status updates (*e.g.* 'red', 'green', 'amber') 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.
LEVEL 3 Defined	**Scope** - A defined, documented process is in place containing criteria, methods and guidelines for the monitoring of a broad range of watched and mitigated risks across core business areas. The organisation is conversant with and goes beyond regulatory requirements for risk monitoring.
	Integration - Procedures are in place to initiate risk monitoring processes.
	V + V - Basic mechanisms are in place to verify that risk monitoring activities are performed as required, largely reliant on lagging indicators. The expertise for validation is generally lacking.
	FB / OL - Risk monitoring activities are reviewed and modified on an event-driven basis.
	SE - Risk monitoring processes generally reside within the responsible unit, with limited cross-functional or external consultation.
	Competence - Detailed knowledge of risk monitoring techniques resides only within the responsible unit.
	Resources - Adequate resources are provided in support of risk monitoring.
	D + R - Risk status updates are compiled and disseminated in support of risk based decision-making.
LEVEL 2 Repeatable	**Scope** - Basic processes are in place to monitor watched and mitigated risks, following basic regulatory requirements and addressing 'mission-critical' risks, but with no internal requirement and no appetite to go beyond what is required by regulation.
	Integration - Risk monitoring is reactive, often initiated in response to an event or situation.
	FB / OL - Risk monitoring is largely rule-based, regardless of context; or mirrors past projects, with limited organisational ability to plan ahead or learn from experience.
	Resources - Limited range of tools and techniques available and applied for risk monitoring.
LEVEL 1 Initial	No formal processes in place for risk monitoring. *Ad-hoc* approach. Limited awareness of regulatory requirements for risk monitoring.

Integrating risk management maturity hierarchy	
LEVEL 5 Optimised	**Scope of functional integration** - Management has defined and implemented a strategy for integrating risk management enterprise-wide, focused on integrating the management of risk towards broader corporate objectives (without subverting functional priorities). This is enabled by flexible management and organisational structures and an understanding of how the organisational risk profile influences corporate performance.
	Integration within business - Risk management processes are continual, explicit components of all business processes, forming part of the organisational culture.
	Integration within business - Company culture, policies, and reward and accountability systems promote the management of risk as 'part of everyone's job'.
	V + V of interface integration - Verification and validation systems enable continuous improvement of risk management, such that changes to individual risk management processes have minimal impact on risk management processes with which they interface.
	FB / OL - Feedback is actively used to improve the integration process, and further enables changes to organisational structures and practices to optimise the integration of risk management across the business.
	Competence - All involved staff, including management, are fully cognisant of the methods and implications of integrating risk management.
	Resources - Resources for integrating risk management are sufficient and allocated optimally and flexibly in response to need.
LEVEL 4 Managed	**Scope of functional integration** - Management has defined and implemented a strategy for integrating risk management at all levels of the organisation and across all functional boundaries of the business, focused on integrating the management of risk towards business unit and organisational risk profiles (without subverting functional priorities).
	Integration within business - Risk management processes are automatically initiated as part of core business processes.
	V + V of interface integration - Risk management process interfaces are understood and controlled, with procedures in place to co-ordinate them (*e.g.* technical exchange, reviewing inputs from each other, follow-up mechanisms to ensure appropriate responses are made in light of changes to monitored risks, *etc.*) and systems in place to verify and validate their co-ordination.
	FB / OL - Senior management review the integration of risk management on a periodic and event-driven basis, modifying established strategy based on feedback from the risk management committee, corporate experiences, regulatory input *etc.*
	SE - Stakeholders work together to define and implement the integration of risk management across the organisation (*e.g.* extensive cross-functional co-operation, the engaging of regulatory bodies, *etc.*).
	Competence - Most involved staff are aware of the methods and implications of integrating risk management.
	Resources - Sufficient resources are provided in support of integrating risk management.
LEVEL 3 Defined	**Scope of functional integration** - Management has defined and implemented a strategy for integrating risk management across core business areas, focused on integrating the management of risk towards functional priorities (*e.g.* engineering, finance).
	Integration within business - Procedures are in place to initiate risk management processes within core business processes.
	V + V of interface integration - Risk management process interfaces are identified and defined, with guidelines describing how they should interact (*e.g.* detailing how, when and to whom risk analysis outputs should be disseminated) and basic mechanisms are in place to verify their interactions. The expertise for validation is generally lacking.
	FB / OL - The integration of risk management is reviewed and modified on an event-driven basis.
	SE - Responsibility for integrating risk management generally resides with one group (*e.g.* risk management committee).
	Competence - Detailed knowledge of the methods and implications of integrating risk management resides only within the responsible group.
	Resources - Adequate resources are provided in support of integrating risk management.
LEVEL 2 Repeatable	**Scope of functional integration** - Risks are largely managed with reference to basic regulatory requirements, often in isolation of functional considerations and context
	Integration within business - Risk management processes are reactive, often initiated in response to events or situations.
	V + V of interface integration - Attempts to co-ordinate risk management process interfaces are initiated only when dependency failures are encountered (*e.g.* when risk monitoring data is found insufficient to inform the review of risk response strategies).
LEVEL 1 Initial	No formal efforts are made to integrate risk management. *Ad-hoc* approach. Limited cognisance of integrated risk management.

Supply chain risk management maturity hierarchy	
LEVEL 5 Optimised	**Scope** - Supply chain risk management encompasses the full risk implications of all supplier-organisation interfaces, addressing product / service risk from concept to delivery.
	Integration - Risk management is seamlessly integrated across the supply chain (*i.e.* the organisation and its suppliers manage risk as a team, using feedback to improve their risk management processes).
	V + V - Management continually establishes measurable targets for improving supply chain risk management, with systems in place to verify their achievement and to validate the means through which they are pursued.
	FB / OL - Feedback is actively used to revise the nature of supplier-organisation relationships and, if necessary, to adapt broader organisational structures and practices (*e.g.* bringing retailing back 'in-house') to optimise the management of risk across the supply chain.
	SE - Suppliers are actively supported and coached in their risk management efforts.
	Competence - The organisation is conversant with international practice in supply chain risk management and is active in improving this, with all involved staff, including management, fully cognisant of the methods and implications of managing supply chain risks.
	Resources - The organisation understands the extent to which different supplier-organisation interfaces influence its overall business performance, enabling the optimal and flexible allocation of sufficient resources in support of supply chain risk management activities.
	Resources - Risk based performance targets for suppliers are incentivised, acting as a spur for continual improvements.
LEVEL 4 Managed	**Scope** - A controlled process is in place to identify, analyse and manage the extended risk implications of all supplier-organisation interfaces, addressing technical, financial, delivery and reputational risks.
	Integration - Supply chain risk management is automatically initiated as part of core business processes.
	V + V - Pre-qualification, selection and retention criteria incorporate measurable risk based performance standards for all suppliers (*e.g.* requirements for the reliability, safety and technical competence of supplied products), and systems are in place to verify their adherence and to validate their expediency.
	FB / OL - Feedback on suppliers' risk based performance is evaluated in real-time with respect to agreed standards (though continuous improvement is not required) and is actively used to improve supply chain risk management (*e.g.* failures are responded to by increasing technical exchange with problem suppliers or altering selection criteria, *etc.*).
	SE - Co-operative relationships are established across the supply chain, encouraging suppliers to work *with* the utility in managing risk for mutual benefit, and all suppliers are encouraged to use an approved, tailored version of the organisation's defined risk management process.
	Competence - The organisation is conversant with sectoral practice in supply chain risk management and makes efforts to exceed this, with most involved staff aware of the methods and implications of managing supply chain risks.
	Resources - Sufficient resources are provided in support of supply chain risk management.
LEVEL 3 Defined	**Scope** - A defined, documented process is in place to identify and evaluate the broad risk implications of core supplier-organisation interfaces, addressing quality, costing and timeliness risks.
	Integration - Procedures are in place to initiate supply chain risk management activities.
	V + V - Pre-qualification, selection and retention criteria addressing risk are established for work performed by core suppliers, and basic mechanisms are in place to verify their adherence. The expertise for validation is generally lacking.
	FB / OL - Supply chain risk management activities are reviewed and modified on an event-driven basis.
	SE - Core suppliers are provided basic support in their risk management efforts (*e.g.* technical exchange and assistance), and are encouraged to implement a formal risk management process.
	Competence - Detailed knowledge of the methods and implications of supply chain risk management resides only within the responsible unit.
	Resources - Adequate resources are provided in support of supply chain risk management.
LEVEL 2 Repeatable	**Scope** - Basic procedures in place for supply chain risk management, following basic regulatory requirements and addressing 'mission-critical' risks, but with no internal requirement and no appetite to go beyond what is required by regulation.
	Integration - Supply chain risk management activities are reactive, often initiated in response to key failures across the supply chain.
	FB / OL - Supply chain risk management activities are based on standards and previous experience, regardless of applicability or currency, with limited organisational ability to plan ahead or learn from experience (*i.e.* the organisation manages risk through sticking with accredited suppliers and those who have performed well in the past).
LEVEL 1 Initial	No formal process in place to manage supply chain risks. *Ad-hoc* approach. Reliance entirely upon suppliers to manage risk.

Change risk management maturity hierarchy	
LEVEL 5 Optimised	**Integration** - Change management is a continual, explicit component of all business processes, forming part of the organisational culture.
	V + V - Management continually establishes measurable targets for improving the change management process, with systems in place to verify their achievement and to validate the means through which they are pursued.
	FB / OL - The organisation proactively responds to significant external changes (*e.g.* market restructuring, changes in the regulatory regime, *etc.*), often adapting organisational structures and practices to pre-empt their risk implications.
	FB / OL - Feedback from change management programmes and pilot tests is actively used to identify and disseminate best practices across the organisation, adapting organisational structures and practices where necessary.
	SE - Staff at all levels of the company are engaged in change management activities, creating an organisational culture which faces up to and adapts to change.
	Competence - The organisation is conversant with international practice in change management and is active in improving this, with all involved staff, including management, fully cognisant of the methods and implications of change management.
	Resources - The organisation understands the extent to which various change management programmes influence its overall business performance, enabling the optimal and flexible allocation of sufficient resources in support of change management.
	Resources - Pilot tests are performed prior to core internal changes to determine feasibility and improvement opportunities, with appropriate resources available.
LEVEL 4 Managed	**Scope** - A controlled process is in place to identify, evaluate (with respect to risk) and manage all changes, however sourced, which could significantly alter the organisational risk profile.
	Integration - Change management is automatically initiated as part of core business processes.
	V + V - The objectives of change management programmes are understood in measurable terms and systems are in place to verify their achievement (*e.g.* tracking that the effect of altering treatment design on process reliability is as desired) and to validate their expediency.
	FB / OL - Feedback on the progress of change management programmes is reviewed in real-time with respect to set objectives, and the execution of the process evolves based on this information.
	SE - Change management processes generally reside within the disciplines causing change (*e.g.* planning and scheduling, engineering), and are informed by cross-functional and external consultation.
	SE - Key external stakeholders (*i.e.* those responsible for, or similarly affected by, change) are mutual partners in change management (*e.g.* the organisation works with the water quality regulator to ensure that the outcome of water quality standard reviews are mutually acceptable).
	Competence - The organisation is conversant with sectoral practice in change management and makes efforts to exceed this, with most involved staff aware of the methods and implications of change management.
	Resources - Sufficient resources are provided in support of change management activities.
LEVEL 3 Defined	**Scope** - A defined, documented process is in place to identify and plan for the risk implications of organisational (*e.g.* re-engineering efforts), technical (*e.g.* alterations in design or manufacture) and regulatory (*e.g.* pricing reviews) change.
	Integration - Procedures are in place to initiate change management activities.
	V + V - Basic mechanisms are in place to verify that change management efforts are meeting their objectives, largely reliant on lagging indicators. The expertise for validation is generally lacking.
	FB / OL - Change management programmes are reviewed and modified on an event-driven basis.
	SE - Processes to manage change generally reside within one unit (*e.g.* planning and scheduling), with limited cross-functional or external consultation.
	Competence - Detailed knowledge of the methods and implications of change management resides only within the responsible unit.
	Resources - Adequate resources are provided in support of change management activities.
LEVEL 2 Repeatable	**Scope** - Basic processes are in place to manage critical changes, although the organisation cannot define the risk implications of change.
	Integration - Change management processes are reactive, often initiated in response to an event or situation (*i.e.* the organisation may be blind to change, responding only after the event).
	FB / OL - Change management activities are retrospective and historical, regardless of applicability or currency, with limited organisational ability to plan ahead or learn from experience.
LEVEL 1 Initial	No formal processes in place to manage change. *Ad-hoc* approach.

Education and training in risk management maturity hierarchy	
LEVEL 5 Optimised	**Scope** - Education and training in risk management is continuous and extends beyond operational aspects (*i.e.* ensuring staff can perform current roles) to develop broader knowledge structures to optimise risk management throughout the organisation (*e.g.* embedding a knowledge of how human factors and organisational structures and practices influence risk).
	Integration - Education and training in risk management is a continual, explicit component of all business processes, forming part of the organisational culture.
	V + V - Management continually establishes measurable targets for improving risk management education and training, with systems in place to verify their achievement and to validate the means through which they are pursued.
	FB / OL - Feedback is actively used to improve both the philosophy and execution of risk management education and training, and further enables the adaptation of organisational structures and practices to optimise its ability to educate and train staff in risk management.
	FB / OL - Risk management education and training programmes are proactively modified in response to internal and external changes and influences on the business.
	Competence - The organisation is conversant with international practice in education and training in risk management and is active in improving this, with all involved staff (*i.e.* trainers and educators) exhibiting a high level of competence.
	Resources - Resources for education and training in risk management are sufficient and allocated optimally and flexibly in response to need.
	Resources - Coaches are provided to support continuous development of individual or team competencies in risk management.
	Resources - Risk management performance is incentivised to encourage continuous development of skills and knowledge.
LEVEL 4 Managed	**Scope** - A controlled process is in place to manage the education and training of all staff in risk management, addressing the full range of technical and managerial aspects and applied at all levels of the company and across all functional boundaries of the business.
	Integration - Education and training in risk management is automatically initiated as part of core business processes.
	V + V - The required skills and knowledge (competencies) for effective risk management are understood in measurable terms (*e.g.* translated into performance data) and systems are in place to verify their development / maintenance and to validate the means through which they are developed / maintained.
	FB / OL - Skills and knowledge developed at the individual, team, unit and organisational level are evaluated against required competencies, and the execution of education and training programmes is evolved based on this feedback.
	SE - Stakeholders work together to define and implement an integrated approach to education and training across the organisation.
	Competence - The organisation is conversant with sectoral practice in risk management education and training and makes efforts to exceed this, with most involved staff (*i.e.* trainers and educators) exhibiting a good level of competence.
	Resources - Sufficient resources are provided in support of risk management education and training, with a wide range of formal and informal vehicles adopted to impart the required skills and knowledge, and staff have access to educational resources on risk management outside of the formal programme.
LEVEL 3 Defined	**Scope** - A defined, documented process is in place to educate and train core staff in risk management, addressing a broad range of technical and managerial issues and applied across core business areas.
	Integration - Procedures are in place to initiate education and training in risk management.
	V + V - Basic mechanisms are in place to verify that the skills and knowledge (competencies) required for effective risk management are developed / maintained through education and training, largely reliant on lagging indicators. The expertise for validation is generally lacking.
	FB / OL - Risk management education and training activities are reviewed and modified on an event-driven basis.
	SE - Responsibility for educating and training staff in risk management resides within one group
	Competence - Detailed knowledge of techniques and methods for educating and training staff in risk management resides only with senior involved staff (*i.e.* experienced trainers and educators).
	Resources - Adequate resources are provided in support of the risk management education and training, with both formal and informal vehicles adopted.
LEVEL 2 Repeatable	**Scope** - Education and training in risk management exists, but is restricted to ensuring that critical staff (*e.g.* finance, reliability engineering) have the required technical skills and knowledge to perform repeat functions in their current risk management roles.
	Integration - Education and training in risk management is reactive, often initiated in response to major failures in risk management.
	FB / OL - Education and training programmes are retrospective and historical, regardless of applicability or currency, with limited organisational ability to plan ahead or learn from experience.
	Resources - Risk management education and training requirements are largely undefined, and are largely reliant on informal vehicles (*e.g.* 'on the job' training).
LEVEL 1 Initial	No processes in place to develop or maintain risk management skills and knowledge. *Ad-hoc* approach. Limited cognisance of required competencies for effective risk management.

Risk knowledge management maturity hierarchy	
LEVEL 5 Optimised	**Scope** - Organisation is regarded as 'best practice' in risk knowledge management, possessing world class systems and infrastructure for recognising, creating, transforming and distributing risk knowledge, with the aims of satisfying operational risk management requirements and to develop organisational 'risk intelligence'.
	Integration - Risk knowledge management is a continual, explicit component of all business processes, forming part of the organisational culture.
	V + V - Management continually establishes measurable targets for improving risk knowledge management, with systems in place to verify their achievement and to validate the means through which they are pursued.
	FB / OL - Feedback is actively used to improve both the philosophy and execution of risk knowledge management processes, and further enables the adaptation of organisational structures and practices (*e.g.* changing incentive structures to encourage knowledge sharing and collaboration between traditionally 'competing' departments) to optimise risk knowledge management across the business.
	FB / OL - Risk information systems and supporting infrastructure are proactively modified to meet changing requirements and situations (*e.g.* as objectives and related risks change).
	Competence - The organisation is conversant with international practice in risk knowledge management and is active in improving this, with all involved staff, including management, possessing a high level of competence in the methods and techniques of risk knowledge management.
	Resources - Resources for risk knowledge management are sufficient and allocated optimally and flexibly in response to need.
	Resources - The organisation is active in researching and developing improved systems and infrastructure for risk knowledge management, with appropriate resources available.
LEVEL 4 Managed	**Scope** - The gathering, storage, analysis and management of risk knowledge is automated and networked across all levels of the organisation and across all functional boundaries of the business. The required granularity, volume and accuracy of risk information are defined.
	Integration - Risk knowledge management processes are automatically initiated as part of core business processes.
	V + V - Systems are in place to verify the efficiency of risk knowledge management processes (*e.g.* the organisation tracks the timeliness, relevancy, breadth and depth of risk information collected and disseminated with reference to defined requirements) and to validate their design (*e.g.* questioning whether the information infrastructure is best suited to meet process requirements).
	FB / OL - Feedback is actively used to improve the execution of risk knowledge management processes (*e.g.* failures identified and information infrastructure improved in response).
	SE - Internal and external stakeholders work together to define and implement an integrated approach to risk knowledge management (*e.g.* the organisation mutually exchanges risk information with regulators).
	Competence - The organisation is conversant with sectoral practice in risk knowledge management and makes efforts to exceed this, with most involved staff possessing a high level of competence in the methods and techniques of risk knowledge management.
	Resources - Sufficient resources are provided in support of risk knowledge management, a portion of which is made available for R + D in risk knowledge management.
	D + R - Risk information (*e.g.* risk analysis outputs, risk status updates) is compiled and disseminated in a clear, concise and actionable format that supports real-time decision-making, and risk reporting mechanisms are effectively co-ordinated.
LEVEL 3 Defined	**Scope** - A defined, documented and largely automated process for risk knowledge management is in place, providing a framework for the gathering, storage, analysis and distribution of risk information and applied across core business areas, with the aims of satisfying operational risk management requirements.
	Integration - Procedures are in place to initiate risk knowledge management processes.
	V + V - Basic mechanisms are in place to verify that the organisation is meeting its information requirements for risk management, largely reliant on lagging indicators. The expertise for validation is generally lacking.
	FB / OL - Risk knowledge management processes are reviewed and modified on an event-driven basis.
	SE - Risk information transfer is generally restricted within divisions or groups, with limited communication on risk across organisational boundaries.
	Competence - Detailed knowledge of the methods and techniques of risk knowledge management resides only within the responsible unit.
	Resources - Adequate resources are provided in support of risk knowledge management.
	D + R - Risk information (*e.g.* risk analysis outputs, risk status updates) is compiled and disseminated in a format that supports decision-making.
LEVEL 2 Repeatable	**Scope** - Basic processes have been established for the collection and storage of risk information, restricted to satisfying basic regulatory requirements and informing the management of 'mission-critical' risks.
	Integration - Risk knowledge management processes are reactive, often initiated in response to an event or a situation.
	FB / OL - Risk knowledge management systems and infrastructure are retrospective and historical, regardless or applicability or currency, with limited organisational ability to plan ahead or learn from experience.
LEVEL 1 Initial	No formal processes in place to manage risk data and information. *Ad-hoc* approach. Limited awareness of information requirements for risk management.

Key: D+R, documentation and reporting; V+V, verification and validation; FB / OL, feedback and organisational learning; SE, stakeholder engagement.

Appendix C

Sample RM-CMM questionnaire response (benchmarking survey)

Appendix D

Sample interview transcript from initial case study

Brian MacGillivray (BM) and Interviewee A (IA)

IA: …Risk champion meetings - we're looking for commentary or advice, not looking for advice on dealing with risk 356….they're not strategy meetings to deal with specific risks.

BM…and the role of the risk champions…

IA:…terms of reference…suggest, review, challenge and determine acceptability of proposals to improve risk management capability in their business streams. We're looking to embed risk management, to secure a common understanding of the range of initiatives that we may choose to undertake, their appropriateness, by refining the approach, make growth possible. What's emerged in recent discussions is the inappropriateness of setting specific objectives for capability improvement, and the appropriateness of weaving capability initiatives into existing plans and programmes. We went through your list of requirements, and the champions were able to influence my perception of initiatives that either they were running or they were aware of, some good ideas came out as to how they may fine tune that into the business…

BM: And the meetings are also intended to get reports back on implementation of policy framework, offer feedback, review?

IA: That's more of an aspiration than an active description, a lot of the traffic is still from me to them, making them aware of our plans and proposals; we're looking to get a more proactive stance from champions to come with ideas and feedback, they're more of an audience for our proposals, rather than being a challenging, innovative dialogue. It's about securing their time and engagement, turn out, of 8 champions, is typically between 3 and 5, rarely full house, there's no serial non attendees – they're engaged…my intention in future is to engage them in more strategic issues, but to a large extent we've dealt with strategic aspects, it's more about implementation, refinement of implementation.

BM: What's the process for drawing up policy, strategy documents, done in isolation by you, or input from (censored) and the Board?

IA: Primarily from myself, circulating written documents, they're reviewed by champions, and endorsement by (censored) forum. Current endorsed policy was subject to several iterations by champions; the board are endorsers, not developers.

BM: How do you determine success in risk management, how do you know if it's adding value?

IA: We've got the capability assessment process, what we lack is a process for determining risk management KPIs, what we are beginning to build are success stories from application of risk management principles, how might it work for me, how will it add value...

BM: …how do you know that the policy / strategy documents are valid, and verify that the implementation is effective…verification from champions….validation as its based on industry standards, board approvals, champion input, and from capability assessments?

IA: The description of feedback from the champions is appropriate for the most part to describe verification. In terms of validating that policy is effective, my counterpart in finance team is the service auditor, its my intention in the future to use his or (censored) resources to go in and find out how effective the application of the policy is.

BM: So you've got the matrix for comparing and evaluating significant types of risks, but how do you determine acceptability?

IA: There's no methodology for determining tolerability, we're at an earlier stage, trying to communicate the range of strategies for dealing with risks, the five Ts….in the monthly management reports there's a column with target score for top ten risks, which goes to board, only one of those risks has a target score… we need to give people the tools for selecting from the 5 Ts, and to provide them a framework for setting target scores and recording them in their management reporting line. While the top ten risks only go to the board, each co-ordinator reports to management team on a monthly basis on key exposures, I'd like to get them to set target scores.

BM: …at present business judgement as to the tolerability of risk, trying to develop a framework for standardising this?

IA: That's right.

BM: Drill down to asset management, methodology for explicitly balancing risk with cost, codes and standards, investment, ways of balancing risk with value?

IA: There may be methodologies within discrete areas of the business, to characterise there as being nothing there is unduly pessimistic, there will be tools there, but they exist as islands with no consistency or overlaying risk management policy or strategy.

BM: Looking at risk analysis, beyond the scoring matrix, what tools and techniques are employed?

IA: There's a raft of standard industry tools that are used according to circumstance, I'm aware of them conceptually, but what we don't have, because there's no business driver, is a map of where those tools are being used, for example FMECA, HAZOP, HAZCOM will be employed within business….the documentation guiding people as to which tools exist and where they are most suitable for application,

or the options available, the method of choice, there are draft documents in existence, but they're not yet formally adopted.

BM: At present, some criteria and guidelines, e.g. in construction, dam safety, but it varies… in programme management decisions, Monte Carlo analysis?

IA: …they're reasonably well established with practitioners, and middle management, part of business processes, but lacking is a coherent strategy for approaching risk analysis.

BM: Expertise resides within functions, streams, not core set of experts?

IA: Yes. The idea is that as the analysis process matures, the risk management team would be able to provide routes to the guidance documentation, would know the range of tools, the applicability of tools, will be able to signpost enquiries to lead experts in the use of those tools within the business, without understanding the nuts and bolts of the tools themselves.

BM: Is the application of these analysis tools verified…e.g. to sign of projects, monte carlo has to have been performed?

IA: Mechanisms for them to be done are built into approval process. Process for obtaining approval requires stages to complete, one of which will be Monte Carlo. As to whether they've been applied accurately and competently, there's probably not that many controls, its not like a set of engineering calculations where calculations are checked and countersigned.

BM: And are the analyses drawn up in manner that helps decision makers, or too technically biased, or not enough data to inform decision…how do you ensure risk analysis is informing decision making processes?

IA: ….the outputs not sitting on a shelf…. whether we're considering all the alternative strategies is another issue.

BM: Is there a separation between the risk analysis and decision making…?

IA: The project and programme managers and the lead director for business stream are the people that make the case for investment decisions to project approval group.

BM: More generally, e.g. for HAZOP, with the risk matrix, is the analyst responsible for the decision?

IA: The analyst is not responsible for decision, middle or senior manager responsible for decision, but the analyst will be party to briefing that individual so the decision should be made in the knowledge of

what the analysis is saying, it wont be the only component in decision making, but it should be visible to the decision maker.

BM: And in terms of decision making, would objectives we attached to risk based decisions, for example timescales, deliverables, is it goal oriented in terms of risk reduction?

IA: Behind the question is the implication that risk analysis is the primary and fundamental element in decision making. The majority of the goal orientation after the decision has been made will focus on cost and physical output, in large projects the risk element will continue to figure significantly – in the delivery of major information system, a significant focus was put on the management of the risk associated with achieving successful delivery of output – but with many other areas of the business, even fairly significant infrastructure investments, I suspect that the risk analysis that's done at the decision making stage is probably not carried forward and monitored at the level of detail that is desirable…

IA: How do you integrate decision making, to make it cross-functional?

IA: (censored) has struggled with cross-functional business structures in the past, one of the reasons we've gone back to a business stream orientation. A lot of the investment in cultural change in the organisation has been to address the pre-existing silo approach, a knowledge of the need for integration, for matrix management. There is the structure and cultural support for cross-silo discussion and agreement, but a lot of the thrust of the business is around business stream delivery, where the risks are contained within business silos themselves.

BM: And in terms of validating decisions…for example peer reviews, would these be deployed to ensure that you're adopting the right strategy to deal with risks?

IA: The management meetings are essentially the peer review, so you get a draft proposal, challenged by all of the directors or all of the managers from the different business streams, who have the opportunity to influence decisions from their perspective from where they sit in the business. If you're talking about post decision reviews, there are processes within our incident and our project delivery elements of the business for appraisal of what's gone before.

BM: Is there a defined risk monitoring process where you're acquiring, compiling and reporting data on evolution of risks…?

IA:…all risks on the register are encouraged to be monitored on a regular basis, more significant ones are brought to management meetings on a monthly basis, and there are staggered management reports that occur at two-weekly intervals that reflect the adequacy of maintenance of the content of significant risks on the database.

BM: Are mechanisms in place to verify that risk monitoring is performed as required, and to the required standard?

IA: Steve is responsible for overseeing that scores of most significant risks are being maintained on a regular basis, this is devolved to risk co-ordinators. But it's not our responsibility to determine if scoring is appropriate or not, although patent over scoring will be addressed.

BM: Do you have defined education and training requirements for risk management?

IA: I'm working on that with the HR people at the moment…building a dialogue with people responsible for training.

BM: What formal or informal education and training packages exist for risk management?

IA: …small training programmes that have primary risk management focus, for example with the implementation of new (censored) system, we had a two day workshop around risk management…but that is exceptional, for the most part risk management is a component within wider training courses…I'm intending to co-ordinate education and training in risk management, trying to build a relationship with HR training staff to get risk to feature on their radar in a coherent manner…where we have advanced is with the champions reviewing the nature of the business stream training programmes, so we're seeing the emergence of risk as a topic in training programmes, whereas two years ago it wouldn't have featured….there's on the job training relating to individual tools, people can read up themselves, exceptionally we may send people on external courses.

BM: Are the information requirements for effective risk management understood and defined?

IA: That's a work in progress, we've had a couple of goes at it, need to revisit it.

BM: What process do you go through, is it about core risks, data you need for analysis, or broader?

IA: It's broader, first to get some understanding of exposure at a numerical level, cumulative risk points in the population of risks identified, but one of the problems faced is the transient nature of exposure.

BM: Are you satisfied with information systems for collection, storage and transfer of risk data…do they satisfy direct operational requirements?

IA: The risk register is the primary, and to large extent sole information system for risk management…risk data is not embedded within broader information systems, with exception of project

management, where risks are reported within an independent system which will can then be fed into risk register.

BM: How do you validate if you're collecting the right data?

IA: Usefulness is a good test, we collect data for senior managers and directors, we get feedback from them as to whether it aids them effectively. Whether the information that's being reported is correct, is something we'd address through audit process, as we get our systems more mature and embedded, the focus moves towards validation...

BM: What is the role of the audit team…in relation to risk management?

IA: A lot of the focus of the service audit team is on strategic risk. Their audit catalyst is driven by the significant risk exposures emerging from the business unit risk assessment process, they're risk oriented in their focus, but only, because of resource constraints, deal with 8-10 projects annually.

BM: What's the brief of service audit?

IA: They'll be reviewing for the most part whether the management strategies that address strategic risks are being implemented, and that other governance issues to do with control of that risk are being implemented, that policies are being applied.

BM: Is information sharing in risk management restricted, restricted within groups or functions?

IA: We're beginning to get that information sharing now, people are identifying risks that exist in other areas, talking cross-boundaries with potential owners.

BM: What process did you go through to institutionalise risk management…?

IA: We've created a corporate framework to support and endorse risk management as a worthwhile process in the business, created the framework within business stream through champions and co-ordinators, figuring of risk management on monthly management meetings to give it visibility and credibility, we've got the hub site with material to provide guidance, we've got the risk and issues database…

BM: Is it policy and procedure driven in practice, or is that overly bureaucratic way of embedding RM?

IA: You need to put that framework in place in part to demonstrate governance, but we're not reliant on beating people over the head with the policy, that's why it's a relatively slow burn approach, the key players through continual reinforcement are the champions and co-ordinators. In truth, we need to give

people more visibility of the subject, more support to allow them to be self-starters, a lot of the material on the hub needs to be developed further, people need to be pointed to it, we then become a resource to support their enquiries.

BM: Is enterprise wide risk management an objective?

IA: It's an objective of mine, two years I would have sold it to directors, now I've adopted an approach of softly softly catchy monkey, where it's a lot of small scale initiatives driven by capability assessment that will eventually lead us to ERM, through growth of risk management through the business – it's not a top down approach any more.

Appendix E

Sample interview transcript from benchmarking survey

Brian MacGillivray (BM) and Interviewee B (IB)

BM: Can you outline the structures and accountabilities for risk management…?

IB: Until recently, 18 months ago, there was a risk management group in division who owned and developed the risk management processes, following the re-organisation, the process development and ownership moved to the head of (censored), this person sits within the utility. Under (censored), you have a business continuity and risk management team – which includes myself, a risk specialist and a risk practitioner – in addition, value and risk management sits within engineering, dealing with project risk registers and modelling for engineering projects…the overall risk management policy is dictated at (censored) headquarters – all about compliance with contract law – from that we develop a set of (censored) risk management arrangements which are owned by (censored), from that 12 utility risk management arrangements…we derive local unit risk management arrangements…Europe, Americas and to lesser extent international, discuss and collaborate on high level risk management arrangements. The (censored) risk management directive from parent company is focussed on corporate governance – though it does say it would expect enhanced levels of risk management to take place throughout the organisation – setting out the bare minimum for risk management, the value added stuff comes in at the European and the business unit level, where we have the distinct risk management processes.

BM: Do you have criteria which defines success in risk management?

IB: We have a double whammy audit process…internal audit come in every year, to check that we're process compliant by drilling down from risk reporting at the highest level, right down through identification, assessment, management, it will also look at the whole range of reporting routine and local risk management practice. Additionally, (censored) come in for our parent company to ensure that we're process compliant…also as a team, we have our own audit function to ensure routine compliance, we do our own local audits to make sure that people are up to speed – for example ensuring we produce reports in on time and to the right format – and we tackle non compliance. We recently had a full audit by a independent company, they've said: you're very good at adhering to processes and you're process compliant, but are you effective at managing risk? They delivered a report with a list of opportunities for improvement, looking at the physical management of risk rather than the reporting mechanisms…we're trying to develop a series of KPIs which will inform senior management on the efficacy of the process, at the moment these are low level indicators, for example action plans developed on time, action plans assigned ownership, red risks assigned contingency plans, more to do with the governance of the processes rather than the efficacy of the solutions.

BM: Is the strategy and its success reviewed on a periodic or event-driven basis by the team and senior management, making changes based on feedback?

IB: We try to take ideas from lower levels to enhance the processes, however we have limited opportunity to influence the directive. The risk register in water and wastewater operations was built using local people, to identify the tool that'd give them the information they need to manage risk in their area, and ultimately support the risk management process…we have a duty to revise the risk management arrangements every 12 months to ensure they still reflect the shape and form of the organisation…additionally, to make sure we're still compliant with corporate policies and procedures…to show they're compliant they do a self-certification exercise.

IB: The Directive suggests they break risk down into one of five categories – structural, operational, taxation, other, etc. – they then sort into sub-categories.

BM: Can you explain how you prioritise risks, for example…risk matrix?

IB: Our measurement of risk is using a set of parameters determined by the directive, likelihood vs. impact...4 by 4 heat map, we have general principle that AB can be managed locally, whereas risks above C+D have breached the tolerance threshold, and need more urgent action and management intervention.

BM: How did you determine this cut-off, was there a methodology or was it arbitrarily assigned?

IB: Truthfully, it's in the directive, we comply with the directive, I'm not sure how much thought has gone into it. We try and relate it to the business plan, C+D risks would make it difficult to deliver and meet business plans…in engineering, cost-benefit parameters are used for acceptable risk, something engineering do within their project risk registers and their modelling, when it comes to representing these risks on the heat map, the standard parameters are applied, but more thinking gone on behind the heat map, so the characterisation of the tolerability of project risk is a truer reflection.

IB: We try to ensure that risks are managed at the lowest possible levels, we try to ensure solutions are generated locally. Where lower management feel they can manage risks outside the tolerance levels, they may do so, but they ensure that these are reported upwards - this facilitates a culture of no surprises…they will still appear on the high level heat map, but will be managed locally.

BM: Across what areas is risk analysis explicitly performed?

IB: All areas, everything from asset based risk, to cyclical risk –seasonal business plan risk, non-asset, geographic specific, plant specific, process specific, HR issues, brand, stakeholder… the directive suggests that our risks are financially based…all risks have a financial cost, but some of our softer impacts are greater than the financial impact.

BM: What methodologies are applied in risk analysis?

IB: We consider the risk in relationship to the range of impacts, for example brand / reputation may have been identified through a local pressure group, isolated risk, we then look at it in terms of the related risks that are out there, e.g. odour, what other odour risks are out there, what groups are affected, what other odour risks are out there, aggregate into generic odour risk, then try and understand impacts on other areas of business, e.g. legal, asset management…we use a lot of peer review to understand how processes and operations interact with each other.

BM: Is there a defined process for risk analysis, in other words…undertaken by procedure, with initiation points?

IB: Couple of ways, the risk management process up to senior management of water / waste or big business units will look at risks in their own area, once it gets to senior management level, we will have a performance and risk meeting with the COO, who will see all heat maps separately, and produce his own heat map, at this point, there's an open discussion about interactions of these risks, across processes, across geographic areas, across customer bases, where are there hotspots, where we've had events….another thing we've done in the past and we're going to bring forward is the PSG – professional support group – other experts – legal, insurance, finance, environmental and quality, health and safety – specialists who will then peer review this range of cross-operational risks.

BM: So there's a common template for risk assessment…expert judgement, peer review…is the method for analysis?

IB: Yes, we say that risk management is the discussion around the risk, and the decisions taken to respond, that's what these groups are here for.

BM: Do you apply other discrete risk analysis methodologies, whether as part of the risk management process or part of business as usual?

IB: The project engineer will wrap up all project delivery risks into one risk, which will then be reported upwards, so he will do all his modelling, using a range of techniques within.

BM: Are there criteria and guidelines for undertaking the risk assessment?

IB: Yes, looking at specific risk tools, yes we do within the engineering format, at higher level, defined within local business units…most are driven within processes, not reactively, although of course we have to respond to events.

BM: Are there any verification mechanisms to ensure risk assessments performed as required, and appropriately?

IB: Only really through audit process.

BM: For risks with cross-functional impacts, do you bring together stakeholder from different units/functions to assess and develop responses?

IB: Yes…high level engagement…PSG…another thing we try to do at lower levels is having developed the operational risk register, we're trying to develop a peer review by tying this into asset plans, so then the asset planning team would have a picture of what's happening in both water and wastewater.

BM: How do you store or document assessment outputs…database?

IB: 75% database recording, the rest documented.

BM: And is risk assessment and decision making part of the same process?

IB: Yes, we try to tie them up as much as is possible, try to make people understand that risk is an integral part of day-to-day activities, and whilst there might be this wonderful framework that they have to feed into, ultimately its about doing their day job and having control of their activities, so process and day to day risk management should be closely linked.

BM: One thing other managers have discussed is that, the existence of a conservative psyche or culture…

IB: We're both risk aware and risk averse, we accept a certain amount of risk because its necessary in undertaking our operations. We aren't too good yet at looking at the opportunity side of risks, we see clearly the negative side rather than the positive side.

BM: And is it common place to attach objectives to risk based decisions?

IB: KPIs are an aspiration. We have performance measures that relate to the governance of risk – how good are people at adding data, using data – but we're not very good at validating that the data is effective, that it has any value. For example one thing we're poor at is tracking the movement of risk, building up a picture of risk, predicting where risks may go in the future based on the past.

BM: When responses are developed, is it common place to attach action plans?

IB: Yes, for strategic risks, action plans will be outlined by senior management level and operationalised locally. At the local level, once risks have been identified, the first thing we do is

reduce risk from gross to net level by putting in place local action plans – where there's an identified need and it can be done for a small cost, we can deliver the action plan immediately, if its something where we need to develop more thought around the solution, a local action plan will dictate a desktop study…within engineering, the action plan is seen as managing the overall project, within operations we see action plans as those things we can do to mitigate the risk as quickly as possible.

BM: Within the action plans, are there criteria by which they can monitor implementation of risk responses?

IB: Yes, depending on route it takes – opex, capex, or investment proposal. The level of formality is dictated by management's attitude.

BM: Do you review and monitor risk responses in light of implementation?

IB: We try and do reviews and learn where we can, but we're a learner in this respect.

BM: Is the process for implementation or risk based decisions defined…with roles and responsibilities, timescales, guidelines?

IB: It should be formal, we have well defined accountabilities and responsibilities, which works very well at higher levels, some fudging of this as we move down levels, but then as we get to bottom – middle management and below – it gets quite formal again. In the middle, a bit less formal, things are less formal.

BM:…would there be a champion established?

IB: We assign a risk owner for each risk, if they're high level risks, we also assign a risk reporter – a key member of that team. At lower levels, the level 1 manager will understand duties, responsibilities, and who they're accountable to….risk champions are assigned for business units, they hold forums where they can learn from each other; water, waste, asset management, asset management, and operations, sit around on an infrequent basis and chat about the future way of managing risk in that company…but what we try and tell people is that everyone is a risk champion, a risk manager.

BM: Is there a defined risk monitoring process where you're acquiring, compiling and reporting data on evolution of risks?

IB: No, not yet…low level risks are revisited on a monthly basis through local WOW meetings up to COO level, they're continually reassessed, their scoring revisited, action plans revisited, their audit is revisited. But we're not very good at doing much more than that at the moment. We've identified the solutions people need at the lower level in order to manage risk, but we haven't identified how to add

value to the risk management process, this is part of the review that went on with independent audit, where they've identified improvement for the future.

BM: And at the higher level?

IB: …revisited through quarterly meetings, there's a 45 minute slot within the (censored) board meeting.

BM: And the idea behind this is to screen for new risks, look at evolution of existing risks, looking at existing action plans?

IB: Yes, that's the idea, how good we are at it remains to be seen.

BM: What's the problem?

IB: We had a divisional risk team, 3 or 4 people, business continuity people, 12 people, now there's no longer a risk team, but a business continuity team with 6 people – one of which is risk specialist – it's a resource issue.

BM: Is the risk reporter / owner required to update database as action plan implemented?

IB: Yes.

BM: This is as a governance issue, verification of implementation?

IB: Yes, also streamlining of database.

IB: Risk management is now one of the cornerstones of our overall strategy for (censored)…we're training 150 team leaders over spring and summer, training another 150 team leader in autumn / winter in risk management as well as other bits and pieces…we're trying to explain where risk management fits in with their functions, how it fits in with their day jobs.

BM: What were the drivers for taking a more formal approach…risk management?

IB: Awareness is key. We have a business plan to meet, regulatory drivers to meet, we have changing strategy as the group develops, its about being a more dynamic company which understands its data, which can use its data, and can look to deliver future solutions.

BM: Influenced by things like…Enron, corporate governance issues…?

IB: We've learnt from these things, Enron, Barings…showed that companies can go under if their controls fail, Railtrack showed that companies could lose their LTO. One wake up call was the idea of corporate manslaughter, made us focus our efforts on certain activities, where we're operating assets with low likelihood of failure but high consequence, for example critical reservoirs….the main driver, however, was RWE and the takeover and contract law.

BM: Practically, how did you institutionalise risk management…we tend to look at it as a case of…

IB: That's accurate, we've always held the introduction to risk management course, which describes the reasons (censored) has the risk management arrangements it has, how these are delivered, as well as looking at some of the tools and techniques we can support – such as cause and effect, event trees, Kepitrago, Whichscower, Monte Carlo, etc. – and then looking at external drivers. We've always delivered that. We've always had holding sessions with key managers who move into new areas and need to understand their responsibilities. We've held workshops with smaller areas of the business where they need help to develop processes…in the last two weeks I've done this with commercial and customer services…now delivering team leader training.

BM: How do you link in risk management with existing processes?

IB: Its about knowing the right pitch to the right people, when it's to senior people, it's about the need for strategic risk management, at the lower level, it's about explaining its not a new cumbersome activity, but a way of helping them do their job and to cover their arse…by giving them the tools they need to show people in the organisation that they have risk, reduces the burden they have on themselves. It's about modifying your pitch to the audiences.

BM: How do you integrate risk management activities so that its supporting the organisation, targeted to its risk profile, rather than say engineering, finance?

IB: One way was the independent audit review, which took an organisational view, asking what is adding value to the risk management process for the whole of (censored), looking at a wish-list of activities, trying to understand which of those are common, developing a process which addresses those common activities, where we can't add value, allow those areas to have specific tools. For example the register for water and waste, which ties into operations, customer service, asset management, but doesn't satisfy everything engineering needs, so we allow engineering to have bolt on tools, such as @Risk...trying to understand what the whole organisation needs, without pandering to everyone's needs to the nth degree.

BM: Is there a process for managing supply chain risk?

IB: That's managed by procurement…my only experience was when we came to doing a re-bid process for contractors, when we looked at business continuity and event management arrangements for individual contractors, to make sure they had BC plans in place and that they were robust...

BM: …and when you're undergoing or planning change…looking at risk implications?

IB: I'm somewhat removed from this, we've got central project teams who look at the company transformation. My experience of those teams, and previous organisational structural changes, we tend to manage risk on a macro level, we try to understand their impact on people and interruptions to processes, but we don't look at the smaller risks involved in that…

BM: Have you defined the E&T requirements for risk management, the required competencies?

IB: Part of the senior leader development programme was the COO looking at succession planning, who are the key people he needs in the organisation, and what are those key skills, risk management was one of six key topics, within risk management, he outlined the major areas of risk management he wanted them educated in – corporate governance, local risk management solutions, (censored) tools and techniques – he wanted people educated on. We implemented these, and added value, for example looking at ways of getting people thinking about risk…the intro to risk management training was identified following discussion with directors about the level of knowledge required by key strategic members of the team, developed by independent consultant who was experienced in undertaking risk management training.

BM: And is that package, or packages, are they initiated as part of the organisation's processes, with initiation criteria, procedures…?

IB: Yes. There's also ad hoc sessions on request, as well as one-to-one hand holding sessions, workshops, etc.

BM: Do you have objectives for the training programmes…so that you can assess whether the competencies are being imparted?

IB: Yes, once each team leader has undergone their range of training, they're assessed on their ability to act on that training, through monthly assessments on which they're scored, and six-monthly meetings with their senior manager which also underpins their succession planning route, to sort out the weak from the chaff.

BM: And are the training programmes reviewed based on feedback?

IB: It's early, but what will happen is that each person that goes through the training will score us on the level of knowledge that they obtain from that session, and we'll analyse that feedback with HR and

senior management, to understand where we may need to adapt the training package to meet future needs.

BM: And have you defined information requirements for risk management?

IB: Not really. One thing that's happened is our team has moved into management systems, which means that we're sitting in an area better connected to the knowledge management community, we'll be sitting down in two months time with our peers to understand how we can use knowledge to underpin processes.

BM: Do you have defined information requirements for discrete areas of risk management, but less defined for process of risk management as a whole?

IB: Yes, one thing we hope to do is create an intranet site, one stop shop for help, to receive feedback on development of the process, and to point people in the right direction on process compliance and about developing local solutions.

BM: Specifically, in the risk assessments, are data sources, information requirements defined, or is it really about expert judgement?

IB: Expert judgement, its about having senior experienced people who can understand where the risk has come from, how its moved, what impacts on it, and how it impacts other areas, it's about expert judgement; without senior experienced people, I'm not sure we have the data to underpin this. Expert judgement offers a huge amount of value, risk management is about the discussion surrounding risk. But one of our conclusions following our hammering from (censored) is that we're not as good at using our data as we should be, area we're seeking improvement, and certainly asset management are keen on this…
one driver for the water and waste risk register was to then start to build on the lack of data in asset management by tying risk to asset plans, we need to build on this, get better quality data.

BM: Are there mechanisms to verify that the organisation is meeting it's information requirements?

IB: Not at present.

BM: At the operational level?

IB: Perhaps, local measures for verification may exist…for example within the sewer flooding database, interruption of supply database, but this is tracked for regulatory drivers, it's not true of whole of risk management.

BM: Is communication / transfer of risk data, restricted by boundaries?

IB: We're very good at discussion across boundaries, the way that people move around is cross-functional, training is cross-functional, etc.

BM: Do you have adequate resources to support information management…?

IB: It's very easy to whinge, but I do feel there's a need to step up, so we can facilitate understanding of how risks are evolving, whether the data is good, whether people are really delivering action plans.

BM: But the IT, the information systems are okay?

IB: Yes, we did an external review, looked at software systems, but felt we could satisfy needs internally.

Appendix F

Sample interview transcript from final case study

(engineering function)

Brian MacGillivray (BM) and Interviewee C (IC)

BM: So there's the project..?

IC: The project…before financial approval has a full risk session carried out, it's done usually by (censored) and his group's involved in that….identifies the large risks not so much the detail, the main sort of risks, and that follows Australia standard process, looking at control measures to be put in place for the high level risks, so that's one form, projects that go through, I should say we don't do the design in house as such, we audit and outsource design on almost all, 90 odd percent, so the designs will be done by consultants on a panel, and those consultants will run a hazop type risk session, depends what sort of magnitude the project is, the big ones always have a hazop session, or multiple hazop sessions, and they're attended by people in here, so that's one part of the process, another part of the process is that when designs are done from outside, they're reviewed by (censored) staff as well, so we have a review process, audit and review process, that's what we do on all of our designs, occasionally we feed comments back.

BM: So QA essentially?

IC: Yes, it's basically we have an informed client role, you know if the organisations didn't have any engineers you'd just take what they through at you, but we've got sort of 20 odd people that have got technical expertise and experience so that's the role we play.

BM: So is the design entirely outsourced, or just the metro?

IC: It's negligible what's done in house, we've got a couple of electrical, a couple of mechanical, etc., we're talking 150 million dollars a year in capital works.

BM: So in terms of, is it outsourced to (censored) or…?

IC: Well there's two parts to it, the metro area is managed by (censored), there's a maintenance and operate contract, but there's a part of that which is….actually to manage the capital works execution, so that the end project, capital works project is inside the (censored) area. (censored) manage the process, includes the design and construction of that, but we'll get involved in a review role again with those, in the country, the rest of its country and dams, and that's the part that (censored) has outsourced the design, we've got a panel of consultants, four or five companies on it that we use.

BM: Talking to the guys it seems like there's the hazop that you mentioned, then there's the more formal probabilistic risk analysis in dam safety and also the generic process, but on top of that, I mean the stuff you do in house, but I suppose more relevantly the stuff that's outsourced, do you know what kind of a role risk and reliability analysis plays in design, I'm thinking about the actual tools or

techniques for identifying hazards, things like the what if analysis, failure mode and effects analysis, reliability block diagrams, I get the impression…

IC: Not, we haven't got formal systems for that, we've got a number of technical guidelines, technical standards which sort of incorporate a lot of those things, so we've got technical guidelines for example which are intended for designers, these will say this is the way we want things done, we'll follow those, we've got technical standards for construction, they'll lay out how things are to be constructed, the other part, the hazop, is more for the specific project looking in detail, you know what ifs.

BM: As I see it you're essentially managing risk through adhering to conservative codes and standards.

IC: They're not conservative, why do you think they're conservative?

BM: I thought that was the water industry practice, or at least historically it's been?

IC: Like I said, we're not, I'm just trying to think why you think they're conservative, the technical standards are just saying this is our standard approach to design, just talking about switchboards, things like that, that's not conservative that's just how we do it, in the technical standards, what they are is they refer back to Australian standards, but Australian standards always have a lot of things, additional information required, so it can be just a standard on something but you'll find there's a schedule at the back of all the other information you need, so a lot of the standards are actually providing additional information but basically following Australian standards, so that's not saying it's tighter than Australian standards, but their standards provide a lot of additional information in many cases, but the other aspect to that is you can say something like concrete for example, we required long life times out of our concrete to build the structures that will last 100 years for example, the Australian standard may or may not be suitable for that, but it's just a question of the value of better specifying something of a higher quality to give that extra life, because the assets are worth a huge amount of money, it's not to be conservative it's looking at the value of it and coming up with something appropriate.

BM: The reason I asked is at least in the UK there's been a historic approach of looking to engineer out risk through using conservative codes and standards with a high margin of safety and since privatisation the idea is to use the most cost effective approach and they're trying to move through reliability analysis to move towards a more cost benefit approach.

IC: Well, I say we use the Australian standards, we're not using, well there are water codes as well there's WASA who have other codes on specifically water things, so we tend to follow those too, but they're Australian water industry sort of code.

BM: Are there any kind of specifications for reliability, I'm thinking maybe in process, which I suppose is outside of engineering, or in dam safety, or I guess there's the ALARP criteria, or in network reliability, the number of interruptions which is acceptable, or is it not?

IC: Our area is more the mech elec, civil, the nuts and bolts rather than the system if you like, the system, I'm wondering who would, that comes back to the concepts at that stage as to how you put the system together.

BM: What about at the component level, would you have specifications for the technical reliability of components, I'm thinking oil and gas, nuclear, there's regulatory pressures to use these, but in the water industry it doesn't…

IC: No, not really, I mean you…the water industry is fairly straightforward in terms of its plant I guess, you take a pipeline, you've got some big pumps in there, a few valves and things, but take a pipeline, there's not a lot of things that go wrong, I mean you can use a pump and we tend to have a specified level of standby, because when you've got to service and maintenance, so you want to have one standby piece of equipment, so there's no specific things for reliability, I mean we base it on past experience with particular manufacturers I guess, and how you prove it's going to last 10 years, instead of 15 or 20, how you do that, it's a bit difficult.

BM: Yeah, I mean there's no failure database for the water industry which there are in other sectors.

IC: But it's not, if you took something like the electricity industry you get an instant effect bang people have lost power straight away, the water industry isn't like that, you've got time, you've got tanks that are full of water etc, I guess the wastewater side is a bit more of a problem, in that you can't stop the sewage coming in so you've got less time to react, but it's not millisecond sort of effects on the customer, so from that point of view the approach is slightly different.

BM: I guess in (censored) there's potential problems with the supply demand balance, so how do you kind of, if you like incorporate this balance into the design of the networks, is it a case that the networks have been there for so many decades and reliability analysis of the network doesn't inform design?

IC: The network is not really our area, that's our systems people in (censored)…that's really the large part of the network, we don't get involved in that.

BM: So they're essentially responsible for the bigger picture if you like?

IC: Yeah, the long term planning plus the big picture of the network, we get down to the level of, on the wastewater side for example when we're going to do a subdivision or something, and they'd be

involved if we're going to hook into a sewer here what's going to be the effect on the network, so a different area looking at network issues and long term planning.

BM: So the methodologies you use for risk analysis, the hazop, the dam safety, are these initiated within a defined process, in terms of there's criteria for when they're applied, there's procedures for their application?

IC: We've got a procedure on hazops, which is an internal document.

BM: Are there specific criteria for initiating when it's performed?

IC: Yeah, I think it's a percentage of the design, 40 or 60% or something.

BM: And these techniques, the dam safety, the hazop, do they have predefined data requirements that go into them, or is it a case of subjective judgement or engineering judgement?

IC: I think it's more a case by case basis, because every job's different, we don't do repetitive projects, they're different to some extent.

BM: So on a project by project basis would you apply these methodologies with predefined data that you would collect and use at the assessment point, or is it a case that you'd arrive at the assessment and if more data is required…?

IC: I think you'd start looking at it and see what you need.

BM: Are there, in your experience, do they, risk assessments, tend to be underpinned by an analytical process, in other words there's data there's information that underpins, or is it a case of get the experts in the room and get the best judgement?

IC: Yeah I reckon it's more a case of experts in the room, when you design new plant there's probably….well you can data from other plant I suppose, it's a bit consistent with our audit role where a lot of people have a lot of experience you can soon see where the holes are I guess.

BM: And is, what kind of people do you get involved in these assessments, is it purely engineers, or is it health and safety, ops, hazops?

IC: It tends to be a range of people, you've got operations people, you've got design people, you want to represent the asset owner cause they've got to spend the money, health and safety might get involved depends what it is you're looking at.

BM: So is this to improve the assessment, and also these are stakeholders in decision making?

IC: They're stakeholders I guess, it might be right, rather than do something, do something in different ways I guess.

BM: So it might be a maintenance solution.

IC: Yeah, I guess.

BM: So you mention you're QA role, does the audit role apply to the risk assessments, the hazops, the dam safety stuff.

IC: Say that again?

BM: Are you performing QA of the hazop, the dam safety, the risk assessments?

IC: We're looking at all aspects I guess…we are involved in any hazops that are run, but it's a total review of what the designs are.

BM: Is there a review of the hazop itself, some kind of peer review or technical review of the process?

IC: No, I wouldn't think so, often they have independent facilitators that come along, I've been to a couple at it, (censored) have one for example, one of our consultants, they get someone along from the petrochemical industry as a facilitator to run the process, it depends on how good the facilitator is how good the thing runs.

BM: And in terms of verification that it's done, are there mechanisms to ensure that these have taken place, to track that these have taken place, the assessments, that a hazop hasn't been missed out, couldn't have gone under the radar?

IC: I don't know if there's a QA for that.

BM: Not necessarily QA, but maybe just a checklist, to tick the box, we've done the hazop.

IC: There is a project checklist, I'm not sure what's on there, that's what the project managers do, have you spoken to somebody in the project area?

BM: I've spoken to some people in projects, I guess we'd looked at hazops at being in the engineering stage…

IC: The project managers still manage the detail design as part of the span of what they're doing I guess.

BM: I guess this is representative of the industry, there's not a lot of risk or reliability assessment, what's the rationale of this?

IC: What was the question?

BM: Risk or reliability analysis in design, engineering design, the sector and (censored) it's a fairly limited scope, not a lot of techniques applied, is that because of the cost, the expertise, or it's just not necessary for the industry?

IC: Not doing reliability?

BM: Reliability, or more detailed risk assessments.

IC: A lot of these stages are pretty simple that you're talking about, pumping, a small pumping station, when you get to the treatment plant you jump a scale, dealing dosing chemicals etc. which are getting close to customers etc., that's different, that's what the hazop's trying to identify, the dosing pump goes and starts injecting, what happens if your power goes, all those sort of what ifs come in there, but I think a lot of the other infrastructure is fairly straightforward and you've got this time delay between the effect as well so it's different from nuclear and electricity and other industries.

BM: So you've got, the system is well characterised, so you can manage the risk with standards and guidelines?

IC: Yeah, the guidelines are our philosophy of what we do, technical standards are construction standards, you know if you're building a pumping station you would just follow the guidelines and spit another one out sort of thing, they're all different to some extent, but they're basically the same in many ways.

BM: So if you look at the standards as essentially your threshold for an acceptable level of risk, so how are these arrived at?

IC: Standards…standards sort of evolved over the years of experience, these are construction standards, these go in tender documents where people bid on construction jobs, so we're talking about the quality of construction, what components go in there, so they're based on Australian standards but they might be modified to provide extra information or we need more stringent outcome.

BM: What about design standards?

IC: That's the technical guidelines, they've evolved through a history of doing designs in the water industry I guess, and we've tried to capture the knowledge of our senior staff and get things down on paper, they cover things like hierarchical control systems, they cover layouts of pumping stations these are the way we lay them out, you know, there's a whole raft of things, it's just to try and make sure the consultant gets something close to what we're looking for.

BM: I was talking to (censored) yesterday about how these evolve, what the process for adapting, he was saying it's not a particularly formal process, it's in his job description, but one of the things he's come across is that they're documented but the rationale isn't…

IC: That's possible, I've got on front of me here a position, seeking a position for technical officer standards, this is a position to focus on standards and to actually drive that process, so we're actually putting in some resources to actually get someone to really focus on our standards and guidelines for the future, so that's a bit off the track but it's actually…we've been through a bit of a restructure, you're probably aware of that, one of the problems is that in the past we've always had a large body of knowledge in larger sections, that's being wound down over 10 years or so, and we're trying to recall all the stuff before the people sort of finally leave, so we haven't lost all the knowledge….and also the reasoning behind why you might do it some way, you can write down what you do, but you're right if you don't know why you did it, or if something is proven not to be good that you don't do it again in 20 or 30 years time, so it's important to have that background.

BM: In terms of the decision making process, again we're going back to the hazops and the dam safety analysis, what is the process for translating these risk assessment outputs into risk reduction strategies, in other words, what I'm trying to find out is there a logical connection between what the risk assessment output is and the decision to deal with it?

IC: I don't think there's a formal process, I think what you're saying is you identify things in the risk analysis you might feed that back into technical guidelines or standards at the end of the day which probably hasn't happened to a great extent, apart from people knowing about it and when they come to update the standards it'll happen in that process, these standards, I don't know if you've seen them or not…they're updated every 12 months, so you get a chance for all our people to sit round a table and go through them and update them, there's probably not a formal register if you like of things that eventuated here coming around and feeding back…

BM: …There's a closed loop between…for a particular project you'll do the project, you'll do the hazop, you'll identify the solution, but there's maybe not a link between that and the technical standards to feed back the information.

IC: There may or may not be, it depends what the result was, it may be the design not doing something properly, or is actually a genuine thing that should be caught up in the standards or guidelines, I don't think it exists in a formal way or not, but with the extra resources here (officer), it gives us a chance to catch up.

BM: So how do you actually identify and evaluate the options to reduce risks, in hazops, (censored) was saying sometimes you come in with predefined generic options and these are evaluated on a project by project basis, what I'm trying to find out is how you balance different options, how do you balance not just the risk reduction, but the cost, ease of consideration, what's the criteria behind it, or is it again a judgement call?

IC: I think so, I mean you need some knowledge of the cost obviously, you're constrained by the costs all the time, but I think it'd be on a people recognising there's some issues there, come out with a satisfactory solution, it doesn't have to be engineering, it could be operating or engineering solution, depends what it is.

BM: So the decisions taken are within the risk assessment?

IC: They'll be within the hazop workshop itself, there's a whole lot of actions coming out from it, and people go away and consult and sort of come up with those solutions.

BM: So you've got your ops, your maintenance?

IC: Yeah.

BM: And is there any kind of peer review of the decisions taken, of the strategies developed, is this part of the facilitators role?

IC: Something that comes out of the hazop?

BM: Yep, a decision to change the design, or to maintenance or operations, how you've responded to the hazop, is there any kind of peer review?

IC: I don't think, the facilitator is usually there just for the session, so they probably wouldn't have a follow up, but the project manager who's responsible for the design, but the project manager would follow that up, make sure those things are done.

BM: When you've taken a decision, what do the objectives look like, how are these tracked, you've not got specific reliability specifications, I guess it depends on the nature of the solution, but can you really determine whether this is reducing risk, or is it a case of you would have cost and component

objectives, specific things you want this decision to do, but not necessarily what you want to achieve in terms of risk….i haven't worded that terribly well….I guess can you validate that a decision, once implemented has reduced risk, or can you just validate that it's been implemented?

IC: I guess it's people's opinion that it reduces risk, because an event doesn't happen doesn't necessarily mean you've changed anything, I guess it's probably subjective I suppose in that sense, people have recognised that in general there's an agreement, you've taken some action, it should be reduced, but I don't know if you can measure these things because the events are not very likely to happen anyway.

BM: And is there a process, maybe this comes into project management, for auditing the success of these changes to design, operation, maintenance or so on, does that come in project management or is?

IC: So you're saying later on when it's built, the feedback?

BM: Essentially the lessons learnt.

IC: The lessons learnt in projects are recorded by a project group…they're establishing a database of lessons learnt…so you do get this, at the moment there's reports are done, but they're sort of not integrated back and easily accessible, so they're putting that back into a database and you can back into that database and pull things out.

BM: In terms of actually implementing these solutions, again if it's engineering solutions it just comes into PM which I'm fairly familiar with, but what if it's an operation or maintenance solution, what's the process for implementing it?

IC: I guess it'd be whoever is doing the design, that'd come into the specifications in the maintenance or operations manual.

BM: Are engineers responsible for the operating guidelines and so forth?

IC: No, we aren't, but I mean the designer, we're not the designer, would, the design, what would normally happen is there would be a requirement in the specifications of the construction contract to provide operating and maintenance manuals, so they'll be, so it's the constructor who has to, they do the final shop type designs, you know you haven't built in the detail yet how to operate it sort of thing.

BM: And in terms of monitoring, I suppose if there's not reliability data that's captured, but is there any other way that you assure risk or reliability in your engineered designs once they're built, operational monitoring or inspections, I guess that's in dam safety or so forth?

IC: Dams are covered, there's a lot of monitoring in dams, instrumentation and lots of physical monitoring of sites, surveys and all sorts of things, that's well covered from the safety point of view.

BM: Beyond dams?

IC: Just the ordinary plant?

BM: Yep.

IC: We get feedback from operations if things were wrong I guess.

BM: There are kind of failure and incident analysis, I guess you've got the root cause analysis, is this fed back into engineering?

IC: This is from when you start operating the plant?

BM: Yes.

IC: Things go wrong….right….not formally I don't think, that's an area that could be improved I guess.

BM: And the monitoring that you do have, for dam safety, it's defined in terms of by procedure, criteria, roles and responsibility and so on?

IC: Andy knows all about the monitoring.

BM: Just finish off having a look at education and training, I guess internally, is there any education and training, formal or informal, in engineering, not just risk management, just generally?

IC: Well, we have internal courses so people go to OH&S, sign offs required for those sorts of things, there's not so much technical in house training, things you get at seminars, workshops those sorts of things more external, so there's training there.

BM: What about for the hazops, for the dam safety stuff, is it a case of it's facilitated by the consultants so you wouldn't have internal training, or is there any kind of workshops you send people off on?

IC: Well kerry went to a workhop in (censored), 2 or 3 day, like a facilitators course, how do run hazops, we have people keeping up to speed on what they're about.

BM: More generally, is it a reliance on professional experience and expertise?

IC: It’s more experience and on the job learning than professional qualifications.

Appendix G

Sample interview transcript from final case study (project management function)

Brian MacGillivray (BM) and Interviewee D (ID)

BM: What does RA address in project management, are you looking purely at the risks that the results of the project will deviate from what your objectives were, or is the risks of doing the project vs not doing, also the relative risk of projects in optioneering, what's the scope?

ID: I think the scope varies depending on where the project is, in the initial stage when the clients come to us, they look at just is it going to be a goer at all, is the project going to go or not go, so it's like a go or no go gate, that risk of…will this be a project itself is an important risk to address in the beginning because you won't spend money, because some of the big, big projects have got spends of several million dollars before it reaches concept development stage, that's one area.

BM: …There's kind of a tiering if you like, there's the risk assessment the no go versus the go, then there's the risk analysis looking at the optioneering stage from project across project, then once it's got financial approval it's kind of the risks of delivering the project or the risks to project delivery, is that fair to say?

ID: Yes.

BM: What I'm not clear about is what form the RA takes when it's looking at is this project a goer or not, what's the form?

ID: Well what we do is we get all of the stakeholders that we know at all a proposal development stage together in a room and say look what we want you to do is tell us anything you think, it's no silly question, that might be a potential risk to us, A) delivering what we said we're going to do, B) doing the job itself, then get the people to identify those risks, put it into a standard 4360 risk matrix, and then look at the probability of occurrence and the impact and then classify them into low, medium or high risk, and then start to put together some kind of a risk analysis of where these risks might lie, how they might occur and some kind of a plan to put together to say look that risk happens, that is how we're going to mitigate or the strategies to mitigate those risks, okay, I'm just looking for some documents here that might give you a typical idea of what we do, this is the new project that we're doing recently called (censored), what kind of risks we have, I mean a risk could be a risk of doing nothing, that is don't do this project, what is the risk, that itself in a way helps to justify the project itself, so for us, and then we do the description of consequences, mitigation measure and any comments that go with it, and each risk has a unique identifier, and I would say the risk register really needs to be kept, from a company point of view, very much up to date, and so there's got to be an implementation plan, how we're tracking this, some of them drop off half way, three quarter way, and some new risks emerge as we go along so it's more an upgrade thing.

BM: So is the risk analysis process is it defined, so is it undertaken by procedure, there's a systematic set of tasks that you undertake, or is it more informal than that?

ID: No, no, we have a project it's called a project planning procedure, so we have project start up to say the first the thing we do is like establish the project steering committee, for the manger to get a brief, get financial approval, sign off, and establish project documentation – what have we got to do, how much have we got to do, where are we going to do it, okay, and then we, in the team, and as part of the project management process we've got a key, concept development stage we have a risk assessment and that is like a corporate procedure and each item, line item of our procedure, is a line item in the programme itself, so a project manager has got to tick and say I've done this activity in the beginning, and I've actually done that, so very much an idiots guide to it, this you know also mitigates our risk because you know we're identifying what we're doing at different stages of the project, prepare estimate, do value engineering, so very much a structured methodology that we follow which minimises our risk of missing out things.

BM: So the concept stage is that the initiation for the risk analysis process?

ID: Yes.

BM: Does it ever occur back in optioneering?

ID: Yes it does occur, this is optioneering stage for Torrance aqueduct, we've not even developed the concept, we're doing risk analysis at the optioneering stage itself.

BM: I pulled this off online, here's the formal initiation criteria for risk analysis, whether it occurs back in planning is this down to individual initiative of project manager, or are there kind of procedures that are hidden within this for the risk analysis back at the optioneering stage?

ID: Ah no, no it depends on the size of the project, projects that go above 3.6 million (censored) which go to cabinet and public works it's mandatory because theirs is a public works and cabinet works that says you should follow this format and these are topics to address, and it says have you carried out formal risk assessment, what are the high and medium risks, so you have to address that you have to carry that out at optioneering stage, likewise when things go over to the finance committee they have a format which similarly addresses risk, it's not dependant on the PM, it's largely driven by the approval authority limits, financial limits dictate it.

BM: And also at the concept stage, there's a financial threshold, is it 200,000 whether you undertake it or not?

ID: Yes.

BM: If it's below 200,000 is there nothing formal done in terms of risk analysis?

ID: I would say that if it's below 200,000 dollars a lot depends on the project manager as well as on, this is at the optioneering stage okay, not after optioneering, so a lot depends on the asset owner as well as the PM, as saying well look it's only 25,000 dollars we don't have that kind of money, we know what to do, we know that this pump needs to be replaced, we know it's bad, we don't want to go around and fart around, we just want to go out and replace this pump, so the project manager then does the start up, he does the planning, at the planning stage he mandatorily has to do the risk analysis, what are the risks during execution not the options anymore because the options are selected by the client.

BM: So at the planning stage it's mandatory regardless of the financial value of the project?

ID: Absolutely.

BM: And the methodology you use, you talked about it, it's the risk ranking technique based on 4360, is this exactly the same as they use at the corporate level for business and strategic planning or is it adapted for PM?

ID: No, 4360 (censored) standard process, standard risk categories.

BM: The actually identification of risks, and I guess looking specifically at the planning stage, do you use kind of generic risk categories to ensure that you're capturing all potential risk, is this within the 4360, you've got the different categories, or is there some other process for capturing what's happened in past projects to say well these are the types of risk we can expect from similar projects so let's make sure we've identified them and assessed them or is it more brainstorming?

ID: What they do, the (censored) corporates already have a standard methodology and standard topics to trigger the questions, they say how about environment risks, how about government risks, how about process risks, how about OH&S type issues, access, you know, whether, okay, they'll trigger us but having said us most of these project managers have gone through, 14 of our project managers are now registered PMs, they have been assessed against national competency standards for PM, which is very detailed, sort of regard to 4360, so RPM would actually be part of what is called continuous improvement or learning, and they'll never start off with a clean sheet of paper it's silly to do so, I would say they'll say well last 3 jobs I've done similar, these are new risks that arose, or lets tackle them, let's address them, let's bring it to the surface and face it now.

BM: And in the actual assessment of the risks you've identified, so in other words evaluating the probabilities and consequences, is this underpinning by any data analysis or information analysis, or is it purely expert judgement?

ID: It can vary, it can vary, I would say that in the meeting I would say very much, many of the items that are easy are addressed by judgement of people, but then often they might go back and say look this risk we don't know, you go back and do some extra, detailed analysis or quantification using a third party, or give me statistical data of what happened in the past?

BM: Can you give me an example?

ID: Yes, there was a risk identified of rock during excavation, and how much do you provision for rock, do you provision 10% for rock, or 20% for rock, you could provision 100% for rock and the price goes up through the roof and the project becomes unviable, so the risk identified in ayre potential I said go and do some borelogs along the pipeline, or where the pipe might go nearabouts and just go and do bores, so we sent somebody out there and spent 3000 dollars got some bore samples, we sort of find no rock, so we said 10% allowance means we cover ourself fairly good, that was like a positive closure of that particular matter.

BM: And in assessment…you've got here one of the questions I was going to ask is are you looking at root causes I suppose the implication is that you are, one of the things is that a lot of companies aren't really getting to root causes and end up treating symptoms, but I guess you're trying to do that here (referring to document)?

ID: Yes, I mean this is like, this is a project that's not even gone through optioneering yet, there are five options on the table and I can sort of give you this to give you a feel for what's being done.

BM: And talking to other people, there's kind of a range of stakeholders that get involved in the assessment process, and I guess this varies from project to project, but what kind of people get involved, you would have maybe environmental, operations, water quality people? In other words, it's not just the PM and the risk management team doing it, there's stakeholder representation?

ID: Yes, in the main I've encouraged people to think who is your internal client, because he or she must attend, or asset owner you might call them, often these have a programme manager who is like a gatekeeper, or police in charge of the project, because we report to the programme manager, the asset owner would be providing the funds but the programme manager looks after programmes over five years, so he'd be involved or she'd be involved, you'd have one or two people from the regions depending on if it crosses boundaries or is it specific to one region, pipelines do cross boundaries so maybe two regions involved, there may be someone from environmental if there is a large construction that would be involved in a new site or outside of what we normally operate in okay, so they're sort of involved, sometimes you get some representative from safety if there's a lot of work along main road shoulders, road closures might be involved, so we have an OH&S representative in there, but the project manager and engineering leader.

BM: And does the assessment process, is it kind of reside within the individual projects or is it driven by the risk management team, in other words, I know they're involved in the assessment process but are they facilitating or are they effectively doing it for you?

ID: They are only facilitating, they do not drive any outcomes there, they are more like a software driver, saying well I don't know anything about this job and I'm not going to drive any particular risk outcome, but if they think that something is getting, I don't know if we get up on the wrong side of the bed and say everything is high, high and extreme, they'll come and say get real here, you do realise what you're putting in here doesn't seem to make sense, this is not consistent with what we've done before, so they might drive certain behaviours or suggest that look, consider it at the end…

BM: Almost like quality assurance?

ID: Yeah, to say look you're totally out of whack, you've got 14 risks of which 12 are extreme, this looks stupid.

BM: What about, I guess it's the same thing verification that you've done the risk analysis in accordance with procedure, again that's the presence of the risk management team, ensuring that I guess, and on the intranet there's a checklist that you've done the risk analysis …so there is verification that it's done?

ID: Yep.

BM: I don't know how long you've been involved in this, but I'm trying understand how the risk assessment process evolves over time, whether you're capturing feedback and using this to improve the process or whether it's stationary.

ID: The good project managers, and we have quite a few, I would say 15 or 16 RPMs, will always embrace the learnings of the last two or three and they will go and talk to project managers you know if they've done a wastewater treatment or re-use plant they will go and bounce ideas, and say tell me what new risks came that you never envisioned up front, and I encourage that and say look if you've got a new job that you've never done before, and I don't want to give the same type of job to one person, if somebody does a very good job you don't give all the good jobs to one person and then nobody else develops in the team, so I'm sharing the load around by saying look go and bounce ideas, suck the brains of good people up front, very very early in the job, and embrace those and say how are you going to address because you sure get two, three risks that you never totally envisaged that can hit you half way through the job, three quarters. And you've gotta then come up with strategies to resolve them.

BM: And in terms of criteria for evaluating whether a risk is acceptable, is it just a case of it's high, very high or extreme it's unacceptable by default and we've got to get strategies in place to mitigate these, or is there kind of more subtlety behind it?

ID: Well I think it's a lot of people together in the room make that call, and with the best judgement and knowledge and probably the reaction or over-reaction of incidents that occurred in near memory, I wouldn't say there is a lot of scientific data all the time, but often there is okay, you've got to give them that, most of them are engineers they like hard facts, so they will rely on some data on what happened, but they're also less emotional, so unlikely to be influenced by something that happened two weeks back because it was something out of the ordinary, so I would say more scientific, but human beings you know?

BM: So essentially it's professional judgement whether a risk is acceptable or not?

ID: Yes.

BM: I pulled this off the intranet, I guess this kicks in, selection criteria, so that would be optioneering maybe, where it's got different criteria for evaluating, essentially ranking a project, project value, project risk and so on, is this what's used at the optioneering stage to kind of balance projects against each other taking risk into account? Or is this something that's out of date by now?

ID: It might be out of date, because some of the project numbers have changed, the values have changed…this is just in the last couple of weeks they're changing these numbers okay, they've got a new criteria called 0 to 100,000, but they're at 200,000 dollars, all projects are minor projects now, and projects from 100,000 to 1,000000 dollars, so the category off 200,000 has disappeared, is not considered to be minor project if it has low complexity and low risk, so they've put, and then they've got anything from 100,000 to 1 million with medium complexity and medium risk is considered to be a medium project, and anything above 1 million is considered to be a huge project, so they've got some silly nomenclature coming up from the 2010 team, so what I'm saying is that's evolving, so what we're talking about here is going to change.

BM: But in principle this is used at the optioneering stage to value different projects, so I guess the weightings and so forth are just a judgement call, and maybe not…?

ID: Well (censored) when he put this up as a contracts and project manager he sat down with the QA manager…they came up with these and said look it's not perfect but it'll be a good idea to flag a better sort of rigour into doing things if we can put some idea behind these.

BM: If we go onto the decision making process, in other words turning the assessments into mitigation strategies, what's the process for doing that, is it a case of, does it happen at the same RA workshop

with all the stakeholders involved, or does the PM kind of go away on his own and think about how can we mitigate these, how are these RA translated…?

ID: Combination of both, in some risk sessions that are simple they actually generate some of the mitigation strategies, and some sessions, some of the items may not be 100% resolved there, so they put an action on the PM and say look you go back and come up with a mitigation strategy and then we'll update the risk, so the PM then has to go back, make phone calls, talk to people, talk to operations, regions, I mean for example (censored) very recently they identified, we had two years to look at it but nobody came back and said putting a pipe in the road shoulder is a problem, everybody was happy that's how (censored) work all the time on the road shoulder, but recently there was a big hole in some road where some semi trailer went into the hole because of pipe burst, suddenly that's become the biggest thing since sliced bread, now they're saying we don't want to see any pipes in the road shoulders, so you can't comprehend, a lot depends on people, and now they're saying woah that pressure 350 bar we've never had that pressure on a road shoulder…if that happens…you've got a semi trailer overturning on the road to (censored), 200 people could die and they scare the shit out of you, and you've got to go back and say why would a carbon ductile iron pipe, fully hydro tested at one and a half times the pressure, why would it fail, now what failed last time, so we've gone back and challenged them and said oh plastic failed, but metal doesn't fail as easily as plastic, so we've got to go back and challenge them not just take it blindly because somebody had experience, so (censored) can be overreacting too, and suddenly what happens is that the pipe's alignment is being changed from road shoulder down to the paddock now we've haven't got that land…and next thing it becomes the biggest area problem on the job because we haven't got a programme in place okay, so I think the regions need to understand that what happened yesterday doesn't dictate the job, but it's got to be a long term assessment of the issue.

BM: I guess what I was going to ask next was whether you're kind of feeding back experience on how risks are realised, but it's almost as though you're doing that much is what you're saying, there's too much emphasis on events that have occurred predominate in people's minds?

ID: It happens, my role as head of engineering or projects now, projects, is to make sure that we do not allow scope creep, I mean I have a simple rule called CWS, C means contractually unacceptable to the client, W means it's not going to work, S is a safety issue, and if somebody can sit down and tell me, demonstrate to me without doubt in my mind that the safety of a human being is compromised or it's not going to work or contractually…I will not let that change happen, full stop, now demonstrate to me without any doubt in mind that that pipe is going to burst, it's not going to burst just like that, and you've got to have some risk, there is no zero risk anywhere.

BM: So do you then serve as almost quality assurance then of mitigation strategies or is this within particularly critical projects or is this across the board?

ID: Whenever there is a significant change, or a change that might have an impact on a project outcome either in terms of budget, programme, cost, or just ability to meet the technical performance or safety, I think there's a flag that gets raised okay, the PMs have direct access to me and say look my project might hit the red because A) a risk is…been raised to my attention or people are unwilling to accept the mitigation strategies that's been put in place, so I'm happy to get involved in those areas bring in a senior management, bring some experience, bring a peer review process in there, get an external consultant get involved in peer review, and then part of the process might be now we've had no examples of that happening and then that case suddenly….

BM: And so you've got a mitigation strategy to deal with a particular risk, are there objectives attached in relation to this, I mean I guess it depends on the nature of the solution whether capital, operational or what not, but would there be in principle timescales, responsibilities, deliverables, or if it's a change back into the concept stage then again it's obviously an adaptation there…you know is there a formalised process for that?

ID: There is a process to allow a process to allow change to milestones okay, largely milestones, budgets, programmes, okay, and that project reduced after we insisted on that process because the client should give us milestones to achieve a cash flow, spend a budget and deliver a finished outcome, and then they've changed their mind about I really could do with two pumps, I really could do with delaying it by three months, and I've said fine, well if you want to change your mind, sign this document and say I've changed my mind, and suddenly what they do is go back and huddle up and say nah, we don't want to change our minds, we want you to deliver what we said, because ultimately it's going back and putting their name and signing off and saying I've changed my mind, and taking responsibility for it actually forces people to think well let's finish this one, next one we'll change our minds okay.

BM: So would that be, would the bulk of mitigation strategies lead to a change in a milestone or deliverable?

ID: Yes, and I think it should flag, you know there is a system called capital reporting here, very good system, now whenever a project manager changes a milestone or a cash flow or a spend or a possible budget, or an approval amount in the…I've sort of said look if the variation is more than plus or minus 5% of what he said last time, because we've said expenditure to within plus or minus 5% is okay, we have, when I say expenditure but not exceeding approval alright, even if there's exceedence of one dollar to approval likely it's got to flag something and that should be surfaced, that project must be reviewed at senior management one level above, maybe two levels above depending on the severity of that exceedence or change, let's say somebody is going to finish it in October and the client really wants in October, cause we're lucky in (censored) in that we've got projects that are either time or cost critical, time critical projects means the client says I want you to finish it on this date irrespective of what it costs, that's a time critical project, because I have 400,000 customers at the bottom of this

pipeline I want to be able to supply them, because the cost of not supplying them is far greater, the revenue, than the value of the project, okay, so you can spend a bit more but I want it then, but then the majority of the projects I would say, 50-60% of our projects are cost critical, not time critical, saying over the next 12 months you can deliver any time, as long as you don't exceed the bottom line dollar, I want it at the lowest cost, you work with me and I can give you a window of 3 months any time to do this job because I have low flow, low consumptions and I have a bypass line so I won't disrupt my customers, okay, and our project managers really have to capitalise on the projects that are cost critical and say yeah, we don't need to work overtime, we don't need to work on a Sunday, we can plan this better, so they must be getting, negotiating a flexible milestone rather than lock themselves into a deadline that is impossible to meet.

BM: So if the majority of the mitigation strategies that lead to changes in cost, or timescales and so on, these are inherently tracked because they're deliverable of the project.

ID: Yep.

BM: But does that let you validate the decisions, validate the mitigation strategies, you know were these successful in managing the risk if you like, or is it just, you know you're tracking the fundamental drivers or project success which is money and time, are you really getting down to whether these are successful mitigation strategies?

ID: Successful risk mitigation strategies...if you look at project management, PM is about managing the programme, the risk, the quality, the scope itself, so it's programme, cost, quality, communication, risk management, human resource management, industrial relations management, safety management, procurement management, these are the eight or nine elements of project management, and risk management is a very important element, now I know that programme, scope, quality and risk, the four are interchangeable, it means if any one changes, the rest of them have to change, whether you like it or not, so if the risk suddenly changes you will impact the programme, cost and quality, all three, quality to the customer would be I want a higher pressure at the end but you won't get the pressure because the programme and cost have changed so they might not have the right pump to supply, okay, so I think the four are interchangeable and the customer cannot suddenly impose another risk or external risk profile changes that doesn't affect all three, it has to effect it, so you know ,the success of the risk ultimately is that you will deliver the remaining three out of the four, whereas if you haven't addressed this you would not do it.

BM: Into the actual implementation of these risk mitigation strategies, again what is the process for implementing them?

ID: The process of implementation is the review period, what I'm saying is that there is a peer review process, we have a peer review and project reviews, these are carried out by people who are not directly

involved in the job, we have a very detailed format to the review, and that one of the questions will be risk, show me the risk, show me the evidence of having done this, especially the risks that are extreme or high, sort of residual risks there, we would want to be demonstrate, the PM has to demonstrate that he has taken an action, I mean for example if somebody says that the risk of this particular process not working is great, then we want to show the project manager, the project manager to show that he has investigated an alternative process, he has gone and done some design for that process, he has gone and got some prices for add on work, you may not implement it but at least if that happens then you're not waiting six months then you're waiting a month to do it okay, because you've already done the remaining work behind it.

BM: And I guess, this is kind of implementing it within, I suppose a project concept or the project design, then actually implementing the project I guess that comes down to, depending on the nature of it, it might be engineering, it might be operations, it might be a contract, so this just becomes an element of implementing the project itself rather than something specific to risk mitigation itself?

ID: Risk mitigation is about, some people can buy the risk, and you can continuously see that happening, people can buy the risk, now if the risk is of the delivery getting delayed, we've had to do that, the risk of a ship sinking in the ocean with two of your pumps that you need, and we bought the risk by saying we do not want the pumps, both the pumps to come in the same ship, and we said what's the cost of doing it, well 20,000 dollars to buy the risk, I want to have two separate ports of delivery, we have two separate ships delivering the same pump, so we bought the risk, the risk of a pipeline not being delivered by june, we said how do we buy the risk, we don't want all the pipeline to come in june, we want some to come in February, march, april, may, june so we know by the end of june we're not making excuses, so we bought the delivery forward for (censored), probably we bought the risk by paying a notional extra for storage and loading and then making sure the pipe's there when the contract says.

BM: I guess what I'm trying to say there's not, per se, a specific process for implementing risk mitigation strategies, it just becomes part of implementing the project, mitigation strategies are just buried within the project?

ID: It has to be, I would actually encourage that, it becomes business as usual, risk management is not something where you get into a room and do separately, you want to do it as a part of a normal, breathing, sleeping, dreaming every day, every day you've got to get into a meeting and say have I got any new risks, what is happening in the world that's changing out there, is the contractor going broke, is somebody going into liquidation, I want to know that every day, and if you need to update your risk register every day that's what you need to do for a big project, that's what a PM gets paid for is to have his risk register every day, business as usual, you shouldn't wait for a three monthly risk session to do so.

BM: Moving on to that, is there a process for monitoring how risks evolve within projects, or is it a case of you do optioneering, and then design, and…?

ID: Peer reviews, I have peer reviews in the project, and these peer reviews are by people who are not directly involved in the, who are not the lead engineer, not the lead project manager, but somebody not involved in the job, they carry out a formal peer review on the job, we look at risks, we look at the project, we look at the programme, we look at interfaces, we look at quantities, we look at measures, we look at process design, we look at the commissioning, construction, we look at any changes that are happening out there in scope…

BM: Is this is a cyclical thing, or is this…?

ID: It can be…a lot depends on how the project is going too, okay, if the project manager continues to have weekly meetings, we have what is called a deliverable schedule every week we see a list of key deliverables that a project might produce, it might produce a spec, it might produce a contract, it might produce a constructed plant, each one is a deliverable, we make a very comprehensive deliverable schedule for all medium to large projects, these are updated every week, so if you see the trend of them meeting all dates, they said they will issue a spec out for tender, they issued it, they said they would have a contract in place, they did it, now if those things start to happen you can see a nice trend there, you can say look that doesn't require an extraordinary peer review every month, maybe once every two months, then there are ones that start to miss some of the milestones, what I do is allow them to change the dates, so in the deliverable schedule it say, I'll give you some examples, it says required completion it says the date, when they miss the date they're not allowed to take the date of the scope, they've got to strike the date, put a new date, once you see two dates being struck, you'd start to say I want to know more about this, what's happening, who's responsible, and I think you've got to get people in the room and say who, and when they say it's me that's when you stop, because if he says I can't do it because (censored) office is not doing, or (censored) is not doing it, some contractor then we say alright let's get the MD's name for that company, let's give them a call, and that's what happens here, we give them a call and then they say ah, we're waiting for (censored) to give us some direction, we say alright, it comes back to me, I am holding it back, the moment that it's I, then I don't have to do anything about it because the person goes and says look, I'll go and fix it.

BM: Okay so this oversight of, if you like the KPIs of project success is capturing I suppose the evolution of the project risk in the big picture sense, but what about the specific risks that you capture at the optioneering or the concept stage, are these update as the project goes along?

ID: Yes, yes.

BM: And is that by procedure or is that something that's kind of initiative of the project manager?

ID: Both, one is the procedure that requires you to continually update the risk, I can check that out okay (checks document), develop the concept stage, prepare the value engineering, project plan, review it says a review with stakeholders, so it looks at all of the review, there's a proper requirement for review, then there's approvals procedure at that point you've got to again go back and say I want to seek your approval and I have looked at these items okay, see here in the concept plan stage it looks at risk analysis and there's a review by all stakeholders and then there's a formal risk assessment stage, so it's having the procedure would force them to do things to, and a lot depends on the quality of the project manager, some PMs are very, very hot on risk analysis, because they, that's their nature and upbringing and they will have extraordinary sessions on there own, they'll drive the risks down to make them go away.

BM: And again, is it, I guess you had stakeholders within the peer review format, are these the same kind of people that are involved in the assessment process?

ID: No, peer review is a totally independent process, and I'm just going to look at where the peer review is, because it was an important part of my (checks document, notes various review stages, e.g. conduct environmental review, review detailed design documentation, perform design reviews and hazop reviews as per format, progress reporting system and then there are peer reviews)…general manager engineering, head of water services arrange peer review of project by those not directly involved, so that's my role to make sure it's done.

BM: And the storage of the assessment, or the monitoring outputs, the decisions made, how are these captured I mean you mentioned a risk register, is this something on the intranet or is it some kind of documentation that's filed away in?

ID: No, it's on the EP data file, if you look at EP data then we've got a good project filing system under EP data, so if you want to get an access, maybe (censored) or (censored) can get you access and show you, take you through some of the risk registers they are on excel spreadsheets for each project.

BM: So you've got kind of the database if you like so that people can look up similar projects and see?

ID: Yeah.

BM: The hazop that you mentioned, is this at the construction stage, or is this something that happens back at engineering before project management get's involved?

ID: Well what's happened is that we've identified hazop to be carried out at the delivery stage, project delivery stage, because hazop by its nature is like a hazard and operability study where you need a detailed process instrumentation diagram, P&ID and that should have, we call it valves, instrumentation and pipelines, so for each, you know, point of access into a valve, outside of a valve we

go and do three things, look at the flow, temperature and pressure, and quality is another new thing that has happened in the last few years, but we look at flow, temperature and pressure, for each variable if we have no flow, more flow, or low flow, so low flow, more flow, no flow, okay, what happens if there is low flow, what would happen to the pump, pipe, what happens if there is more flow, likewise we do for low pressure, more pressure, no pressure, what'll happen if there is no pressure and likewise temperature, more temperature, would something burn out, and for each one of those items we ask a question and if there's a satisfactory answer given then there is no record of it, because if a project manager can show a P&ID and say don't worry if there's more pressure, the pressure transmitter will sense it, close this valve and we're alright, and if this valve doesn't close then we already have a relief valve that will relieve the pressure, so you see on the P&ID and you sign the P&ID and the revision, and hazop becomes accepted at the point, anything that doesn't get signed off is recorded as a hazop action, and the project manager has to go back and develop a strategy to close it out.

BM: So you've got hazop as the more technically inclined methodology to support the generic 4360 process that you've got, and again it's undertaken by procedure, with kind of verification and…any form of quality assurance on that?

ID: Yes, we've actually done a lot of good work on hazop, we went through the international search, we found very good software that can do hazop for us, and then there is a record of closure of those hazops, and the process instrumentation diagrams, very detailed P&IDs are then updated, revised and there's a close out action to say that all hazop actions have been addressed, that's during the design, then in some of the critical projects we've actually gone back and done a hazop at construction completion, and said well hazops picked up the pipes, valves, the pumps, okay, how about access to them, okay, how about operators standing and trying to operate a valve at six foot, can he do it, so it's like an as built hazop, and then at that stage if it picks up anything, it is again required to be done as a punchlist item before the contract is allowed to be closed, so we've got a good system there for hazops too.

BM: So the problems that come out of hazop, is fed back in to make changes, I know some companies do it because it's perhaps a regulatory requirement…?

ID: We do it because it makes good sense to finish it off, so…we have four simple procedures called project start up, we used to have this in like this volume, and we just narrowed them down all the E&P procedures are this, project start up, project planning, project delivery and project closure, and project closure is very simple, confirm project objectives have been met, finalise the project aspect, finalise all approvals, finalise the project report, so there is a report to be made, identify and recommend any areas for improvement, and hand over to the operator, then feedback, discuss the feedback with myself, and there's a formal handover report made, if you go over to the E&P database, if you want I can show it now, we created a handover, I hope I can find it….(moves to computer, discusses lessons learnt etc….there is a project handover and lessons learnt, feedback through a QA officer).

BM: Another couple of minutes ok?

ID: Yep, I've got another meeting coming two people waiting outside.

BM: Education and training in project risk management, you mentioned you had people sent away for accreditation?

ID: 18 months to take through HPM, we had an external assessor come in, it's an evidence based, show me the evidence of all of the elements of project management, and we also are getting people into masters degree courses, the courses, seminars, train them on safety, train them on project management.

BM: And is this a formalised process, or is it?

ID: Yeah, formalised process, yeah.

BM: And do you have kind of objectives for what this is going to achieve for the project managers?

ID: Yes.

BM: Are these understood in measurable terms, competencies if you like?

ID: Yes, I made a document of what we're trying to achieve out of all this, what we're trying to do is have a better control on how we reach best practice in scope management, cost management, quality management, I can send you something of what we're trying to do with the HPM process, send me an email, if I don't send you, just nag me…

Appendix H

Empirical observations relating to the attributes that define maturity in risk analysis in our revised model, derived from the final case study

Attribute	Case study observations
Procedures	Procedures guided the conduct of risk analysis within project management, asset management and OH&S to varying levels of completeness, detail, and prescription.
Roles and responsibilities	Allocations of high level responsibilities were enshrined within the corporate risk management policy. Outside of project management and OH&S, specific risk analysis roles were allocated informally or on a case by case basis.
Initiation criteria	Initiation criteria were formalised within: project management, where risk analysis was initiated prior to financial approval depending on the cost, complexity and novelty of the project, and was updated at key project milestones; and in occupational health and safety, where, for example, manual handling risk analyses were initiated prior to the receipt of hazardous chemicals; and within process engineering, wherein hazop studies were initiated for complex or costly processes at a set stages of design completeness; whilst timescales for revising risk analyses of various asset classes were observed in asset management, though not uniformly.
Resource management	A difficult aspect to assess objectively. However, a recurring theme was the limited range of technical risk analysis methodologies, which one interviewee implied had led to the marginalisation of data analysis in favour of judgement-based assessments in risk analysis.
Input data management	We observed a general absence of predefined strategies of data collection to inform each function's approach to risk analysis. By this, we mean that, at the process level, risk analysis was not typically informed by a prior consideration of the data requirements and methods of capture; instead, data collection was undertaken on an *ad hoc* or case by case basis, except where analytical methodologies were applied.
Output data management	Technical risk analysis methods adopted (e.g. HAZOP) were largely self-documenting, whilst broadly similar reporting formats were adopted within each function for non-technical risk analysis outputs. However, the absence of risk registers (IT-based tools for the storage and access of outputs), combined with cultural and departmental boundaries, appeared to limit the dissemination of risk analysis outputs.
Verification	Management or supervisory signs offs and periodic audits served to verify compliance with risk analysis procedures in OH&S, whilst sign offs and expert facilitation served the same purpose within project management and engineering. Additionally, this expert facilitation, the prior use of the Delphi technique within project risk analysis, and "peer reviews" of varying degrees of formality within each function were mechanisms observed for quality control of risk analysis.
Validation	Approaches to validating risk analysis processes were not widespread, and where undertaken were often implicit or informal. These included adherence to external standards and best practice guides (although these were typically concerned with principles rather than prescriptions); external audits *incorporating* an examination of risk analysis practices (in OH&S); and external peer reviews of risk analysis methods (within drinking water quality management).
Organisational learning	We observed cyclical and event-driven reviews (e.g. triggered by an incident or changes to regulations) of risk analysis processes conducted to varying levels of formality. These were informed by both internal feedback (e.g. verification findings, incident and near miss reports, consultations with management and operating staff, explicit analyses of the risk management performance of projects) and external feedback (e.g. changes to external standards or best practice guides, professional networks, trade journals, peer review findings). Anecdotal evidence suggested that internally driven learnings tended to focus more on error correction, e.g. simplifying risk identification checklists to make them more "user friendly," updating risk analyses to incorporate hazardous events that had occurred in practice but had previously been excluded from consideration (e.g. bore casing failure); whilst true process improvements were externally driven (i.e. fundamental changes in risk analysis processes were driven by changes to external standards or best practice guides).
Stakeholder engagement	A broad spectrum of knowledge, expertise and perspectives was reflected within each function's approach to risk analysis (e.g. the typical make up of the manual handling hazard assessment team included the: health and safety representative; supervisor / team leader; engineering representative; maintenance representative; and the health, safety & rehabilitation co-ordinator). The engagement of external stakeholders was observed to occur in isolated cases, where they added value to the analysis, rather than acting as passive spectators (e.g. where specialist knowledge was required which was not held within the utility).
Competence	Basic training modules in risk analysis were delivered to staff within OH&S, process engineering and project management. Elsewhere, there was a reliance on "on the job" training. No explicit definition of the competencies required for risk analysis, nor methods for measuring whether they existed or had been effectively imparted.

Appendix I

Maturity hierarchy for risk based decision making in revised model

LEVEL 5: *Adaptive*	Validation	A broad range of mechanisms are in place to capture feedback potentially challenging the validity of the risk based decision making process (*e.g.* benchmarking surveys, professional networks, external peer reviews, technical validation of decision analysis techniques).
	Organisational learning	Norms and assumptions underpinning the design of the risk based decision making process are openly questioned, critically evaluated and, where appropriate, revised in light of validation findings (*i.e.* double loop learning).
LEVEL 4: *Controlled*	Verification	Verification extends beyond rigorous mechanisms to ensure procedural compliance (*e.g.* sign offs supplemented by in-depth audits) to provide formal quality control of risk based decision making (*e.g.* conflict resolution techniques, peer reviews, challenge procedures, Delphi technique, *etc.*).
	Organisational learning	Root and common causes of errors in the execution of risk based decision making (*e.g.* deficient communication, overly complex procedures, lack of education and training in the application of decision analysis techniques) are identified and resolved. Modifications to the design of the process are identified, evaluated and implemented within periodic and event-driven reviews, but remain largely reactive and externally driven (*i.e.* mirroring changes to codes, standards, guidelines, *etc.*).
LEVEL 3: *Defined*	**The critical and key risk based decision making practices are explicitly undertaken.**	
	Procedures	Procedures exist to guide the execution of risk based decision making, with an appropriate degree of standardisation, detail, and complexity.
	Roles and responsibilities	Risk based decision making roles and responsibilities are allocated with sufficient regard for staff competencies and authorities.
	Initiation Criteria	Cyclical and event-based criteria are in place to guide the application of decision analysis techniques (*e.g.* multi-attribute analysis, cost-benefit analysis, cost estimates, feasibility studies in engineering, *etc.*).
	Resource management	The requisite monetary, human and technical resources are identified, acquired and deployed in support of risk based decision making.
	Input data management	The requisite data inputs are identified, acquired and deployed in support of risk based decision making.
	Output data management	Risk based decision making outputs are collected, stored and disseminated in a manner that supports risk based decision making, satisfies audit requirements, and facilitates organisational learning.
	Verification	Basic mechanisms are in place to ensure compliance with risk based decision making procedures, focussing on outputs rather than tasks performed (*e.g.* sign offs on receipt of completed decision analyses).
	Validation	The validity of the risk based decision making process is questioned in light of changes to regulations, codes and standards.
	Organisational learning	Non-compliances with risk based decision making procedures are resolved on a case by case basis (*i.e.* treated as isolated errors requiring sanction to prevent their recurrence). Improvements to the design of the risk based decision making process are implemented in a reactive, *ad hoc* manner (*e.g.* in response to changes in codes or regulations).
	Stakeholder engagement	Risk based decision making is characterised by participatory mechanisms combining a broad cross section of internal and external knowledge, experience, skills and perspectives, based on explicit guidelines or criteria for stakeholder engagement (*e.g.* in constructing decision criteria, identifying risk reduction options, *etc.*).
	Competence	Staff exhibit adequate knowledge, skills and experience in risk based decision making. Education and training in risk based decision making is planned and executed based on established competency requirements.
LEVEL 2: *Repeatable*	**The critical risk based decision making practices are explicitly undertaken.**	
LEVEL 1: *Ad hoc*	**Risk based decision making is absent; or the critical practices are implicitly or incompletely performed.**	

Appendix J

Descriptions of the risk based decision making process maturity attributes and their rationale for inclusion within our revised model.

Attribute	Description	Rationale*	Key aspects*
Procedures	The rules guiding the execution of risk based decision making.	Procedures serve to capture and disseminate knowledge of the optimal conduct of risk based decision making so that it is maintained within the organisational memory rather than as hidden expert knowledge (NEA/CSNI, 1999), and so ensure its consistent, efficient conduct.	Appropriate standardisation and formalisation of procedures taking into account personnel experience and knowledge; participation of end users (*e.g.* decision makers) in their development; matching detail with complexity of work; making explicit the rationale for conducting decision analysis; being based on an analysis of the tasks required (NEA/CSNI, 1999; Health and Safety Laboratory, 2003).
Roles and responsibilities	Assignment of personnel to risk based decision making roles and responsibilities.	To avoid the "not my job" phenomenon (Joy and Griffiths, 2005), and ensure risk based decision making receives appropriate focus and resource allocations.	Matching role descriptions and assignment of responsibilities with personnel competencies and authorities (NEA/CSNI, 1999). Supporting well meaning statements that "risk management is everyone's job" with specific requirements.
Initiation criteria	Stages or conditions which initiate the application of decision analysis techniques.	To ensure decision analysis is undertaken to the appropriate level of formality and rigour, commensurate with, *e.g.*, the complexity and criticality of the decision, and the uncertainty and level of risk associated.	Identifying where formal decision analysis is necessary vs. where heuristics (*i.e.* rules of thumb) or professional judgement is sufficient, and making this explicit in criteria for the application of decision analysis techniques.
Resource management	The planning, acquisition, and deployment of funds, techniques and staff in support of risk based decision making.	Resourcing of risk based decision making is particularly critical during periods of reduced budgets and downsizing, which may bring an emphasis on economic rather than safe operation (NEA/CSNI, 1999).	Sufficiency and availability of financial resources; access to sufficiently competent human resources; and a range of risk based decision analysis techniques which reflect the complexity of the organisation's activities, working environment, regulatory obligations and institutional capacities.
Input data management	The identification, collection, and storage of risk based decision making data inputs.	The systematic identification and capture of data requirements serves to ensure decisions are underpinned by objective data evaluation, rather than reflecting best guesses in the guise of "expert judgement."	The definition of data requirements / data sources for risk based decision making, either at the process level or, where not practical, on a case by case basis, and mapping these to data collection and storage systems.
Output data management	The collection, storage and dissemination of risk based decision making outputs.	Risk based decision making outputs must be systematically recorded to inform the implementation process, for audit and training purposes, and to facilitate quality control and future reviews (COSO, 2004; CSA, 2004).	Documenting in-depth the risk based decision making outcomes, not simply the option selected (*e.g.* sources of data, assumptions used, evaluation criteria adopted, justification, *etc.*). This allows scrutiny of beliefs, and helps identify and clarify sources of disagreement. This clarification of the rationales underlying decisions taken promotes respect for the opinions and judgements of decision makers, and directs any required negotiations (*e.g.* during peer reviews or conflict resolution in quality control) towards these issues, as opposed to focussing on the character *etc.* of disputants (Maguire and Boiney, 1994).
Verification	Ensuring compliance with risk based decision making procedures, and providing quality control of the execution of risk based decision making.	The mere existence of procedures is not in itself enough to ensure that staff actions will be consistent with them (Hoyle, 2001; ISO, 2000). Errors of omission or commission (*e.g.* due to misunderstanding instructions, carelessness, fatigue or management override), may cause deviations. Similarly, procedural compliance does not ensure the quality of execution of risk based decision making.	Implementation of mechanisms to ensure adherence to procedures (*e.g.* auditing, "sign offs") and to sanction non-compliance. Quality control mechanisms (*e.g.* peer reviews, Delphi panels) should be implemented with explicit methods for controlling (*e.g.* establishing group consensus iteratively) or evaluating (*e.g.* quality criteria) the quality of the decision process *followed*. Additionally, conflict resolution techniques may prove valuable in decision contexts requiring consensus (*e.g.* strategic level decisions, policy issues, environmental issues), but where high uncertainty, potentially disastrous outcomes, divergent preferences and interpretations of facts or analyses conspire to complicate the reaching of consensus (Maguire and Boiney, 1994). An appropriate balance between the resources required, the constraints of bureaucracy, and the benefits of process control should be struck.
Validation	Assessing the fundamental correctness of	The willingness and means to question the validity of current risk based	Formalised approaches to validation include: statistical or mathematical approaches to validating

	the risk based decision making process design (*e.g.* that the correct techniques are being applied, that the correct initiation criteria are in place).	decision making practices is required to show due diligence and ensure that current practices are legitimate, and is further a prerequisite to the continual improvement of risk based decision making.	technical methodologies, independent peer reviews, and benchmarking surveys; and informally may draw upon: professional networks, trade and scientific literature, *etc.*
Organisational learning	The manner in which the organisation identifies, evaluates and implements improvements to the design and execution of risk based decision making.	Mechanisms for verification and validation are mere panaceas if their findings are not acted upon, *i.e.*, if they are not used to rectify deficiencies in the design and execution of risk based decision making.	Reviews should: be undertaken at specified intervals and on an event driven-basis; consider a broad range of internal and external feedback; focus on improving the validity of the risk based decision making process and the effectiveness of its execution, not on ensuring it complies with a given standard; treat errors of omission or commission in the execution of risk based decision making not as isolated lapses requiring sanction to prevent their re-occurrence, but as opportunities to identify and resolve root and common causes of error; and be supported by a learning culture, wherein current methods and approaches to risk based decision making, and their underlying assumptions, are open to question and critical evaluation.
Stakeholder engagement	The engagement of stakeholders, both internal and external to the utility, for the purpose of harnessing a broad range of perspectives, knowledge, skills and experience in risk based decision making.	The legitimacy of risk based decision making outputs depends upon appropriately broad stakeholder engagement, as risk is an intrinsically multi-faceted construct, whose comprehensive understanding is often beyond the capabilities of individuals or small groups.	A team approach to risk based decision making which pools the knowledge, skills, expertise and experience of a range of perspectives is preferable (Health and Safety Laboratory, 2003; MHU, 2003; Joy and Griffiths, 2005). External stakeholders may be engaged to: capture expertise (*e.g.* consultants); confer additional legitimacy on the analyses; communicate due diligence (*e.g.* regulators); and capture community values and ensure they are incorporated within the decision making process (e.g. reflected in option evaluation criteria).
Competence	The ability to demonstrate knowledge, skills, and experience in risk based decision making to the level required.	The legitimacy of risk based decisions depends to a large extent on the capacity of staff to critically evaluate available information with respect to criteria (implicit or explicit) *via* decision analysis techniques or heuristics, *i.e.* on staff competencies.	Definition of required staff competencies in risk based decision making; evaluation and implementation of appropriate education and training vehicles to develop / maintain those competencies (*e.g.* class room learning, external workshops); providing "on the job" training under adequate supervision; designing and implementing methods for evaluating the efficacy of educating and training (*e.g.* for measuring that the required competencies have been imparted).

*NB for references, see Chapter 7.