An Chomhairle Oidhreachta
The Heritage Council

Working for heritage | Working with communities

Risk Management Policy

& Operational Framework

for the Heritage Council

Approved by the Board of the Heritage Council on July 17th 2020

An Chomhairle Oidhreachta
The Heritage Council

Working for heritage | Working with communities

Contents

1. Introduction

1.1 Policy Scope

In line with requirements outlined in "Section 8.1 - Code of Practice for The Governance of State Bodies"[1] (which require that each State Body develop a Risk Management Policy and the Board approve the risk management framework and monitor its effectiveness), the Heritage Council ('the Council') has implemented a defined and structured process by which risks are identified, assessed, managed and controlled.

The scope of this policy is to establish a framework to identify potential events that may expose the Council to risk, to control and manage this risk within the Council's risk appetite, and to provide reasonable assurance regarding the achievement of the Council's objectives.

1.2 Policy Scope (Personnel Affected)

All personnel (both staff and Board members) at the Council have a responsibility to engage in good risk management practices and contribute to the identification, management and reporting of risks, risk events and known/potential control deficiencies. Further, all personnel are expected to actively anticipate and manage risks and take advantage of opportunities within defined risk appetites. The external and internal risks being faced by the Council are changing constantly and personnel are expected to proactively:

- Utilise experience through knowledge sharing;
- Deal with ambiguity, uncertainty and increasing complexity;
- Prioritise, make decisions and implement solutions on a timely basis;
- Recognise and act on opportunities as they occur;
- Participate in achievement of organisational objectives despite a changing environment.

1.3 Guiding Principles and Objectives

The Council's Vision for Risk Management:

The Heritage Council seeks to adopt best practice in the identification, assessment and control of risks to ensure that they are eliminated or reduced to a level acceptable to the Board in the achievement of its objectives.

The following six guiding principles and objectives outline the Council's approach to risk management in-order to achieve this vision:

i. All members of the Council (staff and Board members) have a responsibility to contribute to the ongoing management, identification and minimisation of risk

ii. Risks are recorded, assessed and reported upon in a consistent and transparent manner

iii. Risks are managed in line with the Risk Appetite Statement (and where this is unknown or unclear, personnel should seek clarity from their direct manager)

iv. Risk events and near misses are reported and investigated promptly and in an appropriate manner

[1] CODE OF PRACTICE FOR THE GOVERNANCE OF STATE BODIES 2016

v. Consideration of risk should inform all decision making (including development of operational plans)

vi. Where preventative or remediation action is required, management will respond promptly and proactively selecting the risk treatment that best meets the needs of the organisation

1.4 Policy Owner

The Board has overall responsibility for risk management within the Council including approving changes to Risk Management policies and procedures. Executive management of the Council is responsible for development and implementation of Council' risk management approach and policy.

Enquiries about this policy or other related risk management issues should be directed to the following:

Michael O'Brien Head of Business Services	Chief Risk Officer	mobrien@heritagecouncil.ie

1.5 Key Terminology

TERM	DEFINITION
Risk	An event (that may or may not occur) that has the potential to affect the Council's ability to achieve its strategic objectives. Note(s): • Risks are characterised by uncertainty or a lack of information, which may relate to the nature of the event itself or its likelihood or impact. • ISO31000:2009 Risk Management Standard extends the definition of risk to also include potential events that could have a positive impact on the achievement of strategic objectives. (the Council defines these events as opportunities which are managed on a case by case business within the business and not reported via the Risk Register)
Risk Management	A process which has been designed to identify potential events that might mitigate against the Council's ability to achieve the policy objectives in its Strategic Plan. The process seeks to control these risks in order to provide reasonable assurance regarding the achievement of the Council's objectives.
Risk Policy	The Council's position with regard to the standards for identification, assessment, tolerance, mitigation, monitoring and reporting of risk.
Risk Identification	The process of determining what risks might happen and under what circumstances they may occur. This involves ongoing scanning of the Council's internal and external operating environment to identify new and emerging organisational, legislative, financial, technological and other factors that could impact the organisation's ability to achieve its strategic objectives.
Risk Assessment	Categorisation of risks (based on Likelihood and Impact) to assist management with prioritising risk remediation and monitoring activities, and determine which risks require Senior Management and Board input and/or intervention.
Impact	A measure of the damage/harm arising from the adverse consequence suffered by the organisation in the event a risk occurs (i.e. a risk event). The Impact of Risks is measured on a scale of 1 – 5 (see Methodology)
Likelihood	A measure of the degree of possibility of a risk occurring in an organisation taking into account the strengths and weaknesses of the organisation's controls, and known instances where the risk has occurred. The Likelihood of Risks is measured on a scale of 1-5 (see Methodology).
Risk Appetite	Level of risk that the Board of the Council is prepared to accept in order for the organisation to achieve its strategic objectives.
Risk Event	The occurrence of a known (or unforeseen) risk. Note(s): • A risk event may occur due to a breakdown in the controls framework or some other unforeseen factor. • Risk events must be reported upon and investigated as per the Council's requirements (which may vary depending upon the nature and materiality of the risk event.) • Events assessed to have the potential to re-occur again in the future, or whose likelihood of reoccurring is unclear, should be communicated to the Council's risk function for inclusion in the Risk Register (if not already included in the register).

TERM	DEFINITION
Controls	Checks and safeguards in place to reduce the Likelihood or Impact of a risk to an acceptable level (e.g. Segregation of Duties, Physical limitations on access, Passwords, authority limits, approvals etc.) Note(s): • Controls may be automated (e.g. System enforced authority levels) or Manual (e.g. Supervisor review)
Inherent Risk	(Also referred to as "raw" risk). Level of risk to an entity in the absence of any controls or management actions to alter a risks Likelihood and/or Impact.
Residual Risk	Risk that remains after management's response (including controls) have been applied to reduce the Likelihood and or Impact of a risk. Within the Council, risk ratings (and other risk related communications and discussions) are based on Residual Risk. Note(s): • In situations where residual risk is not being used, this should be clearly identified and communicated to stakeholders.
Risk Register	List of known risks and associated information (normally maintained in spreadsheet format.). The Council tracks details of all key risks in the Risk Register which is maintained on an ongoing basis by the Chief Risk Officer. In situations where functional areas or projects are maintaining their own risk register, a protocol should be agreed with the Chief Risk Officer regarding the communication and escalation of risks to ensure adequate visibility is provided to Senior Management and the Board.

2. Risk Management Methodology

2.1 Overview

Risk management is an umbrella discipline that cuts across all areas of activity within an organisation, reflecting the fact that risks permeate across all activities and lines of services. To be effective, risk assessment has to be integrated into the organisational planning and budgeting processes, to provide timely and relevant risk information to management. This is a continuous process owned by the organisation and embedded within the operational cycle, starting with risk identification as part of the strategic planning process, carrying through to operational processes and execution, and ending in evaluation. The Council seeks to apply best practice principles in risk management as outlined in the Code of Practice for the Governance of State Bodies (2016) and ISO 31000: 2009.

The risk management process consists of the following steps:

- Risk Identification
- Risk Assessment
- Risk Treatment, including the identification of suitable controls and ongoing monitoring
- Risk Reporting
- Reviewing the Risk Management Framework

2.2 Risk Identification

Risks affect all aspects of organisational activity. Documenting risks (in the form of a register) provides a framework for functional areas and projects to track and assess the organisation's exposure to risk. The risk identification process is carried out annually.

The Risk Register submitted for approval to the Council's Audit & Risk Committee and the Board is a combination of new and emerging risks derived from input received from the Senior Management Team (Heads of Department) and Professional Officers, and various other stakeholders involved in the annual planning and budgeting processes as well as risks flagged in previous years. Managers assess their key operational objectives and then undertake a process to determine an event (that may or may not occur) that has the potential to affect the Council's ability to achieve its strategic objectives.

The Risk Register captures the key organisational risks. There are a number of channels available to assist with the identification of risks including (but not limited to):

- ongoing scanning of internal and external environments
- group workshops
- annual planning and budgeting events
- international standards and recognised frameworks (e.g. ISO 31000[2] & COSO[3])
- professional association publications
- known incidents and near misses
- process flowcharts and risk control matrix

---

[2] ISO 31000:2009 The Irish Standard for Risk Management – Principles and Guidelines

[3] The **Committee of Sponsoring Organizations of the Treadway Commission** (**COSO**) is a voluntary private-sector organization, established in the United States, dedicated to providing thought leadership to executive management and governance entities on critical aspects of organizational governance, business ethics, internal control, enterprise risk management, fraud, and financial reporting. COSO has established a common internal control model against which companies and organizations may assess their control systems.

Descriptions of risks should be kept to a single sentence and should be clear, comprehensible and unambiguous. All risks should be allocated a Risk Owner(s). Descriptions should (1) identify an event or set of circumstances (that may or may not occur) and (2) the impact this may have on the ability of the organisation to achieve its corporate and strategic objectives.

2.2.1 Risk Categories

To facilitate the capturing and reporting of risks in a consistent manner the following categories of risks have been identified:

RISK CATEGORY	DESCRIPTION
Strategic	Those risks associated with failure to achieve the strategic and organisational objectives
Reputation	Risks that may have a significant impact on the reputation of the Council.
Organisation and Management	Risks relating to the governance and management of the Council, including organisational structure and functions.
Financial	Risk of failure to maintain effective financial management and accountability arrangements in all activities
Operational	Those risks arising from people, processes and systems involved in the Council's day to day activities
Legal, Regulatory and Compliance	Risks relating to compliance with statutory/ legal obligations.
External	External factors and parties affecting the Council.

2.2.2 Employee's role in risk identification

The Council encourages a risk culture where individual accountability is encouraged. This means that each employee is empowered to be open and fact-based in discussing issues, making all relevant facts and information available so the organisation can assess the risks associated to the conditions identified by employees. Each employee is accountable for raising and escalating concerns to management about issues that may cause risk or create opportunity.

To ensure that Council's risk register remains up to date, bi-annual risk discussions will be held by Senior Management, which captures current feedback on risk and control. Internal and external events affecting the ability to achieve set objectives are identified and discussed. Based on this feedback, the risk register is updated to reflect the most up to date risk identification and assessment. Risk update and identification is an agenda item in the Senior Management, Audit & Risk Committee and Board meetings.

2.2.3 Procedure for adding, changing or removing risks from the corporate level risk register

On a bi-annual basis, the rationale for new risks, changes to risk profiles or the removal of risks will be documented as part of senior management discussions. Such rationale will also be used to inform the subsequent bi-annual reporting of the Risk Register to the Audit & Risk Committee and the Board.

2.3 Risk Assessment

To assist with determining the level of risk associated with each item in the Risk Register, and to enable management to prioritise remediation and corrective actions, risks are assessed based on their Likelihood (probability of the risk occurring) and Impact (harm to the organisation if it does occur) using the following 5-point scale for each (with 1 = Low and 5 = High).

2.3.1 Standard Likelihood & Impact 5 Point Scoring Scale

SCALE	LIKELIHOOD	IMPACT
5	Almost bound to happen/already happening (expected within 2 months)	Catastrophic, extremely detrimental (e.g. major compliance breach, loss of licence, loss of profit for the year)
4	Very likely, will occur in most circumstances (within next 12 months)	Very significant with significant damage (e.g. event failure, compliance breach, inadequate operational recovery in a timely basis)
3	Likely, may occur (within 1-5 years)	Significant but containable (e.g. control breakdown resulting in material costs, diminished service or relationships)
2	Unlikely, may occur at some point (within 5-10 years)	Minor significance, with minor impact (e.g. operational error, claim pay-out at limited level, staff turnover)
1	Rare, never happen, may occur in exceptional circumstances (not expected in next 10 years)	Insignificant, no significant impact (e.g. customer service issue, embarrassment with stakeholders, minor control failure)

Please note:

- Unless otherwise indicated, all risk assessments performed within the Council are based on Residual Risk (i.e. taking into account the impact of existing controls.)
- Risk Owners are encouraged to document key controls linked to the risk to assist with evaluating the effectiveness of controls design and inform those scoring the risk.
- Known risk events and near misses should be communicated to those scoring a risk to assist in their evaluation.
- Where more than one person is scoring a risk (e.g. during a workshop), the average of the Likelihood and Impact scores should be used. Participating individuals should be requested to abstain from scoring risks on subject areas with which they are unfamiliar.

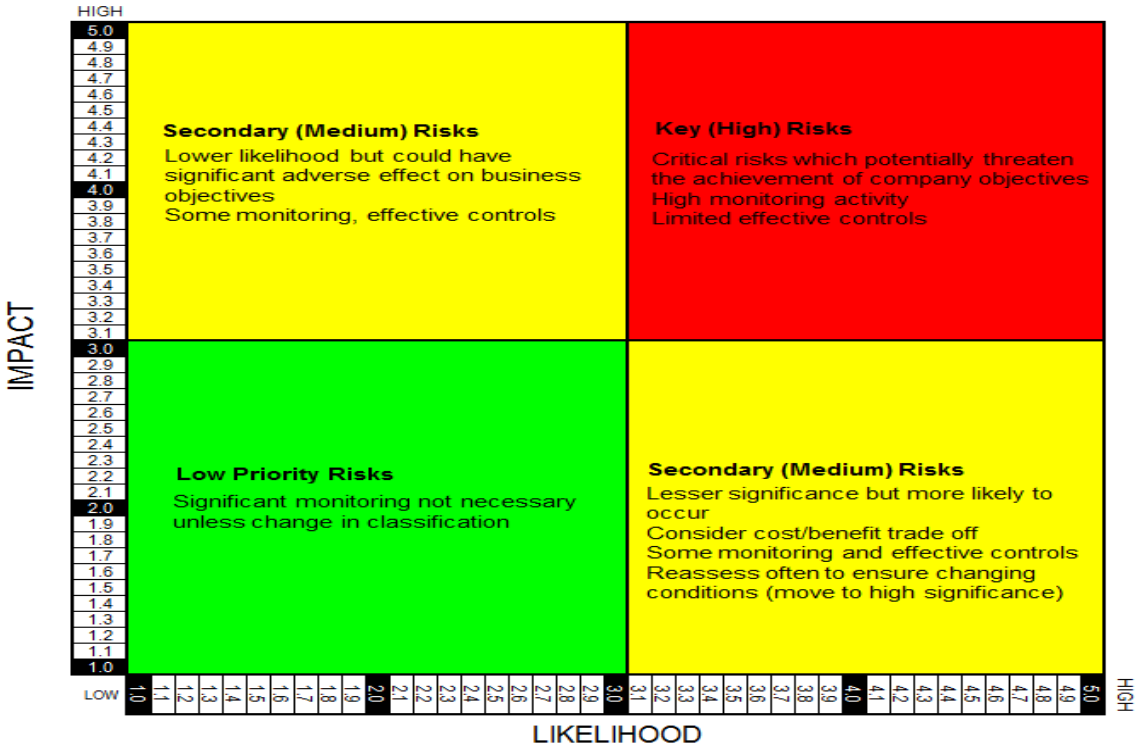
2.3.2 Risk Rating

the Council uses a three-point rating scale (High, Medium & Low) to categorise risks (based on Likelihood and Impact) to assist management with prioritising risk remediation and monitoring activities, and determine which risks require Senior Management and Board input and/or intervention. A risk's rating is determined by plotting its Likelihood and Impact against a pre-defined matrix and is categorised as follows:

- High (also referred to as “Key risks”) – critical risks that threaten the achievement of the Council’s strategic objectives. (High impact with limited effective controls to reduce its likelihood).
- Medium (also referred to as “Secondary risks) – Risks that can have a significant adverse effect on the organisation. (Either a high Likelihood or Impact score creating a scenario whereby they may be unlikely to occur but have a high impact or vice versa).
- Low – actions required typically focus on maintaining the current controls and monitoring to determine if a change in classification

Unless otherwise directed by the Board, the following matrix should be utilised to determine the risk rating.

Risk Rating Matrix



2.4 Risk Treatment

Once a risk rating has been determined the Risk Owner should, in consultation with Senior Management and affected department(s), agree what risk treatment approach will be taken.

Approaches to modifying risk levels can be grouped into four main categories (or "Treatments"):

- Avoidance (eliminate, withdraw from or not become involved)
- Reduction (implement additional or enhanced mitigating controls)
- Sharing (transfer the risk via outsourcing or insurance)
- Retention (accept the risk at its current level and budget for potential events)

Please note:

- Owners of risks listed in the Risk Register are required to provide the Chief Risk Officer with periodic updates to enable tracking of remediation activities to completion.

2.5 Ongoing Monitoring

To be effective, Risk Management must be treated as an ongoing process and integrated into key operational, budgeting and planning activities. Managers and Risk Owners are responsible for monitoring their respective areas and internal/external environments for the emergence of new risks, or factors that may change the Likelihood or Impact of existing risks.

Changes to risks that are tracked via the Risk Register should be reported to the Chief Risk Officer at least bi-annually.

2.5.1 Risk Register Reviews

The full Risk Register should be reviewed and updated by Senior Management bi-annually. Key steps when reviewing the register include:

- Assess risks in the register including how they were identified, monitored and managed
- Consider any new risks proposed for addition to the risk register, including associated controls
- Determine if there are risks which are no longer relevant (and can be "removed" from the register upon proposal by the relevant risk owner)
- Determine progress against previously agreed activities
- Develop and agree remediation activities and consider whether control strategies need to be changed

Risk Owners are requested to review the Risk Register, provide the key controls in place and note any mitigating actions required including the action owner and expected completion date.

An update of the Risk Register is then communicated to the Audit & Risk Committee on a bi-annual basis to review all key risks to determine if corrective action is required and assess progress against agreed upon remediation activities.

The risk register is also subject to bi-annual review and approval by the Board.

2.6 Risk Reporting

Risk reporting is fundamental to risk management. Reporting provides assurances to management and the Board that risks are being regularly reviewed, effectively managed and helps in creating a risk aware culture. Reporting will include:

- Risk as a standing agenda items for Senior Management, the Audit & Risk Committee and the Board;

- Bi-annual update of the Risk Register by Senior Management in conjunction with the Chief Risk Officer;
- B-annual reporting of the Risk Register to the Audit & Risk Committee and the Board;
- Reporting of material risk events (when they occur) to Senior Management, the Audit & Risk Committee and the Board;
- Annual review of the Risk Management Policy by Senior Management, the Audit & Risk Committee and the Board.

3 Risk Appetite

3.1 Risk Appetite Framework

Risk Appetite is the amount of risk that an organisation is prepared to accept, tolerate, or be exposed to at any point in time.

The Board of the Council is responsible for setting the tone for risk management throughout the organisation by clearly articulating and communicating its tolerance for risk ("Risk Appetite") on an ongoing basis. Management and the Audit & Risk Committee are in turn responsible for ensuring the Council operates in a manner that is consistent with the Board's Risk Appetite (and seeking clarification if this is unclear).

The following definitions of risk appetites are applicable for the Council:

Averse	**Avoidance** of risk and uncertainty is a key organisational objective.
Minimalist	Preference for **ultra-safe** organisational delivery options that have a low degree of inherent risk and/or only have the potential for limited reward.
Cautious	Preference for **safe** delivery options that have a low degree of inherent risk and/or may only provide the potential for limited reward.
Open	Willing to consider all potential delivery options and choose the one that is **most likely to result in successful delivery** while also providing an acceptable level of reward.
Hungry	**Eager to be innovative** and to choose options offering potentially higher organisational rewards, including accepting the possibility of financial loss without any guarantee of return on investment

3.2 Overall risk appetite

The Council's role and objectives has a range of inherent risks associated with it. The Council is currently taking an averse to cautious approach to most risks of a strategic, reputational, organisation and management, financial, operational, legal, regulatory and compliance and external nature. The Council is not willing to consider or choose options or opportunities that will result in increased levels of risk being accepted which may result in financial, reputation or other exposure to Council's objectives and activities.

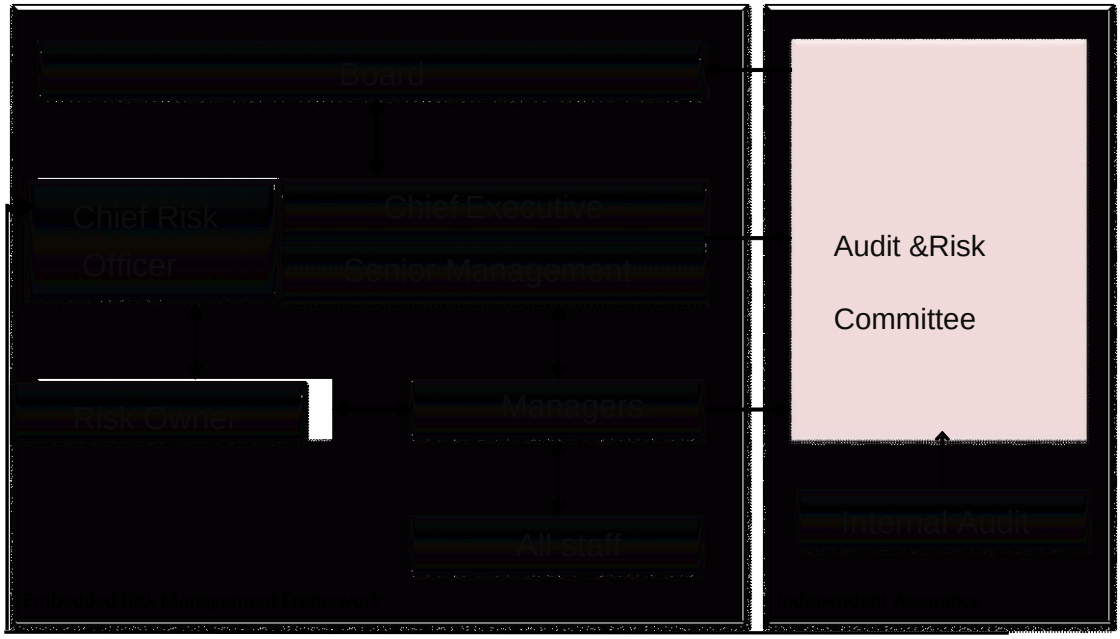
3.3 Changes and Variations to Risk Appetite

At the Board's discretion, the risk appetite can be changed or modified to reflect the changing needs of the organisation. In addition, the Board may elect to set individual risk appetites

(pertaining to a specific activity, functional area, type of risk, impact, client or other criteria) or set appetites based on performance or quantitative metrics to allow for greater flexibility in the management of risk, or ensure sensitive issues are appropriately escalated.

4. Risk Management Governance Structure

4.1 Conceptual Overview



4.2 Internal Control Environment

The primary objectives of the internal control system within the Council are:

- To ensure compliance with applicable policies, procedures, laws, regulations and processes
- Delegation of responsibilities to ensure controls are appropriately managed
- To promote effective and efficient use of resources and operations.

To support the internal control objectives the control environment consists of policies, procedures, authority limits, approval processes and other system and manual controls utilised by the Council to reduce the likelihood and/or impact of a risk to an acceptable level.

4.3 Key Roles and Responsibilities

ROLE	RESPONSIBILITIES
Board	Responsibility for the Council's operations is vested in the Board. The Board has overall responsibility for Risk management including: • The design and operational effectiveness of the Council's Risk management and internal control frameworks • Approve the RM policy, set risk appetite, and approve the RM plan and risk register at least annually; • Receives and considers reports from the Audit & Committee on the effectiveness of the systems of Risk Management. • Establishing an Audit & Risk Committee to give an independent view in relation to risks and risk management systems • Making risk management a standing item on the Board meeting agenda • Advising the relevant Minister of the need to include the RM experience in the competencies of at least one Board member. Where composition of the Board does not allow for this, expert advice should be sought externally; • Appoint a CRO or empower a suitable management alternative, and provide for a direct reporting line to the Board to identify, measure and manage risk and promote a risk management culture in the organisation; • Require external review of effectiveness of RM framework on a periodic basis; • Confirm in the annual report that the Board has carried out an assessment of the Council's principal risks, including a description of these risks, where appropriate, associated mitigation measures or strategies.
Audit & Risk Committee	Responsibility for reviewing the effectiveness of the system of internal control is vested in the Audit & Risk Committee (a sub-committee of the Board). On a periodic basis, the Audit & Risk Committee will review the Risk Register and form an independent view of the risks identified, the likelihood of their occurrence, the potential impact and the adequacy of steps taken to manage them. On an annual basis, the Audit & Risk Committee will report to Board an opinion, based on its review, on the effectiveness of operation of the risk assessment process and management of the risks including the effectiveness of the key controls.
Chief Executive	The Chief Executive is responsible for managing and controlling the operations and administration of the Council, together with such other functions as may be determined by the Board. The Chief Executive is responsible for: • advising the Board on emerging and existing risks that may impact the Council's ability to achieve its strategic objectives ensuring adequate reporting and monitoring mechanisms exist to track risks • ensuring risk events are appropriately investigated and reported.
Senior Management	Senior Management is responsible for co-ordinating the planning, budgeting, allocating resources and overseeing the achievement of the targets set out in the Strategic and Operational Plans. Senior Management fulfils the role of "Risk Sponsor" within the Council and is responsible for: • Promoting Risk Management within the Council and ensuring that it receives appropriate priority and resourcing • The ongoing identification and evaluation of risks that might have an impact on the Council's ability to achieve its Strategic or Operational plans and objectives

ROLE	RESPONSIBILITIES
	• Ensuring that Risk Management is effectively embedded in the Council's planning and operational processes • Promoting and monitoring compliance with approved risk management policies and procedures • Providing a framework for risk event reporting and escalation
Chief Risk Officer	The CRO will co-ordinate the operations of the Council's Risk Management function with responsibility for: • Ownership of the Risk Management policy document including collating and presenting proposed changes to it for the Board's consideration • Promotion of best practice in Risk Management within the Council • Collating risks submitted by management for inclusion in the Risk Register • Co-ordinating risk workshops and discussions as necessary • Monitoring the implementation of risk management systems and actions • Providing advice and guidance to risk owners and management • Critically reviewing the effectiveness of strategies implemented • Reporting to Senior Management, the Audit &Risk Committee and the Board on the operation of risk management processes and procedures.
Managers	All members of the broader Manager group are responsible for the risk management process in their respective areas including: • Ensuring personnel in their area: ○ are aware of the importance of risk management and adhering to approved risk management policies and procedures ○ are aware of how to report new and changing risks ○ are aware of how to escalate a risk if required ○ report risk events and near misses as required • Ongoing identification and evaluation of new and emerging risks • Ongoing monitoring of existing risks (including changes to the Council's internal or external operating environment that may affect the rating of existing risks) • Implementing agreed upon remediation actions arising from the Risk Management Process • Reporting and escalating risk events in-line with the framework communicated by Senior Management
Risk Owners	All risks rated Medium or High in the Risk Register should have a nominated "owner", who is responsible for: • ongoing oversight of monitoring and remediation activities related to that specific risk • making themselves aware of risk events and near misses related to that risk (and co-ordinating the tracking and management response to these) • identifying key controls that mitigate the Likelihood or Impact of that risk • providing advice to Senior Management (or other relevant stakeholders) on potential control remediation or improvement options • providing periodic updates to the CRO on agreed risk action and remediation items • briefing personnel involved in the evaluation of that risk
Internal Audit	• Internal Audit will periodically audit and report on the effectiveness of the risk management process as part of the ongoing Audit Plan.

ROLE	RESPONSIBILITIES
	• Internal Audit may provide technical guidance within this area. • Internal Audit will consider the Risk Register as part of its annual planning process.
All staff	All personnel at the Council have a responsibility to engage in good risk management practices and contribute to the identification, management and reporting of risks, risk events and known/potential control deficiencies.

Appendix A – Sample Risk Register Template (minimum content)

No.	Risk Category	Department	Risk	Raw Risk Ranking			Risk Owner	Controls	Residual Risk Ranking			Actions Required	Action Owner	Deadline for actions
				Impact	Likelihood	Score			Impact	Likelihood	Score			