Chairperson and Subcommittee Members
AUDIT AND RISK SUBCOMMITTEE

12 FEBRUARY 2015

Meeting Status: **Public**

Purpose of Report: For Decision

RISK MANAGEMENT FRAMEWORK

PURPOSE OF REPORT

1 This report seeks approval from the Audit and Risk Subcommittee to implement a proposed comprehensive risk management framework for effective identification and management of Council's significant risks.

DELEGATION

2 The Audit and Risk Subcommittee has delegated authority to consider this report under the following delegation in the Governance Structure, Section C.4.

6 Without limiting the generality of this delegation the Subcommittee has the following functions, duties and powers:

Risk Management

6.9 Ensure that Council has in place a current and comprehensive risk management framework and associated procedures for effective identification and management of Council's significant risks.

6.10 Review and evaluate Council's risk management framework and make recommendations to the Corporate Business Committee on risk mitigation.

BACKGROUND

3 Last year, the Council suffered negative publicity from several incidents, including the Council's support for the Clean Tech Trust.

4 In September 2014, The Tanner Ritchie report made ten recommendations to Council to better inform decision-making when considering significant business proposals (SP-14-1297). Council's actions and responses to these recommendations are provided in Appendix 1.

5 In light of these events, it is timely for the Audit and Risk Subcommittee to ensure that Council has in place a current and comprehensive risk management framework to identify, mitigate and manage future risks.

6 Effective risk management is critical to any organisation's success; it provides enhanced assurance that objectives will be achieved, opportunities will be maximised, and losses will be minimised.

CONSIDERATIONS

Integrated Risk Management Framework

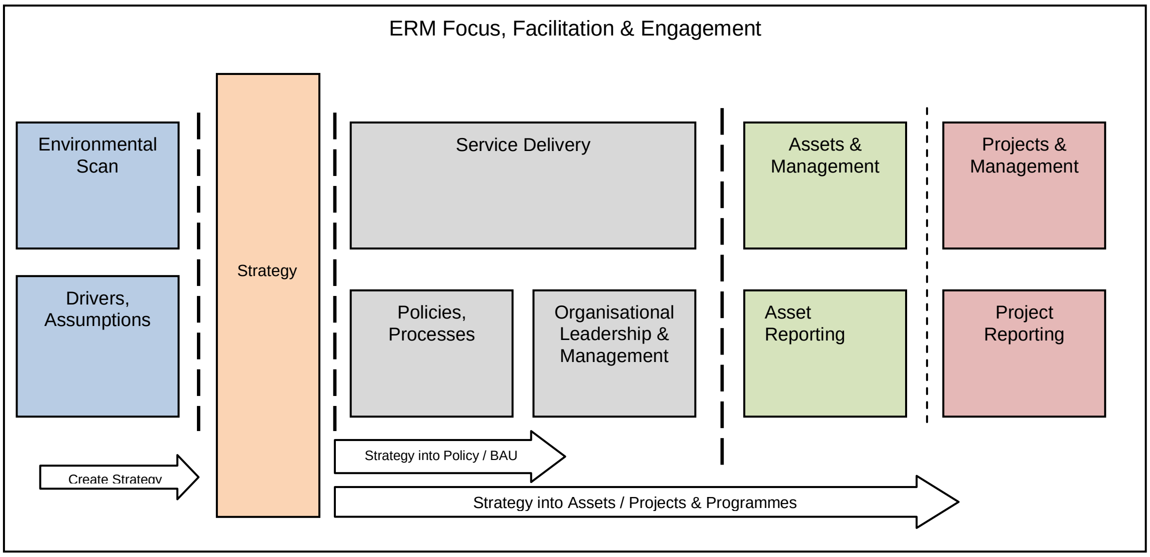
7 An effective organisational approach to risk management is one which embodies and integrates robust risk management philosophy, thinking and practice directly into business activities, capability and culture. It focuses on strategic, tactical and operational achievement.

8 An integrated risk management framework is not a standalone system or document. Rather it is intrinsic to the translation of stakeholder expectation into strategy, into programmes, and into action.

9 Given that risks comprise both threats and opportunities, an integrated risk management framework provides focus, facilitation and engagement on how:

- Strategy is developed to deliver on organisational objectives and manage the risks posed by externalities, stakeholder expectations and desired goals.
- Policies, procedures and programmes are developed to deliver on the strategies and manage the risks identified.
- Risks are managed at essential levels of activity to support the achievement of relevant objectives.

10 An integrated Risk Management Framework as illustrated below:

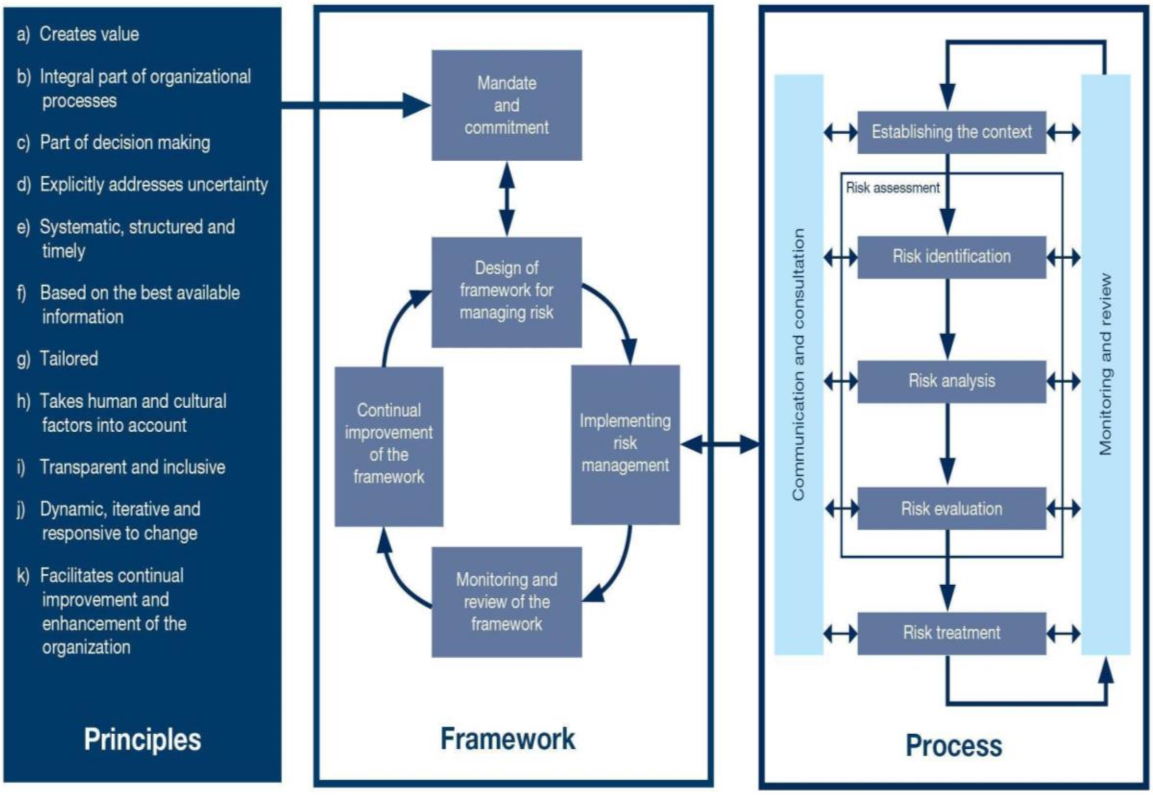


11 An integrated approach to risk management positively influences the right behaviours in the management of activities on a day to day basis All decision-making incorporates the consideration of risk. Risk reporting is easily facilitated and is comprehensive and relevant being based on proactively identified and well thought through information. This gives confidence that the right risks are being managed, in the right way, at the right time and by the right people.

12 This contrasts with a risk management approach that is driven predominantly by a risk reporting requirement or mandate. This tends to result in a compliance based, mechanistic system that the business quickly regards as having little relevance to its day to day activities and decision making. As a result, any risk reporting is based on ill-considered and variable information. Big threats and/or opportunities are easily overlooked and decision making is flawed.

Accepted Risk Management Framework Principles and Guidelines

13 An integrated risk management framework is consistent with the widely accepted and adopted 'ISO 31000 Risk Management Principles and Guidelines' and is generally referred to as an Enterprise Risk Management (ERM) model, as illustrated below.



14 The benefits of an ERM model for the Council would include:

- increase the likelihood of achieving objectives;
- encourage proactive management;
- increased awareness of the need to identify and treat risk throughout the Council;
- improve the identification of opportunities and threats;
- comply with relevant legal and regulatory requirements and international norms;
- improve mandatory and voluntary reporting;
- improve governance;
- improve stakeholder confidence and trust;
- establish a reliable basis for decision making and planning;
- improve controls;
- effectively allocate and use resources for risk treatment;
- improve operational effectiveness and efficiency;
- enhance health and safety performance, as well as environmental protection;
- improve loss prevention and incident management;
- minimise losses;
- improve organisational learning; and
- improve organisational resilience.

15 It is proposed that Council establishes an ERM approach that is consistent with the principles and guidelines of 'ISO 31000 Risk Management' with immediate effect.

Implementation Considerations

16 The Council's development towards achieving a fully integrated risk management framework can be measured and monitored against an ERM Maturity Model (See Appendix 2). The model describes five separate levels of ERM maturity, starting at 'ad-hoc' (Level 1) and progressing to 'Enterprise-wide' (Level 5). Each level considers the organisation's risk maturity against the following key parameters:

- Leadership;
- Culture;
- Risk Management Procedures;
- Capability;
- Integration; and
- Monitoring

17 The Council has taken preliminary steps towards a structured risk management framework and is currently considered to be 'Mandated' (Level 2). Achieving Enterprise-wide' (Level 5), in an organisation the size of the Council, typically takes between two to three years.

18 A proposed implementation plan for progressing to 'Enterprise-wide' (Level 5) has been developed (see Appendix 3). This plan provides for many of the fundamental ERM elements to be in place, and attendant benefits delivered within 12 months, taking the organisation to 'Managed' (Level 4), with some aspects of 'Enterprise-wide' (Level 5). Effort beyond the 12 months period largely involves consolidation and refinement and is targeted at embedding and improving organisation risk management culture.

19 The design principles incorporated in the implementation plan include;

- Strong management mandate, commitment and leadership;
- Focus on organisation risk culture;
- Accountability;
- Appropriate resources;
- Transfer of knowledge, expertise and hence capability to the business;
- Consistent process;
- An all of business integrated approach (strategic, tactical and operational);
- Robust communication and assurance to management and governance levels;
- Encouragement of the right conversations and outcomes;
- Staff awareness and active people engagement;
- Monitoring and review; and
- Continual improvement

20 It is critical that the Risk Management Framework project proceeds in the most efficient manner possible and achieves an optimal solution. In that regard the plan assumes the part time engagement, at least over the initial 12 months, of an external consultant that is highly skilled and experienced in ERM development, implementation and operation and who is aware of the traps and pitfalls of putting ERM in place.

21 An independent consultant has been identified and has already provided assistance with the preliminary thinking and planning. It is important to note that the plan calls for the consultant to place emphasis on knowledge transfer, increasing risk management capability and expertise within the organisation and thereby minimising costs and maximising value.

22 The following table highlights the key risks that have been identified regards the successful implementation of an integrated risk management framework and what measures can be taken to best mitigate these risks.

	Risk Description	**Treatment**
1	Poor day to day management of risks due to the framework being seen by the business as something separate and mainly as a compliance and/or tick box exercise. The business perceives that it is too busy doing business as usual to do this	• Don't throw away what's already working, rather provide encouragement and support. • Communicate the meaning and value of risk management to the business. • Senior management to encourage implementation of better risk management in activities as a cultural norm – the way we do things around here, it is business as usual • Make risk and risk management interesting and a regular topic of manager catch-ups with reporting staff • Value voluntary risk reporting, don't punish or devalue the reporter • Reward good risk management • Risk champions to assist in embedding risk management culture in teams, encouraging the right behaviours
2	Risks keep changing or being redefined when reported due to lack of trust and or accountability for getting it right downstream	• Ensure accountabilities for agreeing, signing-off and escalating risks are defined and well implemented • Trust the accountabilities • Clear process and understanding of how to identify, define, analyse and evaluate a risk
3	Poor understanding of how to identifying and accurately define risks	• Ensure accountabilities for agreeing, signing-off and escalating risks are defined and well implemented • Trust the accountabilities • Clear process and understanding of how to identify, define, analyse and evaluate a risk
4	Risks are over or under mitigated due to poor understanding of organisation risk tolerance and appetite, tendency for being overly risk averse	• Ensure organisational risk tolerance and appetite understanding is adequately evolved, defined and communicated • Encourage calculated risk taking, accept failure in some already accepted high risk ventures

	Risk Description	Treatment
5	Risk management and reporting ends up in silos due to excessive vertical accountability and lack of a cross business thinking	• Ensure cross business initiatives are given risk management focus, encourage cross group risk management thinking • Analyse vertical risk information to identify cross business or otherwise common themes
6	Only threats identified, opportunity dimension of risk ignored due perceptions of risks as only being negative	• Staff awareness, mentoring etc. to provide sufficient focus on the opportunity dimension of risk
7	Poor management of risks due risk management perceived as something the consultant and/or risk manager and/or risk champions do	• Risk management leadership to facilitate and mentor rather than do all the detailed work • Senior leaders to play their role • Make risk management part of performance management • Encourage voluntary reporting
8	Project milestones not achieved due to insufficient internal resource being made available	• Risk champions identified and made available
9	Poor reception of risk reports by Council and/or the Senior Leadership Team due to poor alignment with Council/ Senior Leadership Team expectations	• Discuss expectations with the Audit and Risk Subcommittee and Senior Leadership Team - listen to feedback and adapt quickly

Financial Considerations

23 The cost of the independent consultant in providing assistance with the preliminary thinking and planning will be absorbed within the 2014/15 Annual Plan.

24 Subject to approval to proceed, the total estimated work effort required by the external consultant for the implementation of the risk management framework will be determined.

Legal Considerations

25 There are no legal considerations at this time.

Policy Implications

26 A Risk Management Policy will be developed (targeted for March 2015) so as to inform an integrated risk management framework that provides focus, facilitation and engagement on how:

- Policies, procedures and programmes are developed to manage identified risks.
- Risks are managed at essential levels of activity to support the achievement of relevant objectives.

Tāngata Whenua Considerations

27 There are no tāngata whenua considerations.

Publicity Considerations

28 There are no publicity considerations at this stage.

SIGNIFICANCE AND ENGAGEMENT

29 This matter has a low level of significance under the Council Policy.

RECOMMENDATIONS

30 That the Audit and Risk Subcommittee endorses the implementation of the proposed integrated risk management framework.

Report prepared by:

Mark de Haast
Financial Controller

Approved for submission by:

Wayne Maxwell
Group Manager Corporate Services

Approved for submission by:

Stephen McArthur
Group Manager Strategy and Planning

APPENDICES:

1. Appendix 1: Council's actions and responses to the Tanner Ritchie report recommendations
2. Appendix 2: Enterprise Risk Management Maturity Model
3. Appendix 3: Enterprise Risk Management Implementation Plan

Appendix 1

Council's actions and responses to the Tanner Ritchie report recommendations

Ref	Report recommendations	Action/response	Key controls/mitigations	Timeframe
1	A full business case needs to be prepared for any significant business proposal seeking Council support. The council should seek appropriately qualified external support to analyse any proposal if necessary, and engage in a sound 'due diligence' process.	A business case process for significant proposals/projects has been established that has the following principles: ▪ Business cases will clearly demonstrate the financial, strategic, commercial, feasibility/management and economic cases for change ▪ Proposals will follow the Treasury's Better Business Case guidelines and process which includes a strategic assessment, indicative business case, detailed business case and implementation business cases ▪ Significant business case will be reviewed through its stages by the senior leadership team (SLT) and Council to give confidence to decision makers that investing in a proposal or project is justified ▪ Where necessary, any project or proposal (as part of the business case process) will seek appropriately qualified external support to analyse the proposal ▪ A sound due diligence process will be followed.	▪ Policies and procedures ▪ GM,SLT and Council review and approval of significant business cases ▪ CBC reporting on performance of key projects.	▪ Immediate ▪ Embed as part of the LTP and project/proposal processes.
2	There may be components within the overall business proposal that need specific commercial analysis (i.e. the Stage 2 building proposal in this instance).	As part of the business case process, and where applicable, commercial elements will be examined. These include, but are not limited to: ▪ Building proposals ▪ The procurement strategy ▪ The service requirements, risk allocation and payment mechanisms ▪ Contractual issues.	▪ Policies and procedures ▪ GM, SLT and Council review and approval of significant business cases.	▪ Immediate ▪ As part of any significant business case proposal.
3	The role of the Council in respect of particular projects needs to be determined, and the nature of its interests set out formally and understood by all involved. Why it should invest in a proposal needs to be properly elaborated and reviewed.	As part of the business case process the Council's role in a project or proposal will be critically examined. In order to find a preferred way forward option the business case investment objectives and case for change will examine: ▪ The fit with strategy and case for change ▪ The opportunity for key stakeholders to influence the direction ▪ Existing arrangements, scope, benefits, risks and constraints. There will often be a series of problems that the project or proposal seeks to address, or opportunities that it seeks to take advantage of. These will form the basis of consideration of the options such as: Should the project or proposal be delivered now or in the future? Should it be delivered by the Council? If yes, should it be governed in-house or at arm's-length? The nature of the Council's interests and arrangements with any project and proposal should be clearly outlined and formalised as part of the preferred way forward option.	GM,SLT and Council review and approval of significant business cases.	▪ Immediate ▪ As part of any significant business case proposal.

Ref	Report recommendations	Action/response	Key controls/mitigations	Timeframe
4	If a new organisation is to be established, and if the Council is required to invest in it, consideration should be given to what structural options are available and how the Council's 'ownership' as well as its 'purchase' interests should be formulated.	If a new organisation was to be established the Council would require that key elements would need to be applied include, but are not limited to: ▪ Council approval to establish the organisation ▪ Clarity about the organisation's purpose and strategic direction ▪ Clarity around the organisations' roles and behaviours ▪ Getting the right people, in the governance and management roles ▪ Building and maintaining transparent and accountable processes ▪ Building and maintaining effective relationships.	Business case options analysis and approval processes required to initiate Council consideration to set up a new organisation.	As required.
5	Care needs to be taken to understand the implications of the investment approach or model chosen for the purpose. In particular, the style of management subsequently required for a significant Council investment should be fully explored from the outset.	A key element of the Councils business case process is the feasibility and management case which examines the investment approach and model including: ▪ What are the different options/models that could be used to deliver the project or proposal? ▪ Our ability/track record in sponsoring/delivering the project/proposal? ▪ Management arrangements ▪ What people, financial and time resources will the project/proposal need?	GM, SLT and Council review and approval of significant business cases.	As required.
6	The Council's ongoing relationship with any new entity that it is supporting should be specified in a relevant form of agreement—i.e. either an MoU, a contract for services, or some other form of performance agreement.	The Council will follow the key steps required to implement good contract and relationship management. These include, but are not limited to: ▪ Define the requirements ▪ Develop the performance management framework ▪ Develop the relationship management framework ▪ Develop the risk management framework ▪ Enable continuous improvement ▪ Decide what resources will be needed to manage the contract.	GM,SLT and Council review and sign-off of the relevant form of agreement.	As required.
7	Risks that are identified for the Council should be incorporated into a relevant risk register and regularly monitored and updated. Appropriate mitigation steps should be in place and acted upon.	The Council is fully committed to effective risk management and best practice in the identification, evaluation and control of risks, in order to: ▪ Integrate risk management into the culture of the Council ▪ Manage risk in accordance with standards and best practice ▪ Fully document major threats and opportunities ▪ Clearly identify risk exposures ▪ Prevent injury and damage and reduce the cost of risk ▪ Ensure conscious and properly evaluated risk decisions.	▪ Risk registers for key project risks; and as a key assessment tool for developing the strategic case of the business case ▪ Review of key strategic risks and mitigation strategies throughout the SLT and the Audit and Risk Committee.	Immediate.

Ref	Report recommendations	Action/response	Key controls/mitigations	Timeframe
8	Where there is a technical component to any proposal (e.g. clean technology in this instance) appropriate external advice should be sought. In this instance, were the clean technology enhancements required by the Council actually likely to be commercially viable?	Appropriate external advice will be sought to ascertain the commercial viability of a proposal as part of the business case development process.	As part of the business case review and approval process.	As required.
9	There needs to be clear expectations established from the outset as to financial and service performance reporting requirements.	In line with the requirements of the Local Government Act 2002 the Council will establish expectations and regularly undertake performance monitoring of any organisation or business relationship to evaluate its contribution to the achievement of: ▪ The Council's objectives for the organisation or business relationship ▪ The desired results ▪ The Council's overall aims and outcomes.	Governance, monitoring, control and reporting requirements.	As required.
10	Appropriate steps need to be taken by both parties to a business relationship to understand the other's strategy and business direction so that any issues can be resolved quickly. There is likely to be a need for relationships to be established and maintained at both Councillor as well as at staff levels.	Providing the right environment for both parties to a business arrangement to succeed involves applying key principles such as: ▪ The entity should have a clearly defined purpose. ▪ The entity's governing body should be effective ▪ The parties involved should be assigned clear roles and responsibilities ▪ The Council should be able to hold the entity to account ▪ Mechanisms for accountability to the community must be in place. These principles reinforce the required ongoing and cooperative relationship. They guide the interpretation of the processes that direct, control and hold entities to account; their stewardship, openness, programme delivery and leadership.	Governance, monitoring, control and reporting arrangements.	As required.

Appendix 2
Enterprise Risk Management Maturity Model

Maturity	Leadership	Culture	RM Procedures	Capability	Integration	Monitoring
Enterprise wide 5	Board and senior leaders model best practice RM. RM is incorporated into 'the way we do business'. Stakeholder, customer and supplier input sought. Proactive approach.	RM is central to business as usual and culturally driven All decision-making involves explicit risk consideration Increased focus on opportunities, improvement, innovation and adaptability. Risk is seen as about gaining strategic advantage	Risk is seen as uncertainty RM policy and strategy documented and known to staff. RM procedures are consistent and continuously improved; benchmarking / learning from other organisations.	Key staff and managers are competent and engaged in RM. External advisors may be used under the initiative of in-house personnel. RM success is celebrated. RM is an important performance criteria	RM occurs across hierarchies and organisational boundaries. RM is integral to key business processes, performance management etc operating up, down and across the organisation.	Full RM trend analysis Risk linkages and themes being identified and discussed Value add reporting. Effectiveness of RM is monitored and informs future RM. RM failures reviewed to identify learning's.
Managed 4	Each senior leader actively promotes risk management within their area. RM seen as a means to achieve business goals and add value. Valuable risk conversations are beginning to occurring at relevant forums	Risks are regularly identified by staff and managers and escalated There are few surprises. RM still seen as an add-on to business as usual. Longer-term RM focus implemented.	Risk is seen as uncertainty RM policy and procedures regularly reviewed RM tools and templates are available RM implementation plan underway Risk authorities being linked to delegations	Adequate in-house bolstered with relevant external RM support RM responsibilities are being linked to position descriptions. RM is art of induction RM education sessions regularly available.	RM is applied mainly vertically through the line management structure. although some cross organisation risk think occurring	RM implementation is monitored and actions taken to address shortfalls. RM reports quarterly to Groups, SLT, Board.
Repeatable 3	Senior leaders regularly review risk reports. Strong focus on compliance risks. Medium-term RM focus.	Growing awareness of risk. Increasing willingness to use formal channels to notify and escalate risks. Risk champions may not be valued	RM policy and procedures In place but only partial/inconsistent implementation. Some RM tools and templates developed. RM implementation plan developing	External RM advice sought One or more in-house RM experts appointed RM education sessions provided to some staff and managers. A few have RM expertise	RM is still applied primarily to projects. Silo responses to risks	Periodic RM reports to senior leaders and Board Compliance with RM policy is variable across the organisation.
Mandated 2	SLT or Board mandate for RM One senior leader has responsibility for RM. Specific risks discussed at senior leadership meetings.	Recognition that some risks exist and must be addressed. Risks are seen as negative consequence events Risks are discussed informally and escalated as deemed by the individual.	RM procedures are beginning to be identified communicated. High reliance on the knowledge, experience of individuals. Inconsistent approaches for managing different types of risk	External expert RM management advice Some RM philosophy education to senior leaders. Heavy reliance on historical practice.	RM is seen as an additional requirement to business as usual. RM applied to projects Silo responses to risks	Compliance focus, RM only motivated by reporting requirements RM reports occasionally provided to Board Reports are narrative and based on the knowledge of key individuals.
Ad-hoc 1	Senior leaders address high level risks as they arise. Risks may be perceived as issues Short-term RM focus. Reactive RM.	Perception that notifying a risk is a sign of failure. Risk seen as a loss, harm or cost RM, finance and insurance ambiguous	No standardised RM procedures. Ad hoc approaches applied on a case-by-case basis.	No understanding or experience of risk management and its link to the achievement of business objectives.	RM is seen as an 'extra' which must be done in response to a crisis situation. Compartmentalised responses to risks	No monitoring or reporting of risks.

Appendix 3

Proposed Enterprise Risk Management Implementation Plan (12 months)

Task	By who	1	2	3	4	5	6	7	8	9	10	11	12
Discuss ERM, Risks with Senior Managers	Cons												
Develop ERM Policy, Communicate	Cons/Comms												
Verify current RM capability per Group	Cons												
Develop Corporate RM Plan	Cons/SLT												
Define RM Accountabilities	Cons/HR												
Identify RM Champions & Mentor	Con/GMs												
Develop & Approve Generic Risk tool	Cons/RMCs												
Develop Staff Training Strategy & Plan	Cons/RMCs												
Staff Training and Mentoring	Cons/RMCs												
Develop Group RM Plans	Cons/RMCs/GMs												
Develop Risk Reporting Process	Cons/RMCs												
Group Risk Forums Start then Quarterly	Cons/RMCs/Groups												
SLT Risk Forum Start then Quarterly	Cons/RMCs/SLT												
Risk Communication/Escalation Strategy	Cons/RMCs												
Develop Full RM Manual and Guide	Cons/RMCs												
Audit and Risk Forum Start then Annual	Cons/CE/A&R												
Further Assure RM in Projects, Assets	Cons/RMCs												
Clarify Risk Authorities Link Delegations	Cons/Finance/Legal												
Review/Enhance Risk Reporting Systems	Cons/RMCs												
Review and Report Progress	Cons												

Key: Cons = Consultant
RMCs = Risk Management Champions

Appendix 3
Proposed Enterprise Risk Management Implementation Plan (13 to 36 month)

The Implementation plan for years 2 & 3 focuses on consolidation and refinement and includes:

- ensure all decision making includes consistent risk consideration;
- review and ensure capability;
- further developing risk appetite and risk tolerance understanding;
- engaging people and encouraging the right conversations and outcomes;
- ensure consistency of risk management application in operational areas; projects, asset management etc;
- improving the quality of risk reports;
- analysing linked risks to understand common themes;
- investigating more sophisticated risk management tools;
- establishing further links to delegations and position descriptions;
- understanding the opportunity dimension of risk;
- ensuring good linkages to H&S, business continuity, legal etc;
- monitoring and review of performance, experience and feedback; and
- continual improvement.