Risk Management Strategy

Contents

Document history

Date	Key changes	Approved by
30.1.2024	Revised strategy	Strategy and Resources Committee

Approval of changes

Major changes	Extended Management Team (EMT) Strategy and Resources Committee
Minor changes	Extended Management Team (EMT)
Next update	February 2025

1. Introduction

All organisations, whether private or public sector, face risks to people, property and continued operations. Risk is the chance or possibility of loss, damage, injury, or failure to achieve objectives caused by an unwanted or uncertain action or event.

Risk management is the planned and systematic approach to the identification, evaluation and control of risk. Its objectives are to secure the assets of the organisation and to ensure the continued financial and wellbeing of the organisation.

While the Section 151 Officer has overall responsibility for the risk strategy, the Policy and Communications Team oversees the strategy and risk process. All senior officers must take responsibility for risk management and ensure there are regular reviews of risk.

The Strategy & Resources Committee is responsible for reviewing and approving the Risk Management Strategy.

2. Definition and purpose of risk management

Having a risk strategy is not about avoiding risk, but where possible limiting the likelihood and impact of anything which has the potential to influence the achievement of the corporate priorities. Following this approach enables us to consistently manage risk in accordance with good practice and embed risk management within strategic priorities, business planning, budgeting and reporting processes.

This will help prevent harm, either financial or reputational to the Council, its residents', officers, management, staff and stakeholders, as well as reduce the cost of risk.

Effective risk management ensures:

- We understand the nature of the risks we face - what could go wrong and how these can affect our ability to deliver our corporate objectives.
- We are aware of the extent of these risks - how likely they are to happen and the impact they could have.
- We identify the level of risk the Council is willing to accept.
- We can determine our response to each risk and whether we treat, tolerate, transfer, or terminate the risk.
- We put in place the necessary actions, controls and processes to implement the chosen response to each risk.
- We can do our best to prevent something going wrong and/or minimise the impact.
- We communicate our approach to risk management.

3. Objectives

This strategy's objectives are to:

- Provide staff, councillors and partners with guidance to ensure there is an effective, robust and consistent way of managing risk across the whole Council.
- Set out our approach to risk management and how risk will be identified, mitigated and monitored. This will improve the Council's ability to deliver the corporate priorities and improve outcomes for residents.
- Ensure staff are aware of and understand the risk strategy and the risk framework, as well as how these apply to their own roles and responsibilities.
- Ensure senior staff understand and manage the risks relating to their activities and the impact on the Council's key strategic risks.
- Provide assurance and support the Annual Governance Statement.

4. How we manage risk

We manage risk at three organisational levels, all with associated risk registers.

- **Corporate:** Strategic risks which impact the Council's ability to meet its strategic objectives or statutory duties, are recorded and monitored in the Corporate Risk Register. This is owned and approved by the Management Team and the Strategy and Resources Committee.

- **Committee:** Policy committee risk registers are managed and owned by the head of service for the relevant department and approved by members.

- **Departmental:** Operational risks which impact specific service areas are recorded and monitored in a departmental risk register. This is owned by the relevant head of service. Risks are escalated to the committee or corporate risk register where appropriate.

Programmes and projects have their own risk registers. These are monitored by the project manager and the project sponsor who will be a member of the Extended Management Team. Extended Management Team has oversight of all major projects and escalating risks are added to the departmental, committee or corporate risk registers as necessary.

Risk assessments are also carried out by service areas and these identify any risks which need to be added to the departmental risk registers. These risk assessments cover areas such as lone working, site visits for housing or planning officers, as well as some manual roles.

5. Risk management process

There are four stages in ensuring risks are properly managed and reduced to an acceptable level.

- Stage 1: Identifying risk
- Stage 2: Evaluation and assessment
- Stage 3: Response and action
- Stage 4: Monitoring and reporting

Stage 1: Identifying risk

It is critical we can identify any risks which could prevent the Council from achieving its corporate priorities. These risks can be internal, or external.

- Internal risks come from routine day to day activities such as managing staff, safeguarding, health and safety, financial challenges, or IT systems.
- External risks can have an adverse impact on activities, for example, a cyberattack or extreme weather conditions. External risks are harder to manage as we have less control over them, but we need to be able to anticipate them if possible and put in controls to mitigate their impact.

We need to be able to clearly describe the risk, its cause and effect. This is important when proposing new or significantly revising any projects, policies, or services. The following questions can help identify risks:

- What could prevent us from achieving this objective?
- What could realistically go wrong?
- What do we need to achieve this objective?
- Do we depend on others to succeed?
- What opportunities could arise?

Any identified risks should be recorded in the appropriate risk register so they can be evaluated. Types of risk are listed in Appendix A.

Stage 2: Evaluation and assessment

Once identified, risks need to be analysed, evaluated and prioritised. This helps us understand the threat posed by the risks identified and whether we need to take action to mitigate them.

We need to understand the impact in terms of cost, reputation, service delivery and the likelihood of the risk occurring.

To evaluate and assess risks we use a scoring matrix, based on the likelihood and impact of the risk should it occur. The greater the risk, the more effort required to manage it, where it is within our control and is best use of resources.

During this process, the risk rating will also need to be aligned to our risk appetite, which is set out in section 8.

To ensure risks are rated consistently, a 5 by 5 scoring matrix set out below, is used to assess the:

- **Impact:** This considers how severely the Council would be affected if the risk happens. The potential impact and/or consequences (before and after mitigation)
- **Likelihood:** This considers how likely it is the risk will occur and become an event which needs to be managed.

This initial scoring of risks is known as the inherent risk. This refers to the risk as it exists currently, ignoring any controls already in place to mitigate it.

Once any measures are put in place to manage the risk this is known as the residual risk.

Risk scoring matrix

	Impact				
Likelihood	Minimal	Minor	Moderate	Significant	Major
Will occur	**5**	**10**	**15**	**20**	**25**
Likely to occur	**4**	**8**	**12**	**16**	**20**
Could occur	**3**	**6**	**9**	**12**	**15**
Fairly unlikely	**2**	**4**	**6**	**8**	**10**
Unlikely	**1**	**2**	**3**	**4**	**5**

Risk score levels

High 15-25	Unreasonable level of risk exposure which requires constant active monitoring and measures to be put in place to reduce risk exposure.
Medium 7-14	Reasonable level of risk exposure, subject to regular active monitoring measures.
Low 1-6	Acceptable level of risk exposure subject to regular passive monitoring measures.

Likelihood guidance

- Will occur: The event is expected to occur in most circumstances.
- Likely to occur: There is a strong possibility the event will occur.
- Could occur: The event might occur.
- Fairly unlikely: Not expected, but there is a moderate possibility it may occur.
- Unlikely: Highly unlikely, but it may occur in exceptional circumstances.

Impact guidance

Below are some examples of types of risk and levels of impact.

Risk	Minimal	Minor	Moderate	Significant	Major
Health and Safety	Incident – no lost time.	Injury – no lost time.	Injury, lost time, short term sick absence.	Extensive, permanent, long-term injury or long-term sick.	Death or life threatening.
Service delivery	Short term service disruption.	Loss of service 1 day.	Loss of service 2 to 3 days. Affects single department.	Loss of service 3 to 5 days. Possible impact on vulnerable. Impact on property or non-vulnerable groups.	Loss of service more than 5 days. Impact vulnerable. groups. Affects whole Council.
Reputational	Minor adverse local publicity.	Negative local publicity.	Negative sustained local publicity.	Negative national publicity.	Negative sustained national publicity.
Environmental	Minimal impact.	Minor impact.	Moderate impact.	Serious damage.	Major damage.
Legal	Legal action unlikely.	Minor breach of duty.	Legal action possible. Moderate breach of duty.	Legal action expected. Material breach resulting in damages awarded against the Council	Legal proceedings issued against the Council
Financial	Can be managed within cost centre budget	Can be managed within Head of Service budget.	Can be manged within committee budget	Can be managed within corporate contingency	Cannot be managed within corporate contingency.

Stage 3: Response and action

Once the risk has been identified and its priority determined, the options for managing (mitigating) the risk to either stop it from arising or to minimise the impact should occur. This involves:

- Identifying any existing controls in place.
- Identifying what further controls are required. This will either involve improving existing controls or developing and implementing new ones.
- Accepting it is not possible to eliminate all risk and there are not reasonable mitigations available.
- Mitigating actions should either, minimise the likelihood of the risk event occurring, reduce the frequency or limit the severity of the event should it occur. Residual risk scores should only be reduced when the mitigation is in place.
- Progress in implementing the identified mitigations will be monitored and reported on a quarterly basis.

- The residual risk values need to be determined and recorded, with the controls identified in place.
- If the residual risk value (after mitigation) remains too high and exceeds the risk appetite, further controls need to be identified to ensure the risk is below the risk appetite. If this is not possible, a decision will need to be made about whether the activity can occur.

Once action has been taken to control or mitigate the risks, the next stage is to re-evaluate the impact and likelihood again using the same risk scoring matrix.

The managed risk score is referred to as the residual risk. This gives a better indication of whether the action taken to date is sufficient and if the overall score is within the Council's risk appetite (see Section 8).

Treat, tolerate, transfer, terminate categories
Other control techniques are also applied to manage the risk. These are tolerate, treat, transfer, terminate. The cost of managing risks should be understood and be proportionate to the risk being addressed. Resources should be prioritised to higher level risks that need active management.

- **Treat:** This is the most common way of managing risks. The purpose of treating the risk is to continue with the activity, but at the same time take action to bring the risk score down to a lower, more acceptable level.

- **Tolerate:** This means accepting the likelihood and consequences of the risk. You would typically take this approach when it is not cost effective to act, because the impact of the risk, should it occur is minimal, or not within your control.

- **Transfer:** This means shifting the risk, in whole or part, to a third party. The transfer of risk to another organisation can be used to reduce the financial exposure of the Council and/or pass the risk to another organisation which is more capable of effectively managing it.

- **Terminate:** This means stopping an activity altogether or doing things differently, so the risk is removed.

Stage 4: Reporting and monitoring

All information relating to an identified risk should be recorded in a risk register. As a minimum, this information should include:

- A title or description of the risk.
- The potential impact should it occur.
- The main controls in place to manage the risk.
- A summary of the actions and their progress.
- The risk rating (inherent and residual).
- Comments giving further information and updates on the management of the risk.
- The risk owner.

Each risk register should be reviewed and approved at the right level of management. This should:

- Ensure current controls are effective and do not require further planned actions.
- Ensure identified risks are still relevant and on the correct register.
- Re-assess risks when change happens or new information comes to light, such as new equipment, changes in legislation, or at the start of a new project or procurement.
- Review key project, procurement, contract management and partnership risks and risks which impact outside service areas. This can be when they require more corporate support, increase significantly in score and/or become more strategically important. These risks are escalated to the relevant committee risk register.

Risks are reported and monitored in the following ways:

- **Departmental Risk Registers** are reported to, discussed and reviewed at monthly departmental leadership team meetings. Any escalating risks are highlighted for discussion at Extended Management Team meetings. Following this they may be added to the policy committee or corporate risk registers.

- **Policy Committee Risk Registers** are reported to, discussed and reviewed by Management Team and Extended Management Team each quarter. Any escalating risks which have a wider or more critical impact are added to the Corporate Risk Register. At the end of each quarter the risk registers are reported to the four policy committees and Audit & Scrutiny Committee to provide an update about the Council's most significant risks and assurance about how they are being managed.

- The **Corporate Risk Register** is reported to, discussed and reviewed by Management Team each quarter. Any escalating risks which have a wider or more critical impact are highlighted in a quarterly report taken to the Strategy and Resources Committee to provide an update about the Council's most significant risks and assurance about how they are being managed.

In addition, Extended Management Team regularly discusses escalating risks and this can lead to the addition of risks to the policy or corporate risk registers.

Programmes and projects have their own risk registers. Extended Management Team has oversight of all major projects.

Identifying when a risk should be escalated is an important part of the monitoring process. There may be instances where further action to mitigate a risk cannot be taken by the current owner and it needs to be escalated, eg from the departmental risk register, or project and programme risk register to the corporate risk register.

Risk reporting should:

- Provide relevant, concise, but sufficient risk information which facilitates decision making and action.
- Ensure the views of the Extended Management Team or committee receiving the risk report are passed to the relevant risk owners.
- Focus on the most significant risks, ensuring adequate responses are put in place.

Few risks and risk registers remain static, they evolve over time: Risk characteristics, priorities and responsibilities change and actions get completed.

6. Roles and responsibilities

Responsibility and accountability for managing risk is assigned at different levels in the organisation. Heads of service are delegated responsibility for managing operational risks in their service areas, including those related to strategic priorities.

Each service manager and other risk owners are responsible for assessing the opportunities and threats to their service areas and projects and providing a comprehensive view of these risks.

Each risk is assigned an owner, who is responsible and accountable for the risk. This should be the person with the knowledge of the risk area and sufficient seniority to enable them to allocate resources to manage the risk and ensure actions required to treat it are completed. If the risk owner does not have budget responsibility, any request for resources will need to be escalated to EMT.

We have the following levels of risk owners.

Risk owners	Responsibilities
Committee level Councillors	• Understand the Council's risk management arrangements and corporate risks. • Approve and review the Risk Management Strategy. • Take reasonable steps to consider risk implications during decision making and policy approval. • Proactively participate in and be prepared in advance of committee meetings and hold risk owners accountable. • Ensure the work of policy committees and full council is conducted in accordance with Council policy and procedures for managing risk, with due regard for any statutory provisions set out in legislation.
Corporate level Chief Executive Director of Resources (S151 Officer) Head of Policy and Communications	• Overall responsibility for the Council's risk management performance. • Ensure the Council has effective and efficient risk management arrangements in place. • Ensure all decision making is in line with the policies and procedures for management of risk and any statutory provisions set out in legislation. • Adequate resources are made available for the management of risks facing the Council. • Management of risk performance is continually reviewed.
Corporate level Management Team (MT) Extended Management Team (EMT)	• Take a lead in understanding, identifying and analysing significant corporate risks and opportunities facing the Council in the achievement of key objectives. • Determine the approach to each risk and sets priorities for action to ensure they are effectively managed and reviewed and updated on a quarterly basis. • Identify, develop, manage and update the corporate risk register on a quarterly basis. • Ensure the risk management process is applied to all key and major decisions made by councillors using risk assessments, with all reports requiring decisions. • Is accountable for escalating/deescalating risks between the different risk registers. • Raises the portfolio of risk management, promoting the benefits to councillors and staff, ensuring everyone is aware of their responsibilities and accountabilities and has training. • Prepare performance and risk committee reports informed by EMT discussions.
Departmental level Key Officer Forum (KOF)	• Take primary responsibility for identifying and managing operational risks arising from service activities. • Manage operational risks on a daily basis and input into service and risk discussions. • Carry out risk assessments where appropriate as part of service and operational planning. • Monitor and maintain departmental risk registers. • Allocate mitigating actions to named staff, ensure they are completed. • Provide risk updates at EMT and KOF meetings. • Propose escalation and de-escalation of risks to EMT. • Reports for decisions include comprehensive risk management information to allow effective decisions to be made. • Understand and use the scoring matrix for identifying and assessing risks.

	• Ensure teams are aware of the risk assessments appropriate to their activity and staff undertake training.
Project risks Project managers	• Develop a project risk register using the scoring matrix. • Ensure these risk registers are closely monitored for all projects and throughout the project lifecycle. • Ensure identified mitigating actions are nominated to specific people and completed. • Evaluate and document any potential risk changes. • Decide whether escalation is necessary. • Work with the EMT to maintain the corporate risk register and to manage the risks identified. • Provide updates to committee, operational and corporate risk registers.
All staff	• Comply with the Risk Management Strategy for operational activities and processes. • Comply with mitigating actions identified to reduce risk. • Report potential hazards and risks which cannot be managed to line managers. • Support continuous service delivery and any emergency response. • Work safely to avoid putting themselves, others, or the organisation at risk.
Internal audit	• Provide assurance on the implementation of the Risk Management Strategy. • Ensure internal audits coverage is risk based, considering the risks identified within the corporate and operational risk registers. • Provide assurance about the robustness of the Council's management of risks. • Provide assurance about resilience.

7. Risk management training

Training is provided to staff to ensure they understand their roles and responsibilities, as well as develop their knowledge and understanding of risk management.

All staff involved in risk management will be invited to attend training annually, to ensure they are aware of and understand the fundamentals of risk management.

Managers will be responsible for ensuring their staff attend risk management training and records of training are kept.

8. Risk appetite

Risks must be assessed against the Council's risk appetite.

Risk appetite can be defined as the level of risk an organisation is willing to accept, tolerate, or be exposed to in pursuit of its objectives. This is used to set the maximum risk tolerance. This is the maximum level of residual risk the Council is willing to tolerate after controls and mitigating actions for strategic priorities.

We have adopted the government's guidance on definitions of risk appetite. These are set out in the table below.

Risk appetite may vary between services and activity and should be defined as part of service planning.

Risk appetite	Description
Averse (Very low risk)	Avoidance of all risk and uncertainty by selecting approaches with ultra-low levels of residual risk, with no expected reward or return. This will not result in a loss of reputation, credibility, or money. We would rather abandon projects and initiatives than assume risk.
Minimal (Low risk)	Preference for safe options with limited potential for reward or return with a minimal level of residual risk. We accept risk is unavoidable, but will minimise risks as much as possible. All reasonable steps will be taken to manage the risk.
Cautious (Medium risk)	Choice of safe delivery options offering some modest potential for reward and return which have low levels of residual risk. Actions unlikely to result in a loss of reputation or credibility. Possibility of limited financial loss.
Open (High risk)	Willing to consider all options and choose one most likely to be successful while providing an acceptable level of benefit. Innovation supported if clear benefits demonstrated, we are confident in success and steps taken to reduce the risk.
Eager (Very high risk)	Eager to be innovative and to choose options based on maximising opportunities and potential higher benefit even if those activities carry a very high residual risk.

9. Risk governance assurance

Risk management is a key part of the Council's governance arrangements and the Risk Management Strategy supports the Council's compliance with statutory requirements. Councils must review risk management annually. The Annual Governance Statement, which is part of the annual statement of accounts, details the effectiveness of risk arrangements. The Annual Governance Statement also identifies any significant governance issues which may have resulted from failures in governance and risk management. Risk governance is demonstrated by the following:

- Roles and responsibilities for risk management as set out in Section 6.
- Risk integrated with decision making. Committee reports must include an outline of key risks, along with information about how they are to be managed.
- Risk is embedded at all levels, as in the various risk registers detailed under Stage 4.
- Risks and risk management arrangements are widely discussed at EMT meetings.

In addition to the above, there are several other specific duties the Council is obliged to observe such as responsibilities arising from the Civil Contingencies Act 2004, Health and Safety at Work Act 1974 and equality impact assessments under the Equality Act 2010.

10. Review of risk management

Regular review of risk management needs to be carried out to ensure it is effective and making improvements where necessary.

The service planning and budgetary process is used to set objectives, agree action plans, and allocate resources. Progress towards meeting objectives and the risks inherent in achieving those objectives are monitored regularly. Risk registers provide regular reports about the progress being made in managing risk. This ensures significant risks are identified and evaluated and emerging risks can be added.

Risk management is a continuous and developing process. This is reflected in the annual review of the risk management policy and the implementation of recommendations arising from reviews of risk management arrangements by the internal auditor.

A - Types of risk

Political: These risks include the influence of the external political environment, such as changes in UK government policies which impact the Council, national strikes/fuel shortages, grass roots activism and political criticism. Risks that influence the political priorities of the Council and could lead to failure to deliver.

Economic / Financial: These risks could impact on the ability of the Council to meet its financial commitments or result in a failure to meet expected returns on investment. It covers both internal budgetary pressures, external macro level economic changes and risks associated with insufficient or non-compliant reporting. Examples include cost of living crisis, interest rates, inflation, budget overspend, investment failures, reserve depletion.

Reputational: This is anything which damages public perception of the Council. This could be failure to meet stakeholder expectations as a result of any event, behaviour, action or inaction, either by the Council, our employees or any third party we are associated with.

Social: These risks arise from not meeting social needs as a result of changes in demographic, residential or socio-economic trends. These risks could lead to a loss of credibility or trust from the community. Examples could include housing supply shortages and failure to meet housing needs, decisions or actions involving treatment of people, staff levels from available workforce; not meeting the needs of an ageing population, not being prepared for bringing all people along when changes occur.

Technology: Risks arising from the use or ineffective use of technology resulting in the inadequate delivery of services whether the failure is due to system, process, or performance. It also includes breaches of data security or system integrity, as well as the capacity of the Council to deal with technological advancements and changing demands. Examples include IT infrastructure; staff needs, security standards, digital poverty, and lack of access to digital services.

Legal/Compliance: These risks are related to legal challenges and being subjected to litigation including non-compliance with legal frameworks whether that is in regard to employment, delivery of statutory services, etc. It includes risks from changing national and international regulations which threaten the Council's operations and processes, data protection breaches and failure to comply with health and safety regulations.

Security risks: Risks arising from a failure to prevent unauthorised and/or inappropriate access to the estate and information, including cyber security and non-compliance with General Data Protection Regulation requirements.

Environmental/ Climate Change: These risks arise from the impact of council services. Risks should be identified from both current operations and projects about how they might impact the environment in terms of resilience to extreme weather (flood defences, drought resistance), the wider context of contributions to climate change (carbon emissions etc) and the ability to adapt to future needs of the population.

Partnership/Contractual: Risks arising from failures of partners or contractors and weaknesses in the process for management of joint ventures and commercial endeavours including supply chains. Examples include contractor fails to deliver; partnership agencies have no common goals, insufficient return on investment, service failure, lack of cost control.

People: Risks arising from ineffective leadership and engagement, suboptimal culture, inappropriate behaviours, the unavailability of sufficient capacity and capability, industrial action and/or non-compliance with relevant employment legislation/HR policies resulting in negative impact on performance.

Project and Programme: Risks which change programmes and projects not aligned with strategic priorities and do not successfully and safely deliver requirements and intended benefits to time, cost and quality.