Risk Management Framework

March 2024

Reviewed December 2025

Contents

Introduction 3

Part 1 - Risk Management Policy & Strategy 4

2. What is Risk Management 6

3. Why does the Council need to carry out Risk Management? 6

4. Risk Management Strategy 8

   i. Governance and Infrastructure 8

   ii. Culture ..... 12~~11~~

5. Management of Risks ..... 14~~13~~

6. Risk Appetite Statement ..... 14~~13~~

7. Risk Matrix ..... 16~~15~~

Appendix 1 - ALARM National Performance Model for Risk Management in Public Services ..... 20~~19~~

Part 2 - Risk Management Toolkit ..... 22~~21~~

1. Risk Management Process ..... 23~~22~~

   i. Risk Identification ..... 25~~24~~

   ii. Analyse, assess and evaluate risks. ..... 27~~25~~

   iii. Review of controls and their effectiveness ..... 28~~26~~

   iv. Response to Risk ..... 29~~27~~

   v. Reporting, Monitoring and Communication ..... 31~~29~~

   vi. Integration with Strategic Planning and Decision Making ..... 35~~33~~

Appendix 2 – Corporate Risk Register Template 35

Introduction

This Risk Management Framework pulls together a number of key elements to ensure that the Council establishes and maintains effective risk management. The overarching Framework includes;

i) The Risk Management Policy, Strategy and Risk Appetite Statement which sets out the Council's approach to risk management and;

ii) The Risk Management Toolkit, which sets out the processes that managers will follow to deliver effective risk management.

Part 1 - Risk Management Policy & Strategy

1. Risk Management Policy Statement

We recognise risk management is a vital activity which underpins and forms part of the vision, values, and corporate priorities of the Council as set out in the Gedling Plan. In addition, by having an effective risk management framework in place it will provide the communities we serve with confidence that we can deliver on the priorities we have promised.

The Council promotes continuous improvement and strives to be efficient and effective in all areas of service delivery. This requires the adoption of new ways of working and a willingness to change which sometimes has risks associated with it.

Risk is always present in every activity that we do, and our risk management framework sets out to be proactive in the identification, assessment, and management of key areas of risk. We seek to embed effective risk management within the operation and decision-making process of the Council. Risk management needs to be an integral part of all processes, projects and strategic decisions made, this will include procurement and contracting arrangements. Wherever we work with partners or third parties we will ensure that they are aware of and work in line with our risk management framework.

Our aim is to have a risk management framework that is fit for purpose and appropriate to the size and nature of our operations. We aim to ensure that our risk management framework has a consistent, well communicated, and formal process operating effectively within the Council.

In order to assist in effective decision making it is essential for us as strategic leaders to define the level of risk exposure that we think is acceptable. This is set out in the Risk Appetite Statement. This should inform decision makers on the level of risk that they can take and areas where additional controls will need to be implemented to manage risks being taken.

The risk management framework and the effective management of risks is a key part of the Governance Framework of the Council. Its implementation will provide assurance to all our stakeholders that risk identification and management has a key role in the delivery of the Gedling Plan and strategic objectives.

The Council accepts its legal and moral duties in taking informed decisions about how best to control and minimise the downside of risk, whilst still maximising opportunity and benefiting from positive outcomes.

Through this framework we will involve, empower, and give ownership to all employees and members to identify and manage risk. Risk management will be supported by regular discussions and appropriate actions by Cabinet ~~and~~ , SLT and the Corporate Risk Board including the regular review of significant risks and

reviewing actions to reduce those risks to an acceptable level. The management of risk will be an integral part of strategic and operational planning, as well as being embedded in the day-to-day operation, development, monitoring, and overview of the Council.

[Name]
Chief Executive

[Name]
Leader of the Council

2. What is Risk Management

Risk Management is the process whereby an organisation methodically addresses the risks which may stop them from achieving their corporate objectives. The focus of good risk management is the identification and treatment of the risks to minimise any impact or maximise benefit.

A risk is defined as the “effect of uncertainty on objectives” by the International Organisation for Standardisation (ISO 31000). An effect is a positive or negative deviation from what is expected, and that risk is often described by an event, a change in circumstances or a consequence. By accepting this definition, the Council recognises that taking the right risks in an informed way can be beneficial to the objectives and that risk management is not just a negative process used to stop opportunities being taken.

Risk Management should be a continuous and developing process connected with the organisation’s strategy and the delivery of it in the past, present, and future. It should be embedded into the culture of the organisation and led by the most senior leaders and managers.

3. Why does the Council need to carry out Risk Management?

Risk management is a management tool which should form part of the governance system of every public service organisation. When applied appropriately, risk management can be very beneficial. It can help organisations achieve their stated objectives and deliver on intended outcomes. It can also help managers to demonstrate good governance, better understand their risk profile and better mitigate risks (particularly uninsurable risks). Externally it can help the organisation to enhance political and community support and satisfy stakeholders’ expectations on internal control.

The Council does not operate in isolation and is subjected to constant challenges and external changes which may pose a threat to the delivery of the Gedling Plan strategic objectives or provide new opportunities which have to be considered and addressed on an ongoing basis. Risk management processes provide a mechanism by which these issues and their impact can be identified, assessed, monitored and relevant actions taken to address them.

Some of the most recent examples of the landscape the Council operates in include:

- Covid 19 Pandemic
- Cost of living crisis
- Economic downturn
- Limited finances for Local Government
- Organisational resilience pressures
- Recruitment difficulties for key roles

- New ways of working - partnerships, outsourcing, commissioning
- Brexit
- Innovative technologies
- Agile/remote working methods
- Climate Change
- Local Government Reorganisation

Whilst it is good business practice and essential for good governance processes the Council also has a legal requirement to have a risk management process in place.

The Accounts and Audit Regulations 2015 state:

> *"A relevant authority must ensure that it has a sound system of internal control which—*
>
> *(a)facilitates the effective exercise of its functions and the achievement of its aims and objectives.*
>
> *(b)ensures that the financial and operational management of the authority is effective; and*
>
> *(c)includes effective arrangements for the management of risk."*

Ultimately by having an effective, embedded Risk Management Framework in place to influence its decision making the Council can benefit by helping to ensure:

- The objectives set in the Gedling Plan can be delivered.
- All employees and Members understand the desired culture in relation to risk,
- Decisions to take appropriate risks in certain areas can be made from an informed viewpoint.
- The Council can protect its reputation.
- Operational and financial efficiency is ensured as resources are not lost by taking unnecessary risks.
- The Council can maximise opportunities.
- The Council can demonstrate good governance processes.
- Assets are protected.

4. Risk Management Strategy

i. Governance and Infrastructure

Sponsorship and Positioning of Risk Management

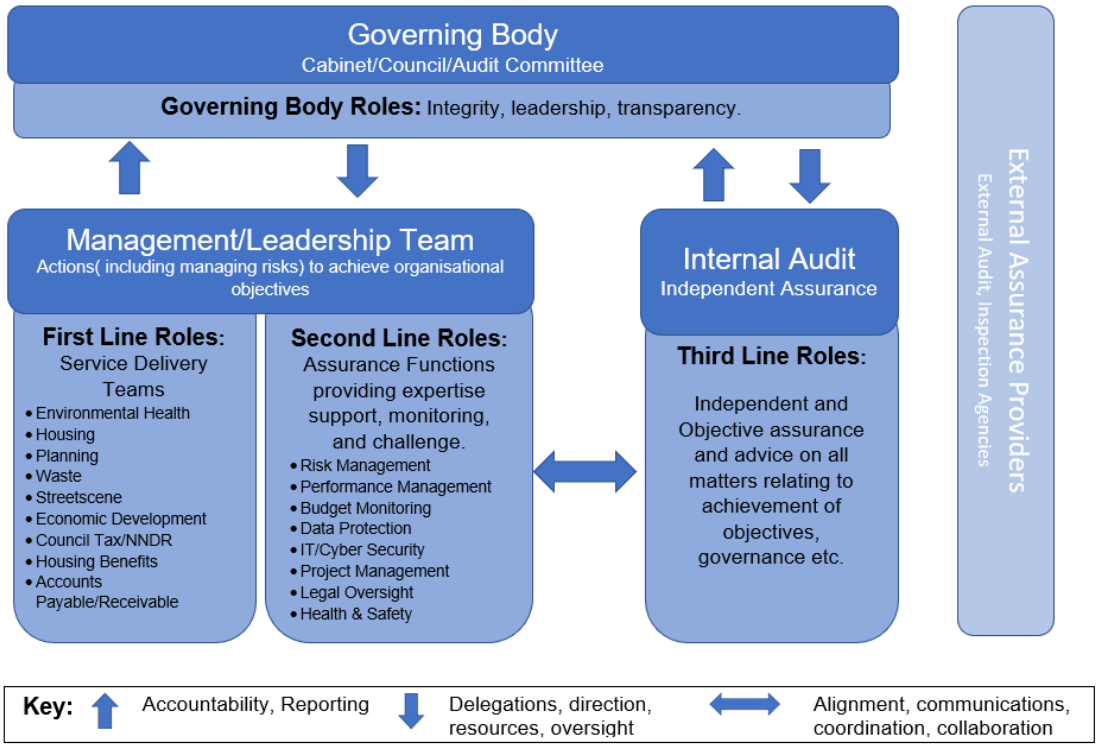
Risk Management needs to be embedded throughout the Council and underpin all of its activities. It is a key governance process and needs to have direction and leadership from the very top of the organisation; as well as being relevant and responsive to the staff delivering services on the ground. The risk matrix and risk appetite statement contained in this strategy will be used across the Council to ensure that a collective understanding and language is adopted when talking about risks.

The Cabinet and SLT are responsible for giving direction, approving the Risk Management Framework, and taking ownership of the Corporate Risk Register. They will ensure that all decisions are taken in accordance with the Council's agreed risk appetite.

The Council's Corporate Risk Board sits beneath SLT and meets every other month to assess risk levels across the organisation. The Risk Board is made up of the Deputy Chief Executive, s.151 officer, Assistant Directors and Senior Managers with responsibility for risk. This board reports risk issues to SLT as they arise and ensures regular updating of departmental risks to support an accurate Corporate Risk register.

The Chief Executive will act as the sponsor for the Risk Management Framework at a strategic level and with the support of the Director responsible for Audit and the Chief Financial Officer, will ensure that SLT decisions are taken in line with the Risk Management Framework.

Management and other corporate reporting/assurance functions will help to monitor and report on the effective delivery of the Risk Management Framework in line with the Institute of Internal Auditors' "3 Lines Model" as set out below:



Roles and Responsibilities

All employees and Members have a role to play in the management of risk as it is a key part of day-to-day service delivery and management of the Council. However certain individuals or groups have specific responsibilities in the oversight and implementation of risk management, more detail on these is set out below.

Risk Management Sponsor (CEO)

- Champion risk management at the strategic level.
- Ensure regular discussions are held on Risk Management and the Council's risks.
- Encourage SLT and senior managers to ensure they have effective risk management arrangements in place for their service areas.

Risk Manager (Director responsible for Audit and Chief Financial Officer)

- Coordinate the organisation's risk management activity.
- Develop and maintain with SLT the risk management framework, methodologies, and tools.
- Chair and oversee the Council's Corporate Risk Board
- Highlight any significant new or worsening risks to SLT, Audit Committee and the Cabinet for review and action.
- Assist in the delivery of the risk management process and aggregation of risk profiles across the organisation.

- Provide risk management guidance, training, and advice.
- Provide the link between risk management and other related disciplines, for example, insurance, business continuity, safeguarding, data protection, cyber security, emergency planning, and health and safety.
- Promote and share best practice risk management across the organisation.

Cabinet

- Approve the Risk Management Framework which includes policy, strategy, and Risk Appetite for the Council.
- Provide assurance to stakeholders that risks are being effectively managed.
- Within individual portfolios understanding and enabling informed risk within their portfolio areas
- Ensuring application of the Risk management framework to support decision making.

Audit Committee

- Gain assurance over the governance of risk, including leadership, integration of risk management into wider governance arrangements, and the top-level ownership and accountability for risks.
- Support the development and review of the Council's Risk Management Framework.
- Oversee the risk management framework, and its implementation in practice.
- Review key risks to the Council and controls in place via the Corporate Risk Register.
- Oversee the integration of risk management in governance and decision-making processes.
- Review arrangements to coordinate and lead risk management.

SLT

- Regularly review the risk management framework to ensure it underpins the organisation's strategy and objectives.
- Recommended the Risk Management Framework to Cabinet for approval.
- Approve the processes to be used by management to manage and monitor risks.
- Review the key risks across the organisation, consider their importance against strategic objectives and action further controls.
- Allocate sufficient resources to address the top risks.
- Report on key risks and controls in line with the organisation's risk management strategy.
- Create an environment and culture where risk management is promoted, facilitated, and appropriately undertaken by the organisation and is embedded in all decision making.
- Champion risk management activities, educate colleagues, and raise awareness of the benefits of managing risk effectively.

- Follow the risk management process as detailed in the Strategy including maintaining the Corporate Risk Register and monitoring actions.
-

Corporate Risk Board

- Ensure an effective risk control framework is in place and operating effectively across all service areas.
- Embedding risk awareness across the Council.
- Working with members to set risk appetite and tolerance.
- Identifying and assessing strategic risks that could impact Council objectives and identifying mitigatory actions.
- Prioritising and categorising risks, and related actions.
- Assigning risk owners and timescales for completion of remediation or mitigation.
- Tracking actions to completion (including related audit actions), escalating to SLT where necessary.
- Monitoring risk levels across the organisation including considering and stress testing individual and multi-variate risks and impacts.
- Reporting on the Council's risk profile and strategic risk to SLT and Audit Committee.
-

~~**Heads of Service**~~**Risk Owners (Assistant Directors and Senior Managers)**

- Communicate the benefits of risk management across operational areas for which they are responsible.
- Help facilitate the risk management process and risk reporting procedures across operational areas.
- Help ensure key stakeholder commitment.
- Ensure risk management processes and risk reporting procedures are completed in line with the organisation's risk management framework for each area under team member's responsibilities.
- Monitor and review the key risks in each area of responsibility regularly but quarterly as a minimum.
- Ensure risk management is explicitly considered in framing Service Plans, Projects and business cases.
- Ensure risk management is explicitly reflected in decision making.
- Ensure completion of action plans associated with risk mitigation.

~~**Managers**~~

- Manage risk effectively in each area of responsibility.
- Complete the risk management process and risk reporting procedures as per the organisation's guidelines.
- Complete, track and monitor the progress of action plans.

All Employees

- Understand and comply with the risk management processes and guidelines of the organisation.

- Monitor work on an ongoing basis to identify new and emerging risks and escalate as required.

Internal Audit

- Create an audit plan aligned with the key Corporate Risks.
- Review and challenge the effectiveness of the risk management framework.
- Review the progress of planned actions.
- Test and validate existing controls.

ii. Culture

To be effective in the long term and to support good governance, effective risk management needs to be embedded into the Council's Culture.

It is important that this Culture is seen to run from the top of the Council down. SLT and Senior Managers should set an example to others when it comes to embracing the importance of effective, embedded risk management in all processes. All managers need to support the roll-out of this framework and ensure that risk management processes once established are followed by all employees.

To do this, it will be necessary to provide relevant training and awareness of the Council's Risk Management Framework to all employees. A training and communication plan will be developed to ensure the framework is effectively rolled out and embedded into the Council and that all employees see that they have a vital role to play.

An essential element needed to embed the Council's risk management into the Council's culture is ensuring that there is a collective understanding of risks and that a common language is used when it comes to quantifying and discussing risks. To achieve this the risk matrix within this framework and the definitions for levels of risk should be used consistently across the Council. This adds clarity so that the level and definition of a risk is understood and means the same thing to everyone regardless of which section or function is talking about it. Unless there is a very good reason any assessments associated with risks should utilise the agreed risk matrix and definitions and operate in line with the Council's agreed risk appetite.

It is also important that the Council's Risk Appetite Statement and risk processes are understood by those we work closely with in partnerships and in contracts. Wherever possible the Council's risk management processes should be used when working with partners and contractors.

All employees and managers need to take ownership and accountability for their role in the Risk Management process as set out in the "roles and responsibilities" section of the strategy. Employees at all levels should be encouraged to raise

emerging risks that they have identified with their line managers with the knowledge that the information will be considered and acted on appropriately where necessary.

In addition to training and awareness the Chief Executive, as the Risk Management Sponsor, will oversee the risk management culture at SLT. They will do this by encouraging positive messages relating to risk management and challenging poor risk management practices such as the failure to adequately consider risk implications when making important decisions or the failure to review levels of risk within service areas or complete actions to mitigate risks within agreed timescales.

As part of embedding Risk Management into the culture of the Council it is important that everyone understands the current position of Risk Management and where we want to get to. To do this we are adopting the ALARM National Performance Model for Risk Management in Public Services which can be found at appendix 1. An initial assessment has been made by SLT and against each of the criteria. The assessment has shown that the Council is at the current level for each category:

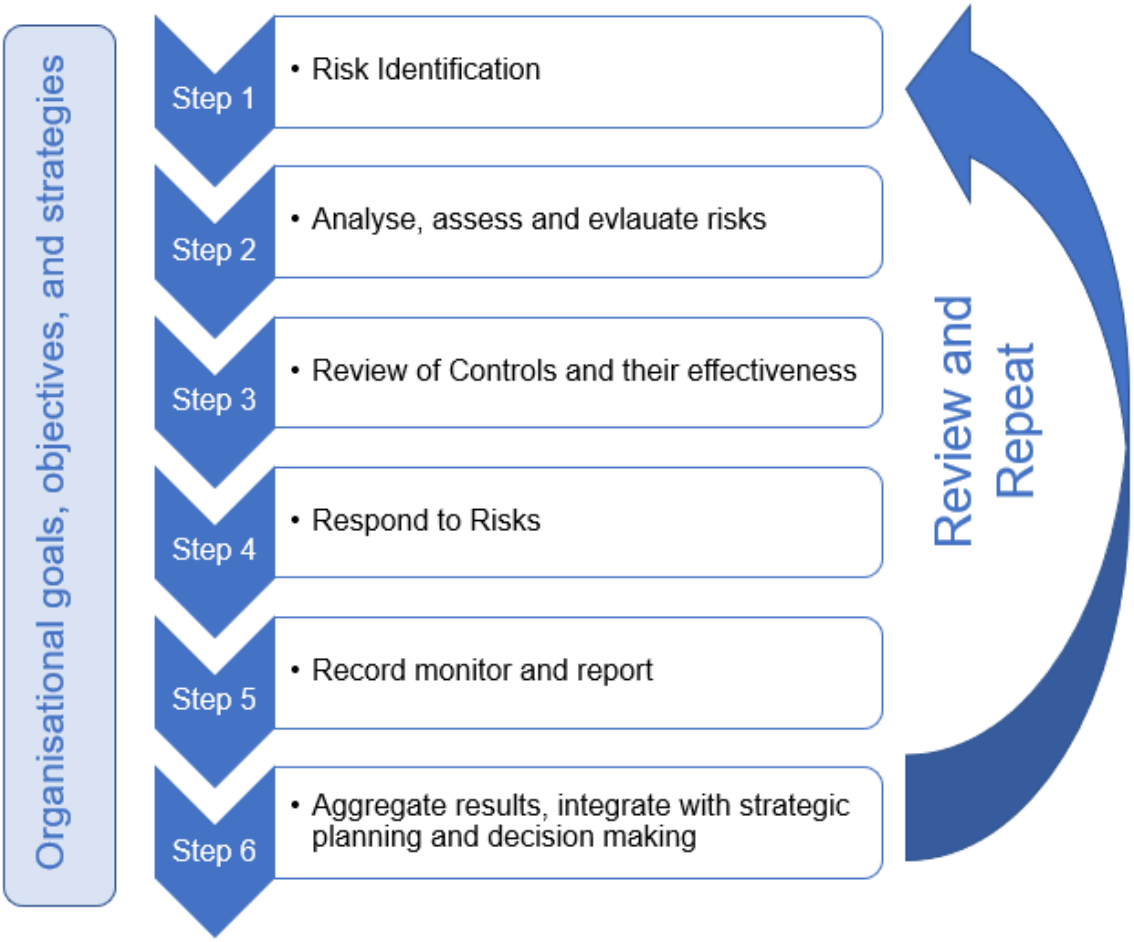
Category	**Rating (1-5)**	**Rating 2025**
Leadership and Management	3	4
Strategy and Policy	3	4
People	3	4
Partnership, Shared Risk and Resources Processes	3	3
Processes	3	3
Risk Handling and Assurance	2	4
Outcomes and Delivery	2	3

It is recognised that it is unlikely that the Council will be able to achieve the rating of "5 - Driving" in all categories due to limited resources and competing demands on officer time**.** Therefore, it has been agreed by SLT that the target will be to achieve at least Level 4 rating- Embedded and Working in each category by April 2025 moving to Level 5 rating - Driving by the end of the Framework 2027.

Since the adoption of the framework in 2024, the Council has had an audit of its risk management processes. In light of the findings of the audit, there has been a further assessment of the ALARM framework. The amended scores are shown in the table above. Overall this shows an improvement in the overall picture for risk management.

5. Management of Risks

The Council will implement an ongoing cyclical review process for the management of risks. As set out in the diagram below.



6. Risk Appetite Statement

Risk appetite can be defined as the amount and type of risk an organisation is willing to accept in the pursuit of its objectives.

The Council's overall risk appetite is set out in reference to the risk appetite definitions below which include the colours used in the risk matrix to show levels the relevant levels of risk. Escalation and reporting thresholds will be reassessed periodically to ensure risks are reported and reviewed within suitable defined limits.

Category	Definition	Risk Levels
Avoid	No appetite. Not prepared to take risk.	N/A
Adverse	Prepared to accept only the very lowest levels of risk, with the preference being for ultra-safe delivery options, while recognising that these will have little or no potential for reward/return	Negligible Risk (Blue)
Cautious	Willing to accept some low risks, while maintaining an overall preference for safe delivery options despite the probability of these having mostly restricted potential for reward/return.	Low Risk (Green)
Moderate	**Tending always towards exposure to only modest levels of risk in order to achieve acceptable outcomes**	**Modest Risk (Yellow)**
Open	Prepared to consider all delivery options and select those with the highest probability of productive outcomes, even when there are elevated levels of associate risk.	Medium Risk (Orange)
Hungry	Eager to seek original/creative/pioneering delivery options and to accept the associated substantial risk levels in order to secure successful outcomes and meaningful reward/return.	High Risk (Red)

Cabinet have agreed that the Council's current overall base risk appetite is defined as moderate.

This means the Council remains open to innovative ways of working and to pursue options that offer potentially substantial rewards, however, also carry a moderate level of risk. The Council's preference is for safe delivery options, especially for those services required by statute and ideally all actions should be within this agreed risk appetite. This means that options should only be pursued if they can be managed as a yellow or lower risk.

However, in an organisation, such as a local authority, where service delivery is diverse and risks take many forms, risk appetite may vary according to the specific circumstances being assessed. For example, an option may be considered to improve the Town Centre that is seen to have a higher level of risk for the Council than the moderate appetite would allow but where the ultimate outcome would bring significant benefits if successfully implemented.

Where an option or decision is being pursued that is deemed to be at a higher level of risk than Moderate then additional controls/safeguards will need to be put in place. This will include formal agreement from the three Statutory Officers (S151 Officer, Monitoring Officer, and Head of Paid Service) and the appropriate decision maker at member level to pursue the option, and increased levels of monitoring and reporting of the risk will need to be established.

7. Risk Matrix

To assist in the management of risks the Council has adopted a 4 x 4 matrix. This has the risk appetite displayed through the use of colour coding of the squares. With the Impact across the top on the x-axis and the likelihood down the side on the y-axis.

	Minor/Non-Disruptive Impact (1)	Moderately Disruptive Impact (2)	Serious Consequences (3)	Major Consequences (4)
Very Likely (4)	**4 (Yellow)**	**8 (Orange)**	**12 (Red)**	**16 (Red)**
Probable (3)	**3 (Yellow)**	**6 (Orange)**	**9 (Orange)**	**12 (Red)**
Possible (2)	**2 (Green)**	**4 (Yellow)**	**6 (Orange)**	**8 (Orange)**
Unlikely (1)	**1 (Blue)**	**2 (Green)**	**3 (Yellow)**	**4 (Yellow)**

The matrix has been colour coded in line with the Council's risk appetite as follows.

Risk Levels	Colour
Negligible Risk	Blue
Low Risk	Green
Modest Risk	Yellow
Medium Risk	Orange
High Risk	Red

The risk matrix is supported by the following definitions.

LIKELIHOOD

4	**Very Likely** >90%	• Event expected to occur. Has occurred and will continue to do so without action being taken. • Indication of imminent occurrence • There are external influences which are likely to make our controls ineffective
3	**Probable** 60-90%	• There is a moderate exposure to the risk. • Reasonable to expect event to occur within a year. • Has occurred in the past. • Is likely to occur within the Council's planning cycle. • There are external influences which may reduce effectiveness of controls
2	**Possible** 30-60%	• There is a low exposure to the risk. • Little likelihood of event occurring - 1 in 10 years • There is a potential for external influences which may reduce effectiveness of controls
1	**Unlikely** 0-30%	• Extremely remote • Not expected to occur but may do so in exceptional circumstances - 1 in 100 years. • There are few or no external influences which may reduce effectiveness of controls

IMPACT

Score	Description	Indicative Guidelines
4	**Major Consequences**	The consequence is so bad that urgent action must be taken to improve the situation or prevent it worsening. External support from the Government or other agencies is likely to be needed: • Catastrophic loss, delay, or interruption to services • Level of financial loss, additional costs, or loss of assets which the Council is unable to resource without additional Government/External support. • One off event which would de-stabilise the Council over several years. • The risk will cause the objective not to be reached, causing damage to the organisation's

		reputation. • Will attract medium to long-term attention of legislative or regulatory bodies. • Major complaints • Significant adverse media interest • Death or life-threatening injury
3	**Serious Consequences**	The consequences are sufficiently serious to require attention by Cabinet and/or full Council: • Loss of key assets or services for an extended time period. • Longer term impact on operational efficiency or performance of the Council or crucial service areas • Financial loss, additional costs or loss of assets which would need a Council decision as the scale of the loss would be outside the Council's budget & policy framework. • The risk would destabilise the Council in the short term. • The intended objectives are unlikely to be met leading to negative impact on the Council's reputation and a significant number of complaints. • Will lead to attention for regulators and External Auditors for a significant time. • Major accident/injuries (but not life-threating)
2	**Moderate/ Disruptive**	The consequence is sufficient to require attention by Leadership Team and cannot be managed within a Service Area • Significant loss, delay, or interruption to a service. • Medium term impact on operational efficiency or performance • Financial loss, additional costs or loss of assets that is within the Council's budget & policy framework but needs a Statutory Officer decision, Leadership Team decision, Cabinet decision or needs to be drawn to Cabinet's attention. • The risk will cause some elements of the objective to be delayed or not achieved, causing potential damage to the organisation's reputation. • May attract medium to short term attention of legislative or regulatory bodies. • Significant complaints

		• Serious accident / injury (but not life threatening)
1	**Minor/Non-Disruptive**	The consequences can be dealt with as part of the normal day-to-day business by the Team Manager and the Head of Service: • Minor loss, delay, or interruption to services • Short term impact on operational efficiency or performance • Negligible financial loss • The risk will not substantively impede the achievement of the objective, causing minimal damage to the organisation's reputation. • No or minimal external interest. • Isolated complaints • Minor accident / injury

Appendix 1 - ALARM National Performance Model for Risk Management in Public Services

Scale	Leadership & Management	Strategy and Policy	People	"Partnership, Shared Risk and Resources Processes"	Processes	Risk Handling and Assurance	Outcomes and Delivery
Driving 5	Leadership uses consideration of risk to drive excellence through the organisation, with strong support and reward for well managed risk-taking	Strategy and Policy are closely aligned to risk management and the threat of failing to achieve objectives	All staff are empowered to be responsible for risk management. The organisation has a good record of innovation and well-managed risk-taking. Absence of a blame culture	Clear evidence of improved partnership delivery through risk management and that key risks to the community are being effectively managed	Management of risk and uncertainty is well integrated with all key business processes and shown to be a key driver in business success	Clear evidence that risks are being effectively managed throughout the organisation. Considered risk-taking part of the organisational culture	Risk management arrangements clearly acting as a driver for change and linked to plans and planning cycles
Embedded and working 4	Leadership is supportive of the risk management process, engages actively and ensures it is embedded throughout the organisation	Risk management principles are reflected in the organisation's strategies and policies. Risk framework is reviewed, developed, refined, and communicated	A core group of people have the skills and knowledge to manage risk effectively and implement the risk management framework. Staff are aware of key risks and their responsibilities	Sound governance arrangements are established. Partners adequately support one another's risk management capability and capacity	A framework of risk management processes in place and used to support service delivery. Robust business continuity management system in place	Evidence that risk management is being effective and useful for the organisation and producing clear benefits. Evidence of innovative risk-taking	Very clear evidence of very significantly improved delivery of all relevant outcomes and showing positive and sustained improvement
Working 3	Leadership take part sporadically in the risk management process and provide some resources	A basic risk strategy and related policies exist and are partially implemented	An individual with Risk Management responsibilities is in place with the correct skills and experience	Risk with partners and suppliers is managed across organisational boundaries but inconsistently	Risk management processes used to support key business processes. Early warning indicators and lessons learned are reported. Critical services	Clear evidence that risk management is being effective in all key areas, capability assessed within a formal assurance framework and against best practice standards	Clear evidence that risk management is supporting delivery of key outcomes in all relevant areas

Scale	Leadership & Management	Strategy and Policy	People	"Partnership, Shared Risk and Resources Processes"	Processes	Risk Handling and Assurance	Outcomes and Delivery
					supported through continuity plans		
Happening 2	Leadership are aware of risk management process but do not actively participate	The need for a risk strategy and risk-related policies has been identified and accepted but not implemented	Risk management is an informal part of a single person's role within the organisation	Approaches for addressing risk with partners are being developed and implemented	Some stand-alone risk processes have been identified and are being developed. The need for service continuity arrangements has been identified	Some evidence that risk management is being effective. Performance monitoring and assurance reporting being developed	Limited evidence that risk management is being effective in, at least, the most relevant areas
Engaging 1	Leadership are not providing guidance with regards to risk management objectives, culture, or practices	The need for a risk strategy and risk-related policies has not been identified. The risk management system is undocumented with few formal processes present	No risk management roles or associated skills are in place within the organisation and there is little desire to implement this	No risk management considerations are given to partnerships	No stand-alone risk processes have been developed	No clear evidence that risk management is being effective	No clear evidence of improved outcomes

Part 2 - Risk Management Toolkit

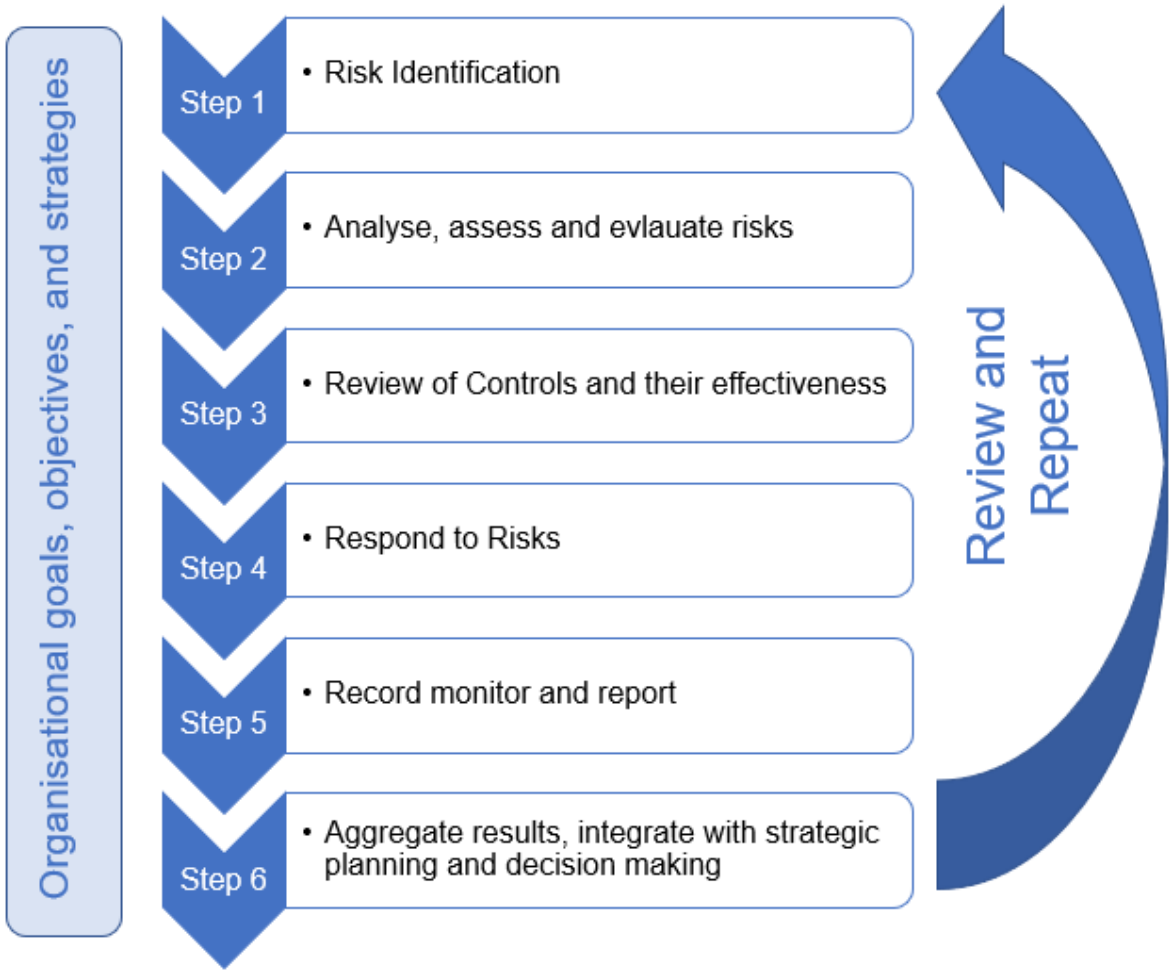
1. Risk Management Process

The risk management process is continuous. It involves identifying the risks, prioritising them and implementing actions to mitigate the top risks on an ongoing basis.

Risks to an organisation can have positive and negative impacts, opportunities should be seen as positive risks and if identified early can be managed well, and the benefits realised.

The Council is adopting a risk management process that can be used to identify and score both positive and negative risks. This process should be embedded across the Council to improve informed decision making and increase delivery if the key objectives. All managers and employees should use the tools and techniques when making decisions whether there is a corporate requirement for a formally documented risk register relating the function/process or not.

The Council's risk management process can be broken down into six steps as shown below.


Organisational goals, objectives, and strategies
Step 1
• Risk Identification
Step 2
• Analyse, assess and evlauate risks
Step 3
• Review of Controls and their effectiveness
Step 4
• Respond to Risks
Step 5
• Record monitor and report
Step 6
• Aggregate results, integrate with strategic planning and decision making
Review and Repeat

i. Risk Identification

Risk identification is one of the first major components of a best practice risk management process. The purpose of risk identification is to generate a comprehensive inventory of risks based on events that might create, prevent, accelerate, or delay the achievement of the organisation's objectives. In order to do this, it is beneficial for all risks to be identified at each level of the organisation; however, we accept that resources are not available to corporately support formal risk registers for all operational functions.

The Council has therefore set a requirement for formal risk registers to be maintained at specific levels of the organisation or for specific reasons, but additional risk registers could be maintained below these to assist managers and to inform the formal risk registers. It is hoped in time that Managers will see the benefit of maintaining risk registers for all of their functions and not just those mandated by this framework.

The first stage of any risk management exercise is to identify the risks that are currently affecting the Council or may do so in the future. To do this a number of steps should be considered.

1. Review the existing risk registers and ask:
    a. Have any of the existing risks changed significantly?
    b. Are any risks missing?
    c. Are there any changes in the next 12 months that could present a risk?

2. Identify new and emerging risks - this could be done via horizon scanning, monitoring relevant industry press, monitoring legislation, known changes to policies.

3. Review previous losses, events, incidents and identify anything useful from the lessons learnt reports.

Risks should not be assessed in isolation and a number of people may be involved in this process including other team or project members. You should use tools such as SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis to try to ensure all areas are covered. Appendix 2 also includes some risk descriptions applied to the Corporate Risk Register which can be used as a guide.

At this stage do not try to limit your thoughts or just roll forward the risks you have previously identified - it is important that you try to include fresh thinking on new and emerging risks every time a risk register is reviewed.

Each risk will be captured in a template on the Council's performance management system and will include:

- a refence number,
- short name
- a description,
- the name of the risk owner (the risk owner should be someone with knowledge of the risk and be senior enough to ensure that all actions are completed)
- the date the risk was first identified and
- the current controls
- Link to the Corporate Risk register reference
- Risk scores (gross, residual, risk appetite)

Written guidance has been created to assist risk owners on how to input risks into the Council's performance management system. In general terms the identification and wording of risks needs to be clear and concise. Risk writing should follow the model proposed by the Government's Orange book guidance for the management of risk. The Orange Book guidance for the management of risk defines risk as 'the effect of uncertainty on objectives' and states that it should usually be expressed in terms of causes, potential events, and their consequences. These are:

- **Cause**. An element which alone or in combination has the potential to give rise to risk.
- **Event**. An occurrence or change of a set of circumstances and can be expected which does not happen or something that is not expected which does happen.
- **Consequence**. The impact that could happen if the risk was to materialise.

If the risk is not adequately defined, it is difficult to demonstrate what actions might be needed to reduce the risk. For example the following risk statement :

"Users unable to use available technology" – is too broad and provides no information as to which technology, why there is a use issue ie is it inadequate training or is it because there is an issue with the technology which prevents users being able to use it? This could be several risks in one, each risk should be identified with the associated cause and consequence.

ii. Analyse, assess and evaluate risks.

Once the risks have been identified it is important to be able to prioritise them in some way so that attention and resources can focus on the areas most likely to have the largest impact on the delivery of the Council's objectives. In order to do this the risks are assessed against two criteria.

- Impact - this is the effect that the risk would have on the delivery of the Council's objectives if it were to occur.
- Likelihood - this is how likely the risk is to occur.

Once scores are calculated we can plot where the risk sits on the risk matrix and give the risk an overall score by multiplying the Impact and Likelihood scores

Impact x Likelihood = Risk Score. E.g. 4 x 3 = 12

The risk score is calculated twice once for the Gross Risk which is the worst-case scenario without any controls in place. The controls already in place to address the risk should then be recorded and the Residual Risk Score is calculated taking the effect of these into account. Finally all risks will be assessed against a target level based on risk appetite.

In order to assist with scoring, a scale for each of these has been determined and these are set out in the risk matrix above. As with the identification of the risks it is useful for more than one person to be involved in the scoring of the risks as this avoids the scoring being skewed by an individual's subjective view.

The way one person sees a risk may differ from another due to many factors including past experience, personal views on the importance of an area and how that person can personally influence the risk. When a group reviews the scores, these personal influences can be smoothed out.

iii. Review of controls and their effectiveness

By calculating both the Gross and Residual Risk Scores it highlights the effectiveness of the controls but also the importance of them operating effectively. Managers may believe a risk is being well managed, but the controls are not operating effectively.

It is therefore important that managers do take some time to assess the effectiveness of the controls that they have in place and make use of other information at their disposal to do this. This should be done at the time the risk register is being produced but also on an ongoing basis as the risk register is being reviewed.

There are many tools which operational managers should be using directly as part of their role as the 1st Line such as:

- Sample checking a sample of transactions to see they have followed the correct process/been properly authorised.
- Checking staff are aware of the correct processes to follow.
- 1 to 1s and monitoring of staff.

Managers can also make use of information from the 2nd Line functions to give them information relating to the effectiveness of the controls they have in place. Lots of information available to Managers can be considered as Key Risk Indicators (KRI) when used to inform the identification of risks and the success in the implementation of the agreed risk reduction methods. The following could be considered as Key Risk Indicators:

- Customer Complaints
- Data Protection Breach information
- Legal Compliance information
- Vacancy/Sickness data
- Performance Management Information
- Accident reports
- Budget Monitoring information
- Project issue logs
- Implementation Timelines - planned vs actual

Managers can also take account of the findings of Internal Audit work who provide assurance on the effectiveness of controls as the 3rd Line function.

iv. Response to Risk

Where a risk is found to be at a level that is unacceptable to the Council and outside of its risk appetite then some action is needed to address the risk. There are four main ways that the Council can respond to an unacceptably high risk:

- **Terminate** (avoidance)

  the Council can simply avoid the risk altogether where this is possible. So, if it is looking at a new development or project to implement but the risk is very high for little return then we should decide not to progress with that decision. Alternatively, we could decide to stop a high-risk activity that we are carrying out if we do not have to deliver that service. This should be the first response we look to; however, it is recognised that the Council is often not able to avoid high risk/undesirable activities.

- **Treat** (reduction)

  We can implement additional controls to reduce the likelihood an/or the impact of a risk to an acceptable level. This is the most common response to a risk that the Council will take. All controls/actions must be SMART actions and monitored through performance management.

- **Transfer**

  This involves transferring the cost of the risk to a third-party for example by insurance, contracting out work, or outsourcing the service. This can work in specific situations e.g., transfer a specific function such as Leisure provision or an insurance policy for vehicle damage in an accident, but unfortunately most business risks cannot be managed by this method.

- **Tolerate** (accept)

  The Council decides to accept the risk and do nothing. This may be acceptable for low risks but is often not an acceptable solution for the higher more significant risks so should be considered as a last resort option. When using this option, it will still be necessary to monitor and review the risk.

When making the decision on which of the options above you want to follow you should consider:

- Existing best practices to treat the risk.
- Critical controls that you will need to achieve the required risk score reduction as part of the risk treatment or mitigation plan.
- Costs associated with different treatment options against associated benefits.
- How other organisations mitigate the same risk.

Action Plan

Most of the options above require an action plan to be produced, this will need to include the following key information for each SMART action identified against the risk:

- The Action being taken.
- A person responsible making sure the action is completed.
- A target date for the action to be completed.

All actions must be recorded and updated on the performance management system..

Escalation of Risk

The change of a risk level within Departmental Risk registers may, if the risk level has become unacceptable escalate the corresponding risk on the Corporate risk Register. These escalating risks will be identified and reported through the Council's performance management system and highlighted to SLT and Audit Committee during quarterly review/report of the Corporate Risk Register.

Assessment of risk on individual projects or proposals which are scored above the council's risk appetite level should have been considered by statutory officers and appropriate controls identified prior to presenting such decisions to the relevant executive or non-executive decision makers.

v. Reporting, Monitoring and Communication

Risk Registers

The Council has developed a corporate template which should be used for all risk registers completed in relation to Council activities and partnerships. This can be found on the Council's performance management system.

To ensure consistency and compliance with the Council's Risk Appetite the Corporate Template **must be used** to record risks for the following mandated risk registers:

- Corporate Risk Registers (One for each Council)
- Departmental Risk Registers maintained by ~~the Heads of Service~~Managers
- Risk Registers for Major Projects (including Transformation Projects)
- Risk Registers for Contracts
- Risk Register for ICT and Cyber Threats

SLT will coordinate and collate the Corporate Risk Register with support from ~~Heads of Service~~managers who will be responsible for Departmental and other Risk Registers.

Due to limited resources the Risk Management function is unable to provide direct support to assist with the compilation and management of other risk registers but will offer advice and guidance to managers and other employees tasked with compiling them.

Risk Registers should be seen as an essential tool to aid in management decision making and should be recorded and reported to the appropriate bodies and meetings within the Council.

Corporate Risk Registers

This is the Council's overarching risk register setting out the most significant risks that may prevent the Council from achieving its strategic objectives as set out in the Gedling Plan.

The full Corporate Risk Register is compiled and monitored by SLT on a quarterly basis. This includes the Action Plans and progress against the actions.

A summary of the risks along with comments on the current position/progress in dealing with the risk is presented the relevant Audit Committee quarterly.

The Chief Executive will oversee the compilation of the Corporate Risk Registers and ~~Head of Finance & ICT~~s.151 Officer will collate management updates but is not responsible for the content of the Corporate Risk Register.

Where risks are escalated within Departmental or other Risk Registers, above a score of 12 (red) , these will be considered in line with the linked Corporate Risk and the Corporate Risk Register updated.

The Corporate Risk register template can be found at appendix 2 to this document.

Departmental Risk Registers

Each of the ~~Heads of Service~~Departmental managers or Assistant Directors will maintain a Departmental Risk Register which will set out the key risks for the whole service area, scoring of risks will be in line with this framework. It is anticipated that these will contain more risks than the Corporate Risk Register and should help to identify the highest risks which need to be considered for inclusion in the Corporate Risk Register.

The Departmental Risk Registers can include major risks not directly associated with the achievement of the corporate plan. It is anticipated that the Departmental Risk Registers will capture the most important risks relating to the major projects and contracts in each area as well as the key operational risks being faced relating to service delivery.

Departmental Risk Registers will be monitored by the relevant Director and their Heads of Service but can be shared with SLT for information purposes and to assist with the compilation and review of the Corporate Risk Register. They will not routinely be reported to Members or Committees.

Project Risk Registers

These must be completed at the planning stages and throughout the life of the project as part of project initiation through to delivery. The Project Manager is responsible for ensuring that a risk register is completed. The risk register should be updated regularly and monitored by the Project Board and Project Sponsor. The Risk register should be scored in line with this framework.

Where external Project Managers take on the role of compiling risk registers, they should be asked to use the Corporate Template and Risk Matrix, or approval must be sort in advance to use an alternative format. Where an external person/organisation takes ownership of the risk register for a project managers need to ensure it covers all of the risks and not just those the third party considers important. Where necessary a Council specific risk register should also be compiled for the project to ensure all risks are captured for example to include a risk that the third-party project manager fails to delivery to agreed specification/timescale. Managers should not look to delegate their role and responsibilities in the risk management process to a third party.

Key risk from Project Risk Registers may be escalated to Directorate Risk Registers and ultimately the Strategic Risk Register.

Contract Risk Registers

A risk register must be completed as part of the management of all strategically important contracts and partnerships. For example, acquisition of key software solutions, significant outsourcing contracts or contracts that support key functions of the Council. As a general guide contracts with a value in excess of £10,000 may require a risk assessment depending on their significance, contracts over £75,000 will require a risk assessment. They should be completed by the relevant Team Managers and monitored by the Head of Service.

The details in these risk registers should help to inform decision making in relation to the management and monitoring of the Contract/Partnership and should help to improve the quality of risk management implications when any committee reports are prepared in relation to the Contract/Partnership.

Key risks from Contract/Partnership risk registers may be escalated into the Directorate Risk Registers and ultimately the Corporate Risk Register.

ICT/Cyber Risks

A risk register must be completed to assess the Council's risk of cyber or ICT security issues. This should be completed by the ICT team and may be impacted by the acquisition of new software solutions.

The details in these risk registers should help to inform decision making in relation to the management and security of the Council's digital systems and networks and should help to improve the quality of risk management implications when any decisions are taken in relation to ICT infrastructure. In addition, the risk register will identify controls required or in place to manage such security risks.

Key risks from cyber risk registers may be escalated into the Directorate Risk Registers and ultimately the Corporate Risk Register. Details on this register are likely to be confidential and access restrictions to this register will be put in place to ensure any insecurities, if applicable are not placed in the public domain thereby increasing risk.

Risk Management Reports

When reporting and monitoring risk registers quarterly, it is important the following information is provided to the people/committee receiving the update:

- assurance that all exposure to risk has been identified, assessed and relevant mitigating control evaluated,
- Clear record of any SMART actions to mitigate risk and progress against those actions.
- a view on whether the exposure the risk is increasing or decreasing for the Council,
- links between different levels of risk registers where relevant,
- how the results of the risk management process are informing decision making,
- the risk management framework and in particular the risk appetite and scoring has been applied consistently across the Council.

Below the Corporate Risk Register it is more important that the risk registers are living documents, regularly monitored, and used to inform decision making by the relevant managers rather than being reported periodically as the focus of a detailed formal reports. They should be reviewed and updated on a quarterly basis as a minimum.

Risk Monitoring

There are two key elements for managers to consider when monitoring risks:

1. **Monitoring risk response effectiveness**

   As the Council and the environment it operates in is constantly changing, it is important to regularly review the risk register to ensure that the risks and agreed actions to mitigate them are still appropriate and being effective.

The use of Key Risk Indicators and the work of Internal Audit are tools that can help managers to monitor the effectiveness of risk responses.

2. Monitoring the risk profile

The Council's risk profile will be constantly changing with changes in the strategic direction of the Council and the impact of external factors such as Government policy, new initiatives, emerging issues. When monitoring the risk profile, it is always good to start with these three basic questions:

- Are there any risks missing from the risk register that should be included?
- Have any of the risks in the risk register changed significantly in terms of impact and/or likelihood and require additional mitigation efforts?
- Is there anything planned in the next 12 months that may give rise to a key risk?

vi. Integration with Strategic Planning and Decision Making

Risk Management and Strategic Planning are fundamentally linked, and it is impossible to carry one out effectively without the other. Strategic Planning is about deciding what the Council is trying to achieve in the medium to long term. Risk Management is about identifying the risks that may stop the Council from achieving those strategic goals.

Whilst it is important that risks are managed at all levels of the Council and for all activities we deliver; with limited resources it is important that the majority of the effort is targeted on the identification and management of risks that could affect the corporate objectives.

When taking decisions, officers and members need clear information about the risks associated with that decision so information about risks should be included in all decision reports.

SLT have a responsibility in ensuring decision reports with poor or missing risk implications do not progress.

Heads of Service should take responsibility for ensuring all reports in their Service area have appropriate risk implications set out before the report is submitted to SLT for review.

Appendix 2 - Corporate Risk Register Template

The risk category and descriptors are given as a prompt to help you to identify the operational risks in services and forms the basis of the Corporate Risk Register. The list is not exhaustive and is only a guide. In departmental registers you should also consider risks that are specific to your service area.

Many risk categories overlap and/or can be considered to be consequences of another category, however the risk category allocated should be based on the 'root cause' of the risk (e.g., an IT system failure may cause financial or reputational consequences but the 'root cause' lies within the IT / Technology category)

This is only a template, the risk registers will be held on the performance management system so may look slightly different in lay out but all information should be captured. At each quarterly review the risk escalation or de-escalation will be identified.

Risk Ref No	Corporate Risk	Descriptor	Gedling Plan Objective	Risk Owner	Key Risk driver	Gross Risk	Risk Appetite	Residual Risk	Controls
1	**Financial**	This refers to the ability of the Council to meet its financial commitments and/or the scale and pace of budget cuts. This relates to income and expenditure and							

		includes internal budgetary pressures, savings/growth considerations, external economic changes etc.							
2	**Capacity/Service Delivery**	This is about ensuring that sufficient capacity is available to deliver services which meet statutory obligations, Council objectives etc and public expectation.							
3	**Health and safety at Work**	This refers to Occupational Health & Safety							
4	**Environmental**	This refers to the environmental impact on the public – it could be related to virus type illnesses or environmental incidents such as flooding which impact on health or related to events which have an impact on the natural environment such as pollution/contamination							
5	**Contractual/partnership**	This refers to both the risks regarding							

		partnership / contractual activities and the risks associated with the partnership / contract delivering services to the agreed cost and specification.							
6	**Reputation**	This relates to public perception / expectation and the impact of media attention.							
7	**Infrastructure/Assets**	This looks at the loss, protection and damage of physical assets and takes into account the need to maintain, protect, insure and plan for unexpected loss.							
8	**Legislative**	This refers to changes to and breaches of current law leading to additional workloads, fines, intervention by regulatory bodies etc.							
9	**IT/Technology**	This relates not only to the impact of Internal technology failure but also changing technological demands							

		and the ability to meet the pace and scale of change.							
10	**Projects**	This relates to the effective management of projects to achieve delivery that is on time, to budget and that meet the needs of the organization.							
11	**Fraud/bribery/Misconduct**	Relates to improper actions committed against the Council either internally or by third parties. Including frauds, bribery, money laundering and misconduct e.g., theft, falsification of timesheets.							
12	**Service Standards/performance Management**	This relates to the setting of acceptable standards and levels of output for a service area and the processes put in place to ensure these are delivered and managed appropriately							
13	**Information/data**	Security – this relates to physical and IT security on site and in-							

		transit or inappropriate disclosure of information.							