Fermanagh & Omagh
District Council
Comhairle Ceantair
Fhear Manach agus na hÓmaí

Risk Management Policy

Updated April 2026

Contents

1. Introduction

Risk management enhances the Council's strategic planning and prioritisation, assists in achieving objectives and strengthens the ability to be agile to respond to the challenges faced. To meet objectives successfully, improve service delivery and achieve value for money, risk management must be an essential and integral part of planning and decision-making.[1] .

Fermanagh and Omagh District Council recognises its responsibility to manage risks effectively to demonstrate its commitment to excellent governance, whilst understanding that risk can never be fully eliminated. The Council is committed to the proactive management of key external and internal risks.

It is important that everyone working for the Council have a clear understanding of how risk management is applied, and that the process of risk management is consistent, appropriate and embedded within all of the organisation's activities.

In this document, Fermanagh and Omagh District Council details how the Council meets the statutory duty requirement of Part 2 of the Local Government Accounts and Audit (Amendment) Regulations (Northern Ireland 2015) 4(1)(b). A local government body is responsible for ensuring that it has a sound system of internal control which facilitates the effective exercise of its functions, and which includes arrangements for the management of risk. The Council draws on the approach set out in 'The Orange Book, Management of Risk – Principles and Concepts,' revised by HM Treasury in 2023 .

Fermanagh and Omagh District Council's Corporate Plan Our Council Our Plan 2024-2028 sets out the Council's Vision, Mission, Values and Goals. Of our four priorities, Priority 4 is One Council: Ensure an efficient, effective and agile Council founded on good governance practices. A core objective of this priority is 'Strong Governance.' To ensure this, we will 'Manage a transparent and effectively governed Council that is responsible to our citizens, while also maintaining strong financial discipline to ensure that we operate within our budgetary limits'.

This Risk Management Policy supports this, along with other plans and strategies.

[1] HM Government (2023) The Orange Book – Management of Risks Principles and Concepts

2. Risk Strategy

The Council's overarching strategy for the management of risk is set out below:

3. Risk Management Framework

The Council's approach is to adopt a risk management framework, which supports the consistent and robust identification and management of opportunities and risks within desired levels across an organisation. The framework supports openness, challenge, innovation and excellence in the achievement of the Corporate Plan objectives.

For the risk management framework to be considered effective, the following principles, in line with HM Treasury guidance, shall be applied:

A: Risk management shall be an essential part of governance and leadership, and fundamental to how the organisation is directed, managed and controlled at all levels.

B: Risk management shall be an integral part of all organisational activities to support decision-making in achieving objectives.

C: Risk management shall be collaborative and informed by the best available information and expertise.

D: Risk management processes shall be structured to include:

- risk identification and assessment to determine and prioritise how the risks should be managed;
- selection, design and implementation of risk treatment options that support achievement of intended outcomes and manage risks to an acceptable level;
- design and operation of integrated, insightful and informative risk monitoring; and

- timely, accurate and useful risk reporting to enhance the quality of decision-making and to support management and oversight bodies in meeting their responsibilities.

E: Risk management shall be continually improved through learning and experience, including learning from 'near misses,' that is, events that did not involve injury or ill-health but reasonably could have under different circumstances[2]. Events might also include those that result in significant financial losses and/or reputational damage.

4. Risk Governance

Risk management is an essential part of the governance and leadership of the Council and fundamental to how the Council is directed, managed and controlled at all levels. Behaviour and culture significantly influence all aspects of risk management at each level and stage and to support the appropriate risk culture, the Corporate Leadership Team ensures that expected values and behaviours are communicated and embedded at all levels.

The Chief Executive and Corporate Leadership Team (CLT) have responsibility to ensure that roles and responsibilities for risk management are clear, to support effective governance and decision-making at each level with appropriate escalation, aggregation and delegation. CLT determine and continuously assess the nature and extent of the principal risks that the Council is exposed to and is willing to take to achieve its objectives and ensure that planning and decision-making reflects this assessment. CLT is responsible for reviewing the internal and external corporate risk registers, respective directorate risk registers and for identifying deep dives into specific risks.

The Internal Auditor is responsible for evaluating and improving the effectiveness of risk management, for regular independent reviews of systems for risk management and compliance and for identifying deep dives into specific risks.

The Audit Panel has responsibility to provide independent assurance of the risk management framework and the associated control environment to the Council. The Audit Panel considers the effectiveness of the Council's risk management arrangements, monitors the quality of the risk information received and ensures that it is sufficient to allow effective decision-making. Risk registers are reported to the Audit Panel twice a year.

The Director of Corporate Services and Governance is responsible for development of the Risk Management Policy. The aim of the Risk Management Policy is to establish and operate appropriate risk management procedures and to promote an organisational culture which ensures that risk management is an integral part of every activity

[2] Health and safety keywords | IOSH

5. Aim & Objectives

The aim of the Risk Management Policy is to establish and operate appropriate risk management procedures and to promote an organisational culture which ensures that risk management is an integral part of every activity.

The policy also seeks to embed good practice guidance by developing and updating a Risk Appetite Statement. This complements the FODC approach to risk management, as set out in this policy, and will further aid effective decision making in relation to risks. The Risk Appetite Statement is attached in Appendix 1

The objectives of the policy are to:

- Further develop the corporate framework for the proactive identification, analysis, assessment, management and reporting of opportunities and risks;
- Take actions and implement controls to minimise the likelihood of threats occurring and/or reduce the impact of consequences should risks occur;
- Clearly identify and communicate the respective roles, responsibilities, and reporting lines for managing risk;
- Continually develop the Corporate Risk Register to facilitate risk administration and reducing duplication between departments in identifying and managing overlapping risks whilst providing opportunities for shared learning across the Council;
- Reinforce the importance of risk management as part of the everyday work of Council employees;
- Incorporate risk management into corporate strategic planning; service & financial planning; policy making; audit and review; performance management and project management processes; and
- Ensure ongoing monitoring and reporting arrangements to all levels.

6. What is Risk?

Risk is the effect of uncertainty on objectives. Risk is usually expressed in terms of causes, potential events, and their consequences [1].

Risk Management is the co-ordinated activities designed and operated to manage risk and exercise internal control within an organisation[1].

7. Why do we manage Risk?

While risk practices have improved over time across the public sector, the volatility, complexity, and ambiguity of our operating environment have increased, as have demands for greater transparency and accountability for managing the impact of risks[1]. Effective risk management therefore: -

Leads to improvements in Strategic Management:

- More informed selection of strategic objectives and associated targets as a result of risk identification and analysis;

- Improved decision making; and
- Enhanced ability to deliver against objectives by improving understanding of background issues.

Leads to improved Operational and Financial Management:

- Better informed financial decision making on budgeting, investment, insurance, and option appraisal;
- Reduction in management time associated in dealing with unforeseen risks; and
- Reduced likelihood of interruptions to service delivery.

8. Roles and Responsibilities

Clear ownership and accountability for risks is essential to an effective risk management process. To manage risk effectively in the Council, clear roles and responsibilities have been established.

Group or Individual	Role and Responsibilities
Council	• Consider and approve the updated Risk Management Policy • Consider and approve a Risk Appetite Statement every three years
Audit Panel	• Provide independent assurance of the adequacy of the risk management framework and the associated control environment, • Consider the effectiveness of the Council's risk management arrangements • Seek assurance that action has been taken on risk related issues identified by Internal and External Audit • Ensure that the Council's assurance statements, including the Annual Governance Statement properly reflects the risk environment and any actions required to improve it. • Review risk arrangements for Strategic Risk Management and monitor the key corporate risks • Identify deep dives into specific risks
Chief Executive	• The Chief Executive has ultimate Officer responsibility for embedding risk management throughout the Council • Ensure that there is an adequate system of internal control in place by mandating that risk is considered at all Directorate meetings and the process of risk escalation is clear. • Report annually on the system of internal risk management control in the Statement of Accounts and the Annual Governance Statement • Ensure all Directors complete a Directorate Statement of Assurance which includes actions relating to strategic and operational risk, key internal controls and governance.
Corporate Leadership Team (CLT)	• Contribute towards the identification and management of strategic and cross cutting risks and opportunities facing the Council. • Receive and consider reports on key strategic risk issues including as part of the annual statement of assurance and performance reports • Promote the integration of risk management principles into the culture of the Council • Review the Risk Appetite Statement every three years • Consider the Directorate risk registers • Review and update the Corporate risk registers • Identify deep dives into specific risks
Heads of Service	• Identify, analyse, and profile service risks • Provide annual assurance on the effectiveness of controls in place to mitigate/reduce risks within their service • Maintain awareness of and promote the approved risk management policy to all relevant staff • Regularly update and maintain service and project risk profiles • Ensure risks are clearly and accurately identified and scored within reports • Ensure risk management is a regular item on team meetings • Ensure that risk management is incorporated into service plans, business plans and performance management • Participate in deep dives into key risks as required • Ensure compliance with all risk management procedures which are incorporated within corporate procedures and strategies

Director of Corporate Services and Governance	• Develop Risk Management Policy with arrangements for periodic review • Continually improve and update risk management procedures based on current best practice and benchmarking results • Design and implement appropriate risk management training, including presentations and on-line training.
Internal Auditor	• Provide independent review of corporate approach to risk management and compliance • Contribute to the accuracy and integrity of the corporate risk register (as part of the risk-based approach to audit) and in particular relation to the effectiveness of mitigating actions and fraud risk • Identify deep dives into specific risks
All Employees	• Maintain awareness of risks and contribute to the control process where appropriate. • Take due care to ensure compliance with any risk management guidelines and other guidelines provided by the Council or required by regulation. • Immediately inform line management if they suspect that adequate controls for a risk are not in place or not up to date. • Inform line management immediately if they see anyone • carrying out an activity which could be detrimental to the achievement of the Council's goals and objectives. • Inform line management immediately of any mistake or suspected mistake that could potentially cause a significant loss. • Take responsibility to ensure that they are equipped to identify and manage risk adequately.

9. When do we manage Risk?

Risk management should be a daily activity at all levels of the organisation. Risk management should be a recurrent agenda item at team meetings, giving staff the opportunity to raise concerns on a regular and timely basis.

Directorate Risk Registers should be reviewed in March and September. Corporate Risk Registers should be reviewed in April and October.

10. Risk Registers

The Council uses the following risk registers to record information about identified risks:

- Corporate Risk Register – External
- Corporate Risk Register – Internal
- Community and Wellbeing
- Environment and Place
- Regeneration and Planning
- Corporate Services and Governance and Chief Executive's Department

Risk Registers are maintained using Excel spreadsheets which are formatted into 3 sections:

- Risk analysis and scoring
- Risk Map – Current
- Risk Map – Post Control

A risk register template is attached at **Appendix 2**. The risk management process in the following section sets out the risk management process at the four key stages and provides guidance on completing the template.

11. Risk Management Process

Following the guidance on risk management, as set out the HM Government (2023) The Orange Book – Management of Risks Principles and Concepts [1], risk management processes at the Council are structured to include:

- ***Risk Identification***, including an assessment to determine and prioritise how the risks should be managed;
- ***Risk Analysis,*** including the selection, design and implementation of risk treatment options that support achievement of intended outcomes and manage risks to an acceptable level;
- ***Risk Monitoring***, including the design and operation of integrated, insightful, and informative risk monitoring; and
- ***Risk Review***, including timely, accurate and useful risk reporting to enhance the quality of decision-making and to support management and oversight bodies in meeting their responsibilities.

Each of these are set out in more detail below.

11.1 Risk Identification

Every six months, members of the Departmental Risk Management Group**,** or the Corporate Leadership Team in the case of the External and Internal Corporate Risk Registers, are required to review the following sections of the Register for each risk identified and amend as necessary:

Category	Risk Number	Risk Description	Causes

- ***Category***: Risks are classified as follows:
  - *Strategic* – a risk that can affect the delivery of the Council's objectives as defined in the Corporate Plan e.g. Failure to implement or deliver on Corporate Plan priorities and actions
  - *Governance* – risks arising from unclear plans, priorities, authorities, and accountabilities, and/or ineffective or disproportionate oversight of decision-making and/or performance
  - *Financial* – risks associated with the adequacy of financial controls e.g. Failure to

plan, manage, deliver, and review the Capital Programme
- *Environmental* – risks relating to the environmental impact of the Council's service delivery e.g. Failure to meet required Infrastructural Development
- *People* – risks associated with impacts on the employees of the Council or arising from the actions of employees of the Council e.g. Failure to achieve satisfactory level of attendance
- *Technology and Security* – risks associated with potential failures in ICT systems e.g. Loss of Council communication systems
- *Project/Programme* – risks that change programmes and projects are not aligned with strategic priorities and do not successfully and safely deliver requirements and intended benefits to time, cost and quality
- *Safety* – risks that are likely to cause harm, injury, ill-health or loss of life.

- ***Risk Number***: A unique reference is assigned for each risk. This number should not be changed as it is linked to the Critical Risk Maps.

- ***Risk Description***: A short description of the risk should be provided.

- ***Causes***: A list of reasons should be identified which could lead the risk to occur.

11.2 Risk Analysis

Current Controls / Actions		LIKELIHOOD	Finance	Staff	Service	Reputation	IMPACT		RISK SCORE		Accept	Transfer	Mitigate	New Actions	Responsibility	New action implementation date / Review date		LIKELIHOOD	Finance	Staff	Service	Reputation	IMPACT		RISK SCORE

At the review meetings, the following should be updated:-
- **Current Controls/Actions:** Actions that are currently in place to prevent, reduce or control the level of the risk.

To determine the appropriateness of actions to be taken, it is necessary to consider each alternative in relation to the following hierarchy:
- **Risk Avoidance**
  - Can the risk be avoided?
  - Does the action/Department in question have to be undertaken/provided?
  - If yes, what alternative delivery options are available (internal/external)?
  - Is there a more efficient/effective way that avoids the risk is question?

- **Risk Mitigation:** If the risk cannot be eliminated, then can the likelihood/impact be reduced through:
  - Strategy (Policy, Objectives, allocation of responsibilities, lines of accountability, training and supervision, monitoring & auditing)
  - People (Information, instruction, and training, communication and consultation, disciplinary procedures)
  - Processes (Re-structuring, re-allocation of courses, new services, new committees/management teams)
  - Systems (Policies and procedures, written instructions, documented authorisations)

- Once control actions have been developed it is important that they are **SMART:**
  - **S** – Specific
  - **M** – Measurable

- **A** – Achievable
- **R** – Realistic
- **T** – Time effective

- Current Risk Assessment Scoring: To effectively evaluate the identified risks each risk is ranked in terms of its impact and likelihood. The scoring is numerical and should be used to determine the overall total score. When calculating Impact scoring, there are four criteria – financial, staff, service, and reputation. The risks are to be evaluated for all and the scoring detailed for each in the appropriate box. Note that for each of the areas – financial, staff, service and reputation a minimum score is 1 for each, giving a total minimum score for impact of 4 (see scale on heat map).
- The overall risk score is a multiple of the **Likelihood** of the event occurring and the **Impact** that it would have on the organisation should that risk materialise/event occur. The following criteria have been established for defining, evaluating, and reporting of risks on an ongoing basis.

Likelihood

Score	Degree of Likelihood	Definition
4	**Very likely**	This uncertainty is very likely to occur within the next 1 – 12 months or is occurring at the present
3	**Likely**	This uncertainty is likely to occur at least once every 1 to 3 years
2	**Unlikely**	This uncertainty is likely to occur and may do so within the next 3 to 10 years
1	**Extremely unlikely**	This uncertainty is extremely unlikely to occur, but may do so in at least 10 years' time

Impact

Score	Finance	Staff	Service	Reputation
4 Major	Additional expenditure/associated costs of more than 12.5% of service revenue	Major impact on all employees in department.	Complete failure in service standards.	Affects all major stakeholders with long term impact on public memory causing damage to reputation
3 Significant	Additional expenditure/associated costs of between 5 – 12.5% of service revenue	Significant impact on some employees in department	Serious disruption in service standards.	Affects more than one group of stakeholders with widespread medium-term impact on reputation.
2 Moderate	Additional expenditure/ associated costs of between 1.5 – 5% of service revenue	Impact on a number of employees	Moderate fall in service standards.	Affects more than one group of stakeholders but only short-term impact on reputation
1 Low	Additional expenditure/associated costs of less than 1.5% of service revenue	Impacts on 1 employee only	Small fall in service standards.	Affects only one group of stakeholders with minimum impact on performance.

The next step is to consider the overall approach to risk management: **Accept, Transfer or Mitigate.**

- **Accept** – The Risk has been identified and logged on the risk register; however no further action will be taken.

- **Mitigate** – Mitigation (or treating/lessening the risk in some way) is essentially concerned with lessening the impact that a particular risk might have and/or reducing the likelihood of the event happening/risk materialising. The relevant Head(s) of service/Director is assigned risks to manage accordingly and will be responsible for implementing new actions pertaining to each risk within a specified time frame.

- **Transfer** – The impact and management of a risk is transferred to another Directorate/Corporate. If accepted, they are then responsible for managing that risk.

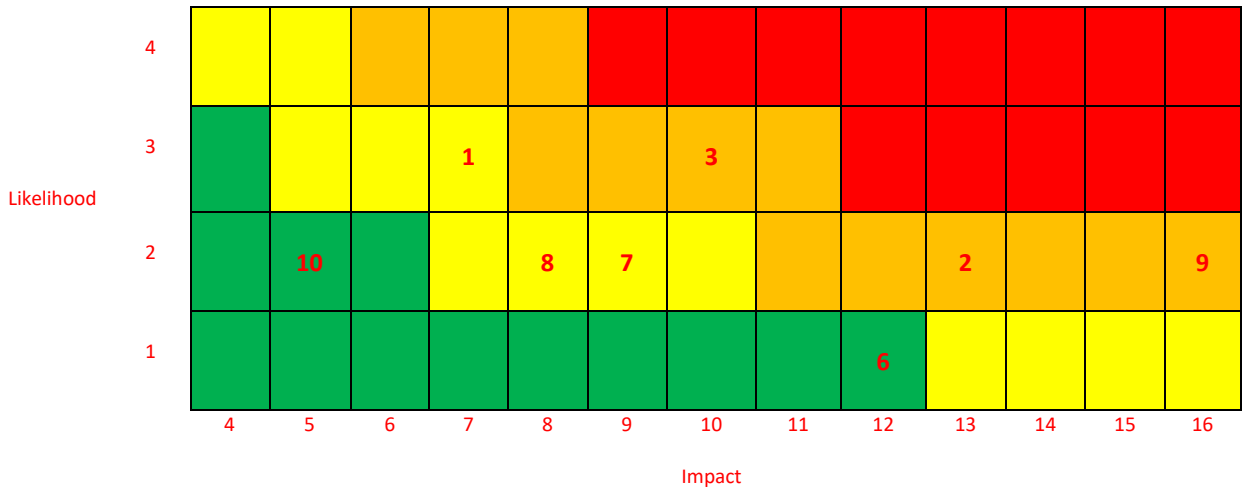
New actions: A set of actions that are to be implemented to resolve, maintain the level, reduce, or transfer the risk are then agreed/updated.

New action implementation date / Review date: Dates must be set for new actions to be carried out or measures put in place to reduce risk. A date needs to be agreed for review if there are no new actions.

Complete Post Control Risk Scoring: The post-control likelihood of the event occurring and the impact it would have should that risk materialise/event occur should be recorded.

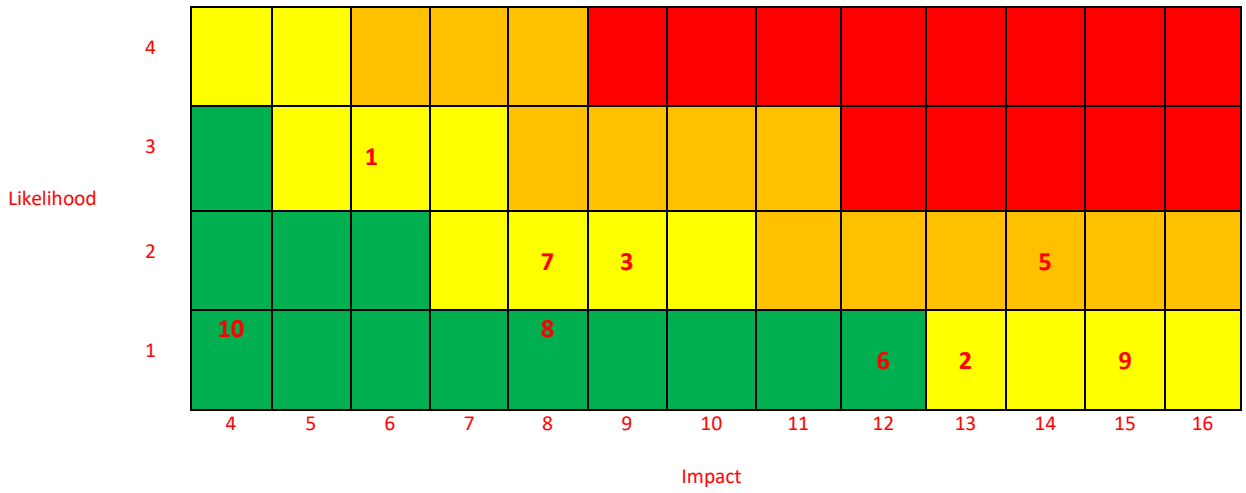
Responsibility: The person/s responsible for managing the Risk need to be included.

Risk Map (or 'Heat Map') – Current: A scatter graph that plots the current risks (number relates to risk number but is scored by impact X likelihood) scores before any agreed new actions have been implemented can then be produced. See example below:



Current risks are plotted within the scatter graph. In the above example, of the 10 risks, there are 2 current risks.

Risk Map – Post Control: A scatter graph that plots the risk score following the implementation of agreed new actions is also added. See example below:



Post control **risks** are plotted within the scatter graph. The 'post-control' score is based on completion/implementation of agreed new actions. In the above example the number of critical risks reduced from 2 to 1, with risk number 4 being critical (red). All other risks incurred a reduced score and were moved on the heat map accordingly.

Reference should then be made to the category of all risks, and the Risk Appetite Statement. Here, the level of appetite for the category will be classified. An assessment can then be made whether the level of each risk is within a tolerable level or not, and further actions may need to be considered in order to manage the risk down. For example, if risk number was a financial risk where the risk appetite for financial risk was AVERSE, then risk 5 would also remain critical and additional actions considered to manage it to a tolerable level.

11.3 Risk Reporting

Complete Summary of Changes Report (Appendix 3). Any changes that are made to a Risk Register must be recorded on a 'Summary of Changes' Report. This includes adding new risks, merging/amending existing risks or transferring risk.

Complete Directorate Risk Management Report (Appendix 4). Any changes should be briefly summarised in the Risk Management Report and signed off by the relevant Director. Any **Risk Escalation Report** should also be attached **(Appendix 5)**.

Centralising Risk Management. Directorates should forward the Risk Register to Corporate and Strategic Services**.** This will include the Risk Maps which will be reviewed by SMT together with the list of Post Control Critical Risks and the plans to deal with them.

11.4 Monitoring and Review

Registers

Directors are required to review their Directorate Risk Register, in conjunction with the Directorate Risk Management Group, which is aligned to the Directorate's objectives and, where appropriate, the corporate risks are cascaded down with more detailed actions relevant to the Directorate or service area.

It is imperative that the Risk Register reflects the objectives contained in the Directorate Plans and Performance Improvement Plan, linked to the objectives within the Corporate Plan, so that operational objectives are achieved. New objectives set should be reflected in the risk management process so that the Council/Directorate can change and evolve to achieve its objectives. **The Directorate Risk Registers are reviewed in March and September.**

The **Corporate Risk Registers (Internal & External) are reviewed by CLT in April and October**, following the review of the Directorate Risk Registers, and any risk escalation requests are considered. The Corporate Risk Registers only contain risks which are deemed to have a significant impact on the achievement of the Council's corporate objectives. How each risk is managed and what additional actions are required are identified and assigned to a CLT member.

The Audit Panel reviews the effectiveness of the Council's Risk Registers and Risk Management processes on a bi-annual basis.

Deep Dives

Principal risks should be subject to "deep dive" reviews by the board and/or Audit and Risk Assurance Committee, with those responsible for the management of risks and with appropriate expertise present at an appropriate frequency depending on the nature of the risk and the performance reported.[1]

A risk 'deep dive' is a detailed, in-depth analysis of a specific risk to understand its root causes, impacts, and current management strategies. It goes beyond surface-level reviews to thoroughly examine all contributing factors, assess the effectiveness of existing controls, and identify any missed assumptions or areas for improvement. The goal is to gain a complete and confident understanding of how to manage the risk effectively.

The Policy

The Risk Management Policy will, under normal circumstances, be formally reviewed every three years. From time to time, updates and re-issues may be circulated.

The Policy will be reviewed sooner in the event of any one or more of the following:

- A failure or weakness in the policy is highlighted.
- Changes in legislative requirements.
- Changes in Government/Council or other directives and requirements.

Appendix 1

Risk Appetite Statement

SUMMARY STATEMENT

Fermanagh and Omagh District Council takes a balanced approach to risk taking in order to deliver its corporate priorities and agreed outcomes for the District. The Council recognises that, in pursuit of its priorities and outcomes, it may choose to accept different levels of risk in different areas. We have established and articulated risk appetites for different categories of risk. The Council will therefore take action to manage risks down to a level which falls within the agreed risk appetite for that category. For risks which are People and Project Management related, we adopt an open approach. For risks which fall into the categories of Strategic, Governance, Financial, Technology/Security and Environment, we adopt a cautious approach. We have a zero tolerance towards all fraud and financial impropriety and our systems eliminate risk accordingly. In consideration of safety we are averse to any risks and have zero appetite for any decisions or actions which puts the safety of people at risk.

FULL STATEMENT

Strategic risks. We have adopted a cautious approach to strategic risks, with a preference for considered risk taking in organisational actions and the pursuit of priorities. The Corporate Plan is refreshed every four years and the Community Plan every 10 years.

Governance risks. We have adopted a cautious approach to all governance risks, including those that are legal, compliance-related, impact business continuity and create reputational risk. Our processes, and oversight/monitoring arrangements enable cautious risk taking within a framework of assurances required for statutory purposes or when incident management is required. Internal controls enable fraud prevention and provide high levels of assurance, detection and deterrence by maintaining appropriate controls and sanctions.

- In terms of legal risks, we are cautious about entering into any challenge without sound evidence before proceeding.
- As a public body, our appetite for risk taking is limited to those events where there is no chance of any significant reputational repercussion for the Council.
- Our aim always to deliver high quality, cost-effective services to the public. On this basis, we also invest in business continuity and emergency planning, with partners regionally and nationally.

Financial risks: We have adopted a cautious stance for financial risks with reference to core running costs and seek safe delivery options with little residual risk. The Council receives ongoing assurance through the Annual Governance Statement that the necessary policies and procedures are in place in line with our statutory duties and the requirements of the Department of Finance and NI Audit Office. Our financial decisions are rightly heavily scrutinised, with value for money being a key factor in decision making. We accept risks that may result in some small-scale financial loss or exposure on the basis that these can be expected to balance out but do not accept financial risks that could result in significant reprioritisation of budgets. We are averse to any form of financial impropriety and have a zero tolerance to fraud and corruption.

People: We have an open approach to how we manage our People and the culture we create to take decisions and managing risks. We are prepared to invest in our people, and recruit and

train to ensure the innovative mix of skills which are needed to deliver the range of Council services. Decision making is devolved to staff at the right level.

Technology and security. We have a cautious approach to technology and security risk. Consideration is given to adoption of established/ mature systems and technology improvements, which are more likely to present value for money. Limited security risks are accepted to support business need, with appropriate checks and balances in place. Security checks meet the necessary requirements for the posts required. Controls are in place for managing staff and limiting the public access to information, assets and estate. With regard to data management, we accept the need for operational effectiveness with risk mitigated through careful management limiting distribution of data within the Council and with our partners, ensuring that personal data is protected in line with the necessary regulations. Assurances will also be provided on how we are protecting the Council from cyber-attacks, whether in terms of the risk of fraud and inadvertent or malicious corruption or modification of data on its IT systems.

Environmental Risks: We are cautious to any actions that have a negative impact on the environment. We have limited appetite for decisions/actions which increase emissions and reduce biodiversity. A balance is keenly sought between social, environmental, and economic considerations thereby reflecting our statutory duty together with our Community Planning partners.

Project/Programme Risks: We are open to risk in terms of supporting innovation in our project and programmes, where there are demonstrable improvements in service delivery. Responsibility for decisions is devolved to the right level of staff so that we can deliver effectively and in a timely way. However, the associated governance, financial, people and technology risks specific to those projects or programme are as per the categories above to ensure consistent standards in how the Council operates.

Safety. We are averse to anything which puts the health, safety and wellbeing of people at risk of harm, injury, ill-health or loss of life. This includes members of the public and employees.

We are averse to anything that may jeopardise people's health and safety. We put in place rigorous systems for, monitoring, training and assessment for the health and safety for all our employees and contractors both for their own and the public's safety in relation to Council property.
We are averse to any risks that pose security or safeguarding threats, in that we adhere to the rules and requirements for recruiting and vetting of staff, depending on their roles and responsibilities.

FODC Risk Appetite Statements outlining optimal and tolerable positions

	Averse	Cautious	Open	Eager
A: Strategic	Guiding principles or rules in place that minimise risk in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 5+ year intervals	Guiding principles or rules in place that allow considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 3–4-year intervals	Guiding principles or rules in place that are receptive to considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 2-3 year intervals	Guiding principles or rules in place that welcome considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 1-2 year intervals
B: Governance	Avoid actions with associated risk. No decisions are taken outside of processes and oversight/ monitoring arrangements. Organisational controls minimise risk of fraud and maximise assurance, with significant levels of resource focused on detection and prevention	Willing to consider actions where benefits outweigh risks. Processes, and oversight/monitoring arrangements enable cautious risk taking. Controls enable fraud prevention and provide high levels of assurance, detection and deterrence by maintaining appropriate controls and sanctions	Receptive to taking difficult decisions when benefits outweigh risks. Processes, and oversight/monitoring arrangements enable considered risk taking. Levels of fraud controls and other internal controls are varied to reflect scale of risks with costs	Ready to take difficult decisions when benefits outweigh risks. Processes, and oversight/monitoring arrangements support informed risk taking. Levels of fraud controls and other internal controls are varied to reflect scale of risk with costs
(+ Legal)	Play safe and avoid anything which could be challenged, even unsuccessfully	Want to be reasonably sure we would win any challenge	Challenge will be Problematic but we are likely to win, and the gain will outweigh the adverse impact	Chances of losing are high but exceptional benefits could be realised in longer term,
Reputational) (+	Zero appetite for any decisions with high chance of repercussion for organisations' reputation	Appetite for risk taking limited to those events where there is no chance of any significant repercussion for the Council	Appetite to take decisions with potential to expose organisation to additional scrutiny, but only where appropriate steps are taken to minimise exposure	Appetite to take decisions which are likely to bring additional Governmental/ organisational scrutiny only where potential benefits outweigh risks
C: Financial	Avoidance of any financial impact or loss, is a key objective	Seek safe delivery options with little residual financial loss	Prepared to invest for benefit and to minimise the possibility of financial loss only if it could yield upside opportunities	Prepared to invest for best possible benefit and accept possibility of financial loss (controls must be in place)
D: People	Priority to maintain close management control & oversight. Limited devolved authority. Limited flexibility in relation to working practices. Development investment in standard practices only	Seek safe and standard people policy. Decision making authority generally held by senior management	Prepared to invest in our people to create innovative mix of skills environment. Responsibility for noncritical decisions may be devolved	Innovation pursued – desire to 'break the mould' and challenge current working practices. High levels of devolved authority – management by trust rather than close control
E: Technology	General avoidance of new systems/technology developments	Consideration given to adoption of established/ mature systems and technology improvements.	Systems/technology developments considered to enable improved delivery.	New technologies viewed as a key enabler of operational delivery.

		Agile principles are considered	Agile principles may be followed	Agile principles are embraced
+Security (+ Data Management)	No tolerance for security risks causing loss or damage to property, assets, information or people. Stringent measures in place, including: • Staff vetting maintained at highest appropriate level. • Controls limiting staff and visitor access to information, assets and estate. • Access to staff personal devices restricted in official sites	Limited security risks accepted to support business need, with appropriate checks and balances in place: • Vetting levels may be flexible depending on the posts required • Controls managing staff and limiting visitor access to information, assets and estate. • Staff personal devices may be used for limited official tasks with appropriate permissions	Considered security risk accepted to support business need, with appropriate checks and balances in place: • New starters may commence employment at risk, following partial completion of vetting processes • Controls limiting visitor access to information, assets and estate. • Staff personal devices may be used for official tasks with appropriate permissions	Organisational willing to accept security risk to support business need, with appropriate checks and balances in place: • New starters may commence employment at risk, following partial completion of vetting processes • Controls limiting visitor access to information, assets and estate. • Staff personal devices permitted for official tasks
	Lock down data & information. Access tightly controlled, high levels of monitoring	Accept need for operational effectiveness with risk mitigated through careful management limiting distribution.	Accept need for operational effectiveness in distribution and information sharing	Level of controls minimised with data and information openly shared
F: Environmental	Zero appetite for decisions/actions which increase council emissions in areas such as energy & buildings, resource management, transport and land use and which reduce biodiversity. Optimum balance between social, environmental, and economic considerations must be achieved.	Limited appetite for decisions/actions which increase emissions and reduce biodiversity. Balance is keenly sought between social, environmental, and economic considerations and achieved in most cases.	Accept the need for some decisions/actions which may increase emissions and reduce biodiversity. Accept that the balance between social, environment and economic considerations is not always achievable in some cases.	Willingness to pursue action which increase emissions and reduce biodiversity. Accept that the balance between social, environmental and economic considerations cannot be achieved and that economic and social considerations will prevail over environmental considerations.
G: Project / Programme	Defensive approach to transformational activity. Aim to maintain/ protect, rather than create or innovate. Priority for close management controls and oversight with limited devolved authority. Benefits led plans fully aligned with strategic priorities, functional standards	Tendency to stick to the status quo, innovations generally avoided unless necessary. Decision making authority generally held by senior management. Plans aligned with strategic priorities, functional standards	Innovation supported, with demonstration of commensurate improvements in management control. Responsibility for noncritical decisions may be devolved. Plans aligned with functional standards and organisational governance	Innovation pursued – desire to 'break the mould' and challenge current working practices. High levels of devolved authority – management by trust rather than close control. Plans aligned with organisational governance
+ (Operations)	Defensive approach to operational delivery – aim to maintain/protect, rather than create or innovate. Priority for close management controls and oversight with limited devolved authority	Tendency to stick to the status quo, innovations generally avoided unless necessary. Decision making authority generally held by senior management. Management through leading indicators	Innovation supported, with clear demonstration of benefit/improvement in management control. Responsibility for noncritical decisions may be devolved	Innovation pursued – desire to 'break the mould' and challenge current working practices. High levels of devolved authority – management by trust rather than close control
Safety	Zero risk appetite for any decision/actions which puts the safety of people at risk.	Awareness of the need to protect people from risks to health or likelihood of harm	Limited awareness of the need to protect people from risks to health or likelihood of harm.	Acceptance that the safety of people may be jeopardised in pursuit of decisions/actions.

	Full awareness of the need to protect people from any risks to health or harm. Robust systems in place to protect people from the risks to health or likelihood or harm, with the appropriate equipment or processes necessary to mitigate risk to lowest level.	Some systems to protect people from risks to health or harm in place.	Limited systems, equipment and processes to protect them.	Lack of awareness of the need to protect people from risks to health or likelihood of harm. The absence of systems, equipment and processes to protect them.

Appendix 2

Risk Register Template

					Current Risk Assessment							Action						Post-Control						
Risk Number	Risk Description	Causes	Current Controls / Actions		LIKELIHOOD	Finance	Staff	Service	Reputation	IMPACT		RISK SCORE	Accept	Transfer	Mitigate	New Actions	Responsibility	New action implementation date / Review date		LIKELIHOOD	Finance	Staff	Service	Reputation	IMPACT		RISK SCORE

Fermanagh & Omagh District Council
Comhairle Ceantair Fhear Manach agus na hÓmaí

Appendix 3

……Directorate Risk Register
Summary of Changes
Date of Review:

Risk No.	Description	Change

Fermanagh & Omagh District Council
Comhairle Ceantair Fhear Manach agus na hÓmaí

Appendix 4

Risk Management Report
…….Directorate

Date of Review Meeting:	
Attendees: **Apologies:**	
1. Changes in profile over the last 6 months.	
2. Summary of issues over the last 6 months.	
3. The effectiveness of control measures in place	
4. Any new emerging issues	
5. Updated list of critical risks	

This report represents the most current knowledge regarding all the risks involved.	
Signed	
	Director
Date	

Fermanagh & Omagh District Council
Comhairle Ceantair Fhear Manach agus na hÓmaí

Appendix 5

Request to Escalate Risk to Corporate Register
…… Directorate

Date of Review Meeting:	
Attendees: **Apologies:**	
1. Risk No.	
2. Existing Controls	
3. Risk Score (Post Control)	
4. Reason for Escalating Risk to Corporate Register	

Signed	
	Director
Dated	