APPENDIX I

Risk Management

POLICY STATEMENT AND STRATEGY

Document Details:

Owner/Lead Officer	: Head of Internal Audit & Assurance Service, Corporate Resources Department
Created	: January 2026
Review Arrangements	: Annually
Next Review Date	: January 2027
Ratified by	: Chief Officers (Annually)

Contents

Risk Management Policy Statement

1. Local government in the UK will begin to plan for significant changes starting in 2026. The Government is currently reviewing numerous councils' business cases with the outcome of replacing all two-tier county and district councils with single tier unitary authorities. It also has ambitions to devolve powers across England by implementing Mayoral Strategic Authorities (MSA). Unlocking devolution will allow better alignment to public services, boost economic growth and place funding and powers closer to residents to empower communities. Reforms will have a significant impact on every community and will result in fundamental change to councils creating many risks but also significant opportunities.

2. Despite the Government outlining principles for funding reform, stressing allocations were based on robust analysis and demand drivers, last minute unexpected post-consultation changes at the end of November 2025 redirected funds to urban councils at the expense of rural areas, despite updated assessments showing county regions have the greatest increase in needs. This change in approach was confirmed when the provisional Local Government Finance Settlement for 2026/27 was published on 17 December 2025, with the decision to continue the Recovery Grant to a limited number of authorities being detrimental for Leicestershire. The provisional settlement also failed to offer enough clarity to councils on how rising demand for SEND and historic deficits will be funded and what this means for their long-term financial stability. Significant cost and demand pressures also persist in children's and adult social care and home-to-school transport. Councils face ongoing uncertainty, high service demand, and budget challenges through 2026 and beyond, raising widespread concerns about short- to medium-term sustainability and their ability to meet statutory duties.

3. The Council's four-year Strategic Plan agreed in May 2022, was refreshed to set out its revised long-term vision and priorities to 2026. The Council is continuing to operate in an extremely challenging financial climate. Whilst the proposed next four-year MTFS forecasts a balanced budget for 2026-27 (after use of £23m earmarked reserves), significant gaps remain in the following three years.

4. Local authorities that foster effective risk management and aim for a 'no surprises' culture are better positioned to meet objectives, sustain services, deliver value for money, and uphold good governance with stakeholders. Robust risk management balances protection from harm with openness to calculated risks and opportunities. While new complexities and risks will emerge, they also create chances for innovation, collaboration, transformation, community engagement, and new approaches to service delivery.

5. While protecting the most vulnerable, the Council promotes a risk-aware culture that encourages creativity and innovation. Risks are identified, understood, and proactively managed rather than avoided. Risk management is central to the Council and its partners, enabling it to meet current community needs and prepare for future challenges

6. This Policy Statement and Strategy provide an integrated framework for effective risk management. It assures stakeholders, partners, and customers of a consistent approach to managing risks and opportunities across all activities, aligned to and supporting delivery of the Council's Strategic Plan, its other plans, strategies and related programmes.

7. This Policy Statement and Strategy are fully supported by Chief Officers, who are committed to embedding risk management across the Council. Its success depends on the cooperation of all managers and employees to ensure effective use of resources. The Policy and Strategy will be presented to the Corporate Governance Committee (the Committee) and Cabinet as part of the MTFS.

Leicestershire County Council Risk Management Strategy

1.0 Defining Risk and Risk Management

Leicestershire County Council (the Council) has adopted these definitions of risk and risk management from the ISO31000:2018 'Risk management – guidelines' which are applied in the Association of Local Authority Risk Managers (ALARM) 'Risk management tool kit 2021':

Risk is defined as:
The effect (positive or negative) of uncertainty on objectives.

Risk Management is defined as:
Coordinated activities to direct and control an organisation with regards to risk

By managing risk effectively, the Council will be in a better position to safeguard against potential threats and make the most of potential opportunities to and retain and improve services and continue to provide value for money.

This Risk Management Strategy outlines how the Council will use risk management to successfully deliver corporate, departmental and service objectives and priorities.

2.0 Why undertake risk management?

Statutory requirements

Part 2 of the Accounts and Audit Regulations 2015 (Internal Control) places explicit requirements on the Council around risk: -

- Paragraph 3 (c) - the Council must ensure that it has a sound system of internal control which includes effective arrangements for the management of risk;
- Paragraph 4.4 (a - iii) – the Responsible Financial Officer (the Director of Corporate Resources) must determine, on behalf of the Council financial control systems which must include measures to ensure that risk is appropriately managed;
- Paragraph 5 (1) the Council must undertake an effective internal audit to evaluate the effectiveness of its risk management processes.

Local (external) audit requirements

Under the Local Audit and Accountability Act (2014) the Council's local (external) auditor (currently Grant Thornton LLP) is required to satisfy itself that the Council has made proper arrangements for securing economy efficiency and effectiveness in the use of its resources i.e. its value for money arrangements. As part of its work on governance arrangements, the auditor considers how the council monitors and assesses risk and gains assurance over the effective operation of internal controls including arrangements to prevent and detect fraud.

Constitutional requirements

The County Council's Constitution (revised 5 December 2024), Part 3: 'Responsibility for Functions' contains several references to risk management.

- Section B: Responsibility for "County Council" functions – Corporate Governance Committee (the Committee).
    - The functions delegated to the Committee shall be all those non-executive functions relating to the promotion and maintenance of high standards and integrity within the Authority in relation to governance, risk etc
    - Committee Terms of Reference – Section 2: Governance & Risk1&2
        - 2. 5 - To review and monitor the effective development and operation of risk management in the Council including the Council's risk management framework.
        - 2.6 - To review and make recommendations to the County Council on the Council's Risk Management Policy Statement and Strategy.
- Section D: General scheme of delegation to Chief Officers
    - 5(h) that any exercise of delegated powers by officers, shall have identified and managed appropriate strategic and operational risks within the officer's area of responsibility

[1] These align to the oversight of risk management arrangements as being a core function of a local government Audit Committee as referred to in CIPFA's Guidance on Audit Committees 2022.

[2] The Council's Local Code of Corporate Governance (2022) complies with the 'Delivering Good Governance in Local Government; Framework' (2016), specifically Principle F which advises that good governance is promoted when there is management of risks and performance through robust internal control and strong public financial management.

Leadership Behaviour requirements

Risk management is a central part of the Council's strategic management principles. It is the process whereby managers methodically address risks with the goal of achieving sustained benefit within their own activity and across the portfolio of all activities. The focus of good risk management is the identification and treatment of these risks. Specifically, the Leadership Behaviour 'Think' (taking the time to reflect and analyse) sets expectations for experienced and strategic managers to make informed decisions based on evidence, available information and data, reflecting and evaluating the team's work and performance to make continuous improvements where required.

Management should evaluate risks and opportunities that will improve their service and manage those accordingly, and regularly horizon scan to understand the likely impact on their service, forward planning, weighing up any risks and making future decisions accordingly.

3.0 Benefits of risk management

Risk management is a tool that forms part of the governance system of the organisation. When applied appropriately it can bring multiple benefits - taken from the ALARM 'Risk management tool kit 2021':

Improved operational efficiency	Better delivery of intended outcomes	Maximised opportunities
Reputation protection	Achievement of the organisation's objectives	Reduced losses from workplace accidents and illnesses
Better mitigation of key risks	Demonstration of good governance	Enhanced political and community support
Protection of budgets from unexpected financial losses or increased ability to secure funding	Increased effectiveness of change projects and programmes	Protection of assets
Enabling risk taking in chosen areas	Improved management information to inform decision making and planning	Setting the desired risk culture

4.0 Risk Management Strategy objectives

The objectives of the Council's Risk Management Strategy are to:

- Fully embed risk management into the Council's culture and service planning processes, to support achievement of objectives.
- Ensure there is an effective framework for consistently identifying, assessing, managing/mitigating, reviewing, reporting and communicating risks across the Council.
- Improve the communication of the Council's approach to and importance of risk management.
- Improve the coordination of risk management activity across the Council.
- Ensure Chief Officers, Members, the Committee, and external stakeholders have assurance that the Council is mitigating risks to achieving key priorities and complying with corporate governance standards.
- Manage risk in accordance with best practice and ensure compliance with statutory requirements.
- Maintain clear roles, responsibilities and reporting lines for risk management within the Council.
- Measure and partake in regular comparison and benchmarking activity.

5.0 Risk Appetite and Risk Tolerance

The Council recognises that only by taking risks can it achieve its aims and deliver beneficial outcomes to its stakeholders.

The Institute of Risk Management (IRM) defines risk appetite as, “the amount of risk an organisation is willing to take in order to meet its strategic objectives”. A range of appetites exist for different risks, and these may change over time.

The IRM defines risk tolerance as, “the boundaries of risk taking outside of which the organisation is not prepared to venture in the pursuit of its strategic objectives”.

Risk appetite and risk tolerance help an organisation determine what high, medium, and low risk is. In deciding this, the organisation can:

- More effectively prioritise risks for mitigating actions
- Better allocate resources
- Demonstrate consistent and more robust decision making
- Clarify the thresholds above which risks need to be escalated in order that they are brought to the attention of senior management and/or Members.

Risk Appetite Statement

Chief Officers collectively agree the Council operates in a high-risk environment which is likely to persist. This requires defining acceptable risk levels (high, medium, low) by impact and likelihood, enabling prioritisation and proportionate actions aligned to decisions and service impact.

The Council will take risks in a controlled manner, reducing exposure to a level deemed acceptable. In order to take advantage of opportunities, the Council will support innovation and the imaginative use of resources. However, the Council will seek to control all highly probable risks which have the potential to:

- Cause significant harm to service users, staff and the public.
- Severely compromise the Council’s reputation.
- Significantly impact on finances.
- Significantly impact on the environment.
- Jeopardise the Council’s ability to undertake its core purpose.
- Threaten the Council’s compliance with law and regulation.
- Create opportunity for fraud and corruption or inadvertent loss through error.

Taking the above into consideration, the Council's current **overall** risk appetite is defined as **'Open'**, meaning it is prepared to consider all delivery options and choose those with the greatest potential benefits, even where risks are higher. Appetite varies by activity: greater risk may be accepted to support innovation, while compliance and public confidence in the Council require a cautious approach. Specific risk appetites can be adjusted with appropriate approval by appropriate officers and/or Members. Overall, the Council may need to accept proportionately higher risks to address growing financial challenges.

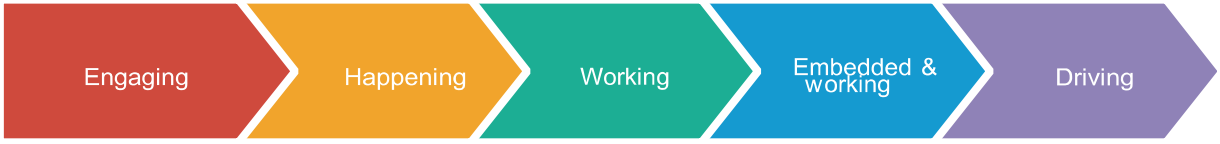
The Council will review risk appetite and tolerance annually to ensure risks are being managed adequately. **Annexes 1 and 2** provide further details.

6.0 Risk Management Maturity

All organisations are on a risk management journey with differing levels of risk management maturity. Risk management maturity refers to how well-established risk management is as a discipline across the organisation.

The Council continues to review its current risk management capability to help it direct resources in the areas that need improvement and further development, ensuring the risk management arrangements remain fit for purpose in this changing environment.

ALARM has developed and published a National Performance Model for Risk Management in Public Services (2016) to illustrate what good risk management looks like in a public service organisation. There are 5 levels.



An independent objective review of the Council's risk management arrangements by the Council's previous insurers, considered that the work undertaken by the Council further strengthened its position in respect of risk management standards and practices, thus increasing the likelihood of it attaining the higher grading of 'risk management is embedded and working' (level 4).

The Council has new insurers, and it is intended to arrange for their risk management team to undertake a further independent review. Pending planning with the insurer for an external evaluation, the outcome of an objective internal audit scoped, 'To evaluate how effectively Leicestershire County Council identifies, assesses, manages, and monitors risks that could impact its strategic goals, operations, and overall stability' is awaited, and recommendations for improvement will be considered.

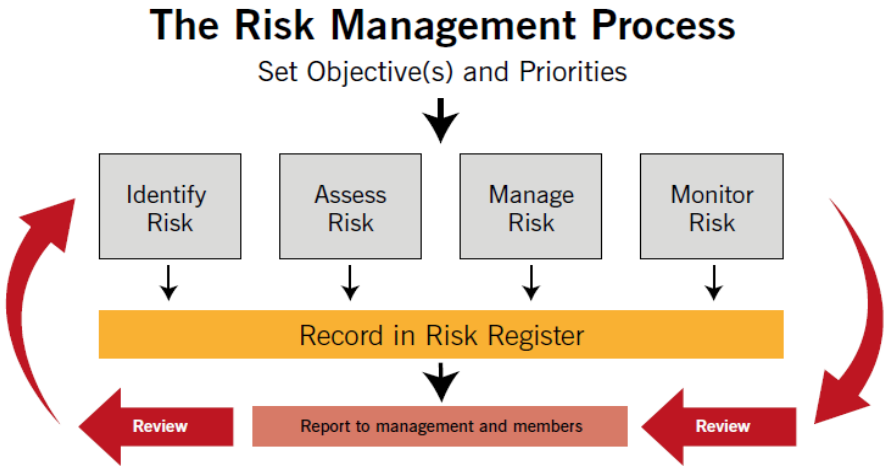
In its report on the Council's Value for Money arrangements for 2024-25, Grant Thornton stated that the Council has reasonable arrangements to manage strategic risks with a Risk Management Policy Statement and Strategy in place. The Committee holds responsibility for risk management and is informed of changes to the Corporate Risk Register (CRR).

The Auditor did not make any improvement recommendations on risk management arrangements.

The Council also networks and shares information with other similar organisations e.g. East Midland Risk Management Group (Six County Councils, five City/Borough/District Councils) which enables the Council to benchmark its position.

7.0 The Risk Management Approach and Process

Risk management is a continual process involving the identification and assessment of risks, prioritisation of them and the implementation of actions to mitigate both the likelihood of them occurring and the impact if they did. Risks and issues require different responses. Risks require proactive controls and issues require active resolutions. A risk is a potential future event. It is something that could happen, but it has not yet occurred. An issue is a problem that has already happened or is currently happening. The Council's approach to risk management will be proportionate to the decision being made or the impact of the risk, to enable the Council to manage risks in a consistent manner, at all levels.



Explanations of the stages within the risk management process:

Identify risk	A mixture of: - • Review existing registers - Has the impact or likelihood of any of the risks recorded changed significantly? Are any risks missing from the risk register? • Review outputs from independent service reviews e.g. inspections, audits • Clarify objective(s) and priorities from the Service Planning process and identify risks (or opportunities) which might prevent, delay (or alternatively escalate) achievement of objectives. Determine what are the consequences if this occurs.

	• Monitor local and nationwide developments considering the nature of emerging risks, threats and trends • Review relevant national reports, technical briefings, specialists and guidance.
Assess risk	Assess the inherent risk (Impact & Likelihood) using the Council's risk assessment criteria prior to the application of any existing/known controls i.e. evaluate the "Original risk score"
	• Decide and agree the course of action (5T's) i.e. tolerate (accept) treat (mitigate), transfer, terminate or take the opportunity.
Manage risk	Identify and assess the controls/actions already in place to mitigate each risk to arrive at the "Current Risk score". If Current Risk score is still high even with controls: • Is the scoring correct? • Determine the best way to manage the risks – apply the 5Ts . • Determine whether the cost of implementing further mitigating control is merited when compared to the risk reduction benefits achieved. • Develop SMART actions (i.e. specific, measurable, attainable, relevant and time-bound) and assign target dates and responsible officers to achieve the desired "Target Risk score".
Monitor, Review and Report	Use the Risk Management Matrix and Risk Tolerance levels to determine the frequency of review, monitoring, risk escalation and reporting.

Annex 2 provides details of the risk measurement criteria, risk map, risk escalation and reporting arrangements.

8.0 Application - Service, Department, Corporate & Specialist Risks

Risk management supports good governance by assuring stakeholders that risks are effectively managed. It is embedded in the Council's corporate departmental business planning process to identify and address key risks across services. Escalation provides senior management with a clear view of risks, enabling informed decisions on resource allocation and areas of concern.

There is an established framework in which consistent application of the process should ensure the flow of appropriate risk information across the Council as follows:

Service and Department Risks

The Council's Risk Management Strategy requires identifying risks linked to service or departmental priorities and defining mitigating actions. All new service/business plans must include a risk assessment, with significant risks logged in the Departmental Risk Register.

Heads of Service are responsible for identifying risks arising from their service plans assessing likelihood and impact using the Risk Matrix, recording risks where necessary, and ensuring accountability for actions within set timescales. Departmental Risk Champions provide support for risk identification and assessment.

Corporate (and high scoring Departmental) risks - Corporate Risk Register (CRR)

This process will provide Chief Officers and Members with a central record of corporate risks, to ensure consideration is given to high scoring, strategic cross cutting (or Departmental) risks that could impact the financial, political or reputational arena.

- Following a timetable set for The Committee meetings, Departmental Risk Champions and management teams will review Department Registers to identify and consider risks for escalation to the CRR, either individually or consolidated from Departmental Risk Registers.
- The Internal Audit Service will confirm that the reviews have been consistently undertaken, provide a level of challenge to the outcomes and co-ordinate the production and reporting of the CRR, through to Chief Officers and ultimately to The Committee.
- Whilst most risks are expected to come through this route it might not capture all of the strategic risks facing the Council. Therefore, horizon scanning, information from relevant publications and minutes from key meetings will also provide a basis for including additional risks on the CRR.
- A more detailed update of the CRR (providing additional information on current and further controls/actions on how the risks are being mitigated), is presented annually to the Spring Committee.

9.0 Specialist areas of risk management

Local Government Reorganisation risks

The Government is scheduled to announce before the summer parliamentary recess, its decision on reorganisation to the two-tier systems of local government in Leicestershire. Within the County Council's proposal, under the section 'Detailed Options Analysis' the risks (and benefits) of the three main options have been assessed against the Government's criteria (High Quality and Sustainable Public Services, Finance, Unlocking Devolution, Stronger Community Engagement and Neighbourhood Empowerment and Effective Representation and Governance Structure. Before the outcome is known, work

will be expected to start addressing the impact of reorganisation on the Council's financing and resources, priorities, service provision, governance arrangements and staffing. A compendium of strategic and operational risks will be developed potentially using the experiences of previous reorganisations and any tools/guidance provided for example by the Ministry of Housing, Communities and Local Government (MHCLG), the Local Government Association (LGA) https://www.local.gov.uk/publications/lgr-risks-examples-and-options-mitigation-councils

Project, Programme and Portfolio Risks

Risks affecting project or programme objectives will be managed by the relevant Project or Programme Board. Where these risks impact strategic or departmental objectives, they should be assessed and, if necessary, escalated to the appropriate Departmental, Portfolio, or Corporate Risk Register. The decision to escalate rests with the Senior Responsible Officer (SRO) or Sponsor, supported by the Project or Programme Board.

To complement the corporate strategy, the Transformation Unit is developing and embedding detailed guidance and practice to ensure consistent and effective management of the Strategic Change Portfolio's exposure to risk which is essential to the successful delivery of change and realisation of benefits.

Project or programme closure reports must identify risks or issues to be transferred to Business as Usual (BAU), with clear ownership assigned. Where appropriate, these risks should be escalated to the relevant Departmental or Corporate Risk Register

Partnerships

Risks which could impact on achieving the partnership's objectives will be managed through the appropriate Partnership Board and associated governance structures. However, where partnership risks impact upon strategic or departmental objectives then consideration should be given as to whether those risks should be identified, assessed, and escalated to the appropriate Departmental or Corporate Risk Register. The Council's approach for identifying, assessing and managing risk within partnerships will continue to be developed.

Health, Safety & Wellbeing Risks

The Health, Safety & Wellbeing Service provides advice and guidance to managers and staff on all aspects of Health, Safety and Wellbeing. In addition to providing advice and support, the Health, Safety & Wellbeing Service also helps to monitor the performance of the organisation through audits and inspections, set targets for continual improvement, provide operational training and awareness for staff and also respond to accidents/ incidents in order to ensure they are adequately investigated, and the likelihood of further harm is reduced. In addition to this there is an employee counselling service.

Regular reports are provided to the Departmental Management Teams, the Chief Executive, Chief Officers, and the Council's Employment Committee. A separate risk assessment process is in place.

In 2024, new mandatory health and safety training and new and updated Occupational Health and Safety Management System (OHSMS) guidance was published. The revised guidance places a stronger emphasis on proportionate health and safety management. A revised Policy Statement was approved in September 2024. In 2025 a new 5 year health and safety strategy was approved.

Resilience and Business Continuity

Business Continuity Management (BCM) complements the Council's risk management framework and is required under the Civil Contingencies Act 2004. BCM focuses on the impact of disruption, identifying priority services and what is needed to maintain obligations. It ensures plans are in place to protect people, premises, technology, information, supply chains, stakeholders, reputation, and essential services.

The Resilience and Business Continuity Team coordinates continuity and response plans at corporate, departmental, and service levels to minimise disruption by prioritising critical functions and defining resources, roles, and responsibilities. The resilience element addresses incidents requiring multiagency coordination when BCM alone is insufficient.

The team reports annually to the Corporate Governance Committee.

Risk Financing

Risk financing is the process of deciding how an organisation will pay for loss events in the most effective and least costly way. It balances retaining and transferring risk, manages the financial impact of retained risk, and typically involves internal funding or external insurance (such as catastrophe cover from the Council's insurers).

The goal is to ensure the organisation has sufficient resources to continue its objectives after a loss. Risk financing includes identifying risks, selecting financing methods, and monitoring their effectiveness. Options include self-insurance and commercial insurance, with the choice depending on the organisation's size, financial position, risk profile, and objectives.

Under normal circumstances the Council is largely self-insured but transfers the larger risks to insurance companies by contributing premiums. In the event of a financial loss, the Council is entitled to indemnity, subject to the terms and conditions that are in place. However, not all risks can be insured e.g. service demand and these need to be managed by the Council

The Insurance Policy is revised annually, presented to the Committee in January and then to Cabinet in February to support the MTFS. The Insurance Service presents an annual report to the Committee in September.

Property and Occupants Risk Management

Following the Grenfell fire and 2017 terrorist attacks, the Council formed a corporate group to review fire safety in the Council's owned and procured properties and later broadened its scope to include its identification and management of terrorism and marauder risks. The

group meets quarterly, includes representatives from across services, and works closely with insurers, brokers, and emergency services

Terms of Reference are reviewed annually against other property groups to avoid duplication or gaps. The group reports to the Director of Corporate Resources, to Chief Officers as required for any significant issues, and to the Committee annually.

A decision will be required on what role the group may take in a Protect and Prepare Group which could be established to meet the requirements of ACT for Local Authorities (an initiative led by Counter Terrorism Policing to support local government partners to embed counter terrorism considerations into their day-to-day work).

Counter Fraud

The Internal Audit Service conducts a biennial Fraud Risk Assessment (last approved December 2024), informed by national and local intelligence. This process grades fraud risk areas, identifies emerging threats, and guides the Council's Anti-Fraud and Corruption Strategy and resource allocation. Outcomes also shape the internal audit plan. New legislation and regulations are reviewed for potential fraud impact. An annual report is provided to the Committee on counter fraud and related initiatives.

Information & Technology (I&T) and Data Protection Risks

A safe and secure I&T infrastructure underpins the working of the Council, both technically and in terms of data protection. To support this, IT & Digital Services holds and maintains its own divisional risk register which, where appropriate will feed through to the Departmental and Corporate Registers. Regarding data protection, the Information Governance Team develop, maintain and monitor compliance with a wide range of policies designed to protect information and data.

Regarding the ever-increasing threat to cyber security, the Council has an established Technical Security function (headed up by the Technical Security Officer) that sits within the Architecture and Compliance Team. This function takes responsibility for identifying emerging threats and risks, maintaining the cyber risk register and planning, and monitoring ongoing activities to continually improve the council IT Security posture. The Officer reports to the Information Security Governance Group (ISGG) which is a forum for cyber security policy, risk, strategy and best practice. The ISGG also plays a key role in ensuring the organisation secures Public Services Network (PSN) compliance and its annual PSN certificate, which is necessary for maintaining access to central government and agency information systems.

To support the Technical Security function in delivering its objectives, the implementation of technical controls and operational management aspects of cyber security and governed by the IT Security Operations Group (ITSOG). The group meets fortnightly to discuss emerging cyber security concerns and ultimately aims to implement security solutions and improvements which align to LCC cyber security roadmap – the aim ultimately to strengthen the council's cyber posture.

Externally, active threats are shared with other councils through Warning, Advisory and Reporting Points (WARPs) and guidance is taken from the National Cyber Security Centre

(NCSC). Arrangements are in place with an independent security specialist to provide an incident retainer service. Cyber security is integrated into the corporate risk management process.

During 2026, the Council will self-assess against the Government's Cyber Assessment Framework.

Climate Change Risks

The Climate Change Committee (CCC) was established under the Climate Change Act 2008 and advises the UK on reducing emissions and adapting to the impacts of climate change. The CCC publishes an Independent Assessment of UK Climate Risk. Every five years, the Government publishes its Climate Change Risk Assessment (CCRA) which endorses and summarises the CCC's assessment, sets out the overall government approach, responds to the priority risks identified and produces a National Adaptation Programme.

Officers refer to the CCC's Independent Assessment of UK Climate Risk and the CCRA to identify high priority risks relevant to the Council. Officers have identified three groups of services based on their key functions in relation to climate and weather-related risks. Following the last CCRA in 2022 (next due 2027) a comprehensive review and risk assessment exercise was completed. 8 high risks and 56 medium risks were identified. Recommendations included working with service areas to develop action plans to mitigate identified high risks and developing a Climate Adaptation and Resilience Strategy and Action Plan for the area.

The 2024-25 Environmental Performance Report shows that six high risks remain on the climate change register, down by two since the 2022 assessment. The identified risks relate primarily to highways and property assets, business continuity and flood risk.

Due to capacity issues, to date it has not been possible to undertake significant work to address the other climate change risks. However, the Council's Cabinet agreed in October 2025 to allocate £2m of funding (reallocated from the earmarked reserve for carbon reduction) towards a programme of flood mitigation and climate adaptation and resilience measures, including resource to update the climate risk register and identify measures that can form a realistic action plan.

Support

The above processes will be supported by the following:

- Ownership of risks (at appropriate levels) assigned to Chief Officers, managers and partners, with clear roles, responsibilities and reporting lines within the Council.
- Incorporating risk management into corporate, service and business planning and strategic and partnership working.
- Use of the ALARM Risk Management Toolkit throughout the Council
- Providing relevant training on risk management to officers and Members of the Council that supports the development of wider competencies.
- Learning from best practice and continual improvement.

- Seeking best practice through inter-authority groups and other professional bodies e.g. ALARM.

10.0 Risk Management Roles and Responsibilities - structure

The following structure is unique to the Council and is influenced by its risk management maturity, resource capacities, skill sets, internal operations and existing operating structures. The Council's risk management framework aligns to existing structures and reporting lines. **Full details** of risk management roles and responsibilities can be found in Annex 3.

Leadership	Corporate	Departmental	Assurance Services
Cabinet Lead Members Chief Officers	Corporate Governance Committee (CGC) which includes 2 Independent Members who provide an external perspective Corporate Risk Management Group (CRMG)	Department Management Teams (DMT) Heads of Service Programme/ Partnerships Risk Champions Staff	Risk Management* Internal Audit Governance

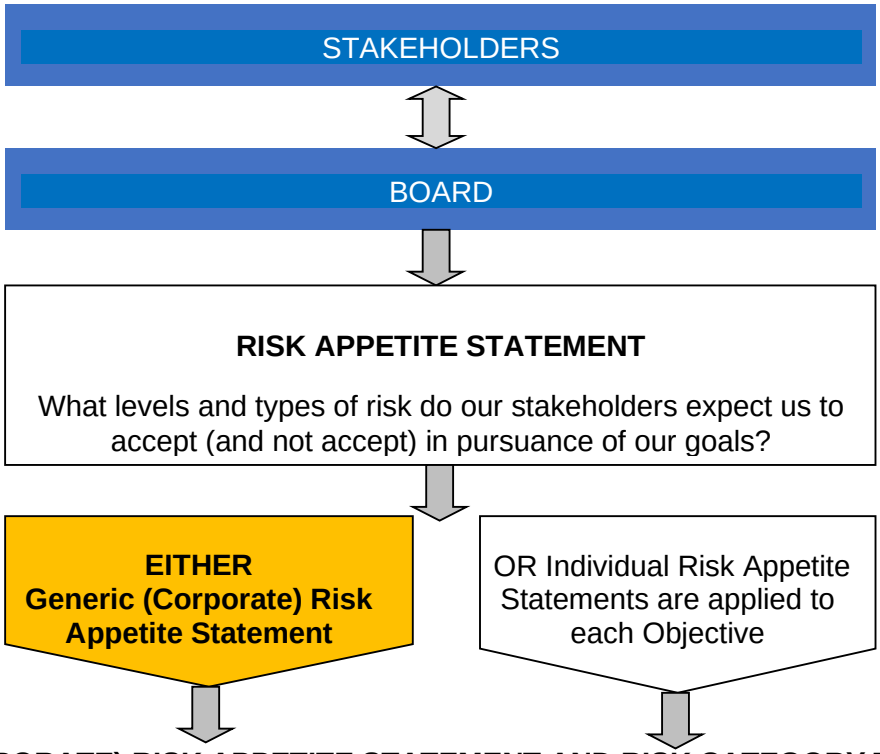
***** ThThe Head of Internal Audit & Assurance Service (HoIAS) is responsible for the administration and development of, and reporting on, the Council's risk management framework (RMF). Revised Global Internal Audit Standards (GIAS) were implemented into local government from 1 April 2025. The GIAS UK (public sector) require that this 'impairment' to independence and objectivity is recorded in the Internal Audit Charter (re-approved by CGC in November 2025) and (to avoid any conflict of interests) any audits of the RMF are overseen from a manager outside of the Service.

11.0 Continuous Improvement

Regulators and risk management professionals advise that it is good practice to continuously improve risk management methodologies in line with recommendations from regular assessments and adapt to changing economic conditions.

To this effect, the Council's Risk Management Policy and Strategy and related documents will be reviewed at the specified frequency or after the release of new legislation or government guidance that affects risk governance, internal controls, financial management or the regulatory regime for public service organisations. They will also be reviewed following the results of any audit /review by Internal Audit Service or an external third party.

Annex 1 – Risk Appetite



GENERIC (CORPORATE) RISK APPETITE STATEMENT AND RISK CATEGORY TYPES

AVOID	No appetite. Not prepared to accept any risks.	**Risk Categories Examples**: Health & Safety, Business Critical systems, Customers, Safeguarding, Data Security, People, Climate Change /Extreme Weather
AVERSE	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.	
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.	Delivery partners, Non - critical systems,
MODERATE	Tending always towards exposure to only modest levels of risk in order to achieve acceptable, but possibly unambitious outcomes.	
OPEN	Prepared to consider all delivery options and select those with the highest probability of productive outcomes, even when there are elevated levels of associated risk.	Leadership; Devolution; Growth and Infrastructure Collaboration; Alternative delivery models; Integration; Transformation; Digital; Commercial trading, Property investment, Suppliers.
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.	

Annex 2 - Risk Impact Measurement Criteria

Scale	Description	Department Service Plan	Internal Operations	People	Reputation	Impact on the Environment	Impact from*[1] the Environment	Financial per annum / per loss [1]
1	Negligible	Little impact to objectives in service plan	Limited disruption to operations and service quality satisfactory	Minor injuries	Public concern restricted to local complaints	None or insignificant damage		<£50k
2	Minor	Minor impact to service as objectives in service plan are not met	Short term disruption to operations resulting in a minor adverse impact on partnerships and minimal reduction in service quality.	Minor Injury to those in the Council's care	Minor adverse local / public / media attention and complaints	Minor local impact	Minor damage	£50k-£250k Minimal effect on budget/cost
3	Moderate	Considerable fall in service as objectives in service plan are not met	Sustained moderate level disruption to operations / Relevant partnership relationships strained / Service quality not satisfactory	Potential for minor physical injuries / Stressful experience	Adverse local media public attention	Moderate local impact	Moderate damage and risk of injury	£250k - £500k Small increase on budget/ cost: Handled within the team/service
4	Major	Major impact to services as objectives in service plan are not met.	Serious disruption to operations with relationships in major partnerships affected / Service quality not acceptable with adverse impact on front line services. Significant disruption of core activities. Key targets missed.	Exposure to dangerous conditions creating potential for serious physical or mental harm	Serious negative regional criticism, with some national coverage	Major local impact	Major damage and risk to life	£500-£750k. Significant increase in budget/cost. Service budgets exceeded

5	Very High/ Critical	Significant fall/failure in service as objectives in service plan are not met	Long term serious interruption to operations / Major partnerships under threat / Service quality not acceptable with impact on front line services	Exposure to dangerous conditions leading to potential loss of life or permanent physical/mental damage. Life threatening or multiple serious injuries	Prolonged regional and national condemnation. Serious damage to the reputation of the organisation i.e. front-page headlines, TV. Possible criminal, or high profile, civil action against the Council, members or officers	Major regional or national impact.	Wide scale damage and risk to life	>£750k Large increase on budget/cost. Impact on whole council

[1] Note that a different financial rating is used for the pension fund investments

Risk Likelihood Measurement Criteria

Rating Scale	Likelihood	Example of Loss/Event Frequency	Probability %
1	Very rare/unlikely	EXCEPTIONAL event. This will probably never happen/recur.	< 20%
2	Unlikely	Event NOT EXPECTED. Do not expect it to happen/ recur, but it is possible it may do so.	20-40%
3	Possible	LITTLE LIKELIHOOD of event occurring. It might happen or recur occasionally.	40-60%
4	Probable /Likely	Event is MORE THAN LIKELY to occur. Will probably happen/recur, but it is not a persisting issue.	60-80%
5	Almost Certain	Reasonable to expect that the event WILL undoubtedly happen/recur, possibly frequently.	> 80%

Risk Scoring Matrix

Impact

5 Very High/Critical	5	10	15	20	25
4 Major	4	8	12	16	20
3 Moderate	3	6	9	12	15
2 Minor	2	4	6	8	10
1 Negligible	1	2	3	4	5
	1 Very Rare/Unlikely	**2 Unlikely**	**3 Possible**	**4 Probable/Likely**	**5 Almost certain**

Likelihood

Risk Tolerance/Reporting Criteria

Tolerance Levels	**Current Risk Score**	**Expected Actions by Risk and Action Owners**	
White	1 to 2	Controls	No action required
		Monitoring =	No action required
		Escalation =	No action required
Low	3 to 6	Accept Risk or Maintain Controls	Existing controls may be sufficient. No additional controls are required unless they can be implemented at very low cost (in terms of time, money, and effort). Actions to further reduce these risks are assigned low priority.
		Monitoring =	Review six monthly
		Escalation =	Service/Area manager
Medium	8 to 12	Maintain Controls or Further Controls to reduce rating	Controls required but consider in light of 5 Ts- Consideration should be as to whether the risks can be lowered, where applicable, to a tolerable level, but the costs of additional risk reduction measures should be taken into account (time, money and effort).
		Monitoring =	Continued Proactive Monitoring/Review at quarterly / Reporting to DMT
		Escalation =	Business Partners / Relevant AD / DMT
High	15 to 25	Further Action/Controls to reduce rating	Controls and further actions necessary. Substantial efforts should be made to reduce the risk. Arrangements should be made to ensure that existing controls are maintained. The risk reduction measures should be implemented within a defined period.
		Monitoring =	Continued Proactive Quarterly Monitoring / Report to CGC
		Escalation =	Chief Officers /Lead Member

A Departmental risk with a current risk score of 15 or more **must** be escalated to Chief Officers (either as an addition to the Corporate Risk Register, or as an emerging risk for further debate). Risks with a current risk score of 15 will still appear on Department's registers but should only be excluded from the Corporate Risk Register after debate and approval from Chief Officers.

Annex 3 – Risk Management Roles & Responsibilities - Detail

Leadership:

Cabinet

Understands the key risks facing the Council, determines the level of risk and ensures risk management is delivered to mitigate risks by:

- Ensuring that a risk management framework has been established and embedded.
- Approving both the Council's Risk Management and Insurance Policy Statements and Strategies as part of the Medium-Term Financial Strategy.
- Ensuring relevant risk considerations (if relevant) are included within reports which may have significant strategic policy or operational implications.

Lead Members

- Responsibility for gaining an understanding of the risks facing their area of accountability (in conjunction with the relevant Director/Chief Officer) and periodically reviewing how these risks are being managed.

Chief Officers

Leading and ensuring effective management, monitoring and review of risk management across the Council by:

- Establishing a control environment and culture in which risk can be effectively assessed and managed.
- Directing the level of risk, the Council is prepared to accept (appetite and tolerance levels).
- Encouraging the promotion of risk awareness, rather than risk avoidance.
- Reviewing and, approving the Council's corporate and strategic risks on the CRR quarterly and their importance against the Council's vision and priorities.
- Taking the role of Transformation Delivery Board in managing Portfolio Level risk.
- Taking the role of Crisis Management Group in managing any significant responses
- Assisting with the identification of significant new and emerging risks as they become known - for consideration and addition to the CRR.
- Following the review and approval of the CRR, to determine whether a potential reputation or consultation matter needs to be forwarded to the Communication Unit.
- Providing challenge to the risk scoring mechanism to ensure risks are managed by balancing undermanaging risks (unaware and no control) and over-managing them (over-control).
- Ensuring their respective portfolio lead members are regularly briefed on departmental (and corporate) risks.
- Ensuring that risk assessments (if appropriate) are detailed in Cabinet or Scrutiny reports upon which decisions are based.

- Reviewing annually both the Council's Risk Management and Insurance Policy Statements and Strategies.

Corporate:

Corporate Governance Committee (CGC) including Independent Members

Provides assurance for the Council that risk management is undertaken and effective by:

- Reviewing the effectiveness of the risk management and internal control framework.
- Reviewing the Council's Risk Management Policy Statement & Strategy and how it is being implemented.
- Receiving regular progress reports on the CRR and other risk management related initiatives.
- Reviewing, scrutinising and challenging the performance of the Council's risk management framework; including reviewing progress against planned actions from the previous quarter.
- Receiving presentations on specific areas of risk.
- Receiving reports from Internal and External Audit to determine the extent to which they indicate weaknesses in control, risk management and governance arrangements.

Corporate Risk Management Group (CRMG) via Departmental Risk Champions

Provides assurance that the risk management framework and its processes are working as intended and are effective by:

- Acting as the main contact for their department and its management on risk matters (including specialist risks (H&S, Insurance etc.).
- Representing their department at the Corporate Risk Management Group.
- Encouraging the promotion of risk awareness, rather than risk avoidance.
- Assisting in the implementation of any revisions to the risk management framework and promoting use of the Risk Management Toolkit.
- Providing coaching, support and advice on risk management to Chief Officers, Heads of Service and other managers within their service/department.
- Providing support to the other departments' Risk Champions.
- Maintaining on behalf of their Chief Officers, a departmental risk register that complies with corporate guidelines.
- Providing regular risk updates to DMT's as per the agreed reporting criteria and risk timetable.
- Providing challenge to the risk scoring mechanism to ensure risks are managed to add value by aiming to achieve the balance between undermanaging risks (unaware and no control) and over-managing them (over-control).
- Ensuring that corporate risk information and requirements are communicated to their department.

- Assessing the relevance of corporate, other departmental service, programme, project and partnership risks and their impact on their department.
- Reviewing cross cutting risk areas where risks of one department impacts on the risks of another.
- Providing overview and scrutiny to the results of the Fraud Risk Assessment process, in relation to departmental risks.
- Providing regular updates to the Internal Audit Service for corporate risks to enable reporting to the Chief Officers and the Committee.

Departmental:

Departmental Management Teams (DMT)

Ensuring that risk management is implemented in line with the Council's Risk Management Strategy by:

- Appointing a Risk Champion for the department and authorising them to progress effective risk management that adheres to corporate guidelines, across their services.
- Ensuring that risk management is integrated within the annual service planning process.
- Taking full ownership of risks within their departmental risk register and agreeing risk mitigation actions, with defined timescales and responsibilities – including those departmental risks that are also in the CRR.
- Reviewing and challenging risk registers for their Service Areas on a quarterly basis if appropriate.
- Adhering to the corporate risk reporting timetable so that DMT meetings and risk monitoring tasks are aligned.
- Ensuring that the CRR accurately reflects only those key strategic risks facing the Council. The DMT scrutiny process should encompass a review of all departmentally identified corporate risks (new and those already identified), to critically evaluate the following:
    - Whether the risk is an ongoing corporate risk
    - Are all mitigating actions identified? Are they SMART (i.e. specific, measurable, attainable, relevant and time-bound)? Are they working adequately or are additional actions necessary?
    - The current risk score (Impact and Likelihood) is accurate and is not 'over-scored' in terms of likelihood particularly if a range of current controls have been identified as embedded and working adequately
    - Only consider any further actions/additional controls after determining whether any cost of implementing further mitigating control is merited when compared to the risk reduction benefits achieved. If required, further actions should also be SMART and record 'expected timeframe/due date' which should improve the robustness of the target risk impact and likelihood scores
- Receiving reports on risk management activity and review key risks regularly.

- Undertaking regular departmental horizon scanning for new or emerging risks, ensuring communication of these through appropriate channels and incorporation within the Departmental Risk Register if appropriate.
- Suggesting recommendations for the removal of current corporate risks that are considered as lower levels of risk.
- Taking ownership of identifying and managing project, partnership and business as usual risks effectively, and escalating risks to the Portfolio, Departmental or Corporate risk register where appropriate.
- Ensuring that risk management considerations are included in all Cabinet, Scrutiny and Regulatory bodies reports in respect of strategic policy decisions.
- Providing assurance on the effectiveness of risk management within their department as part of the Annual Governance Statement process.
- Following the review and approval of the Departmental Risk Register, DMTs to determine whether a potential reputation or consultation matter needs to be forwarded to Communication Unit.

Heads of Service

Providing assurance to DMT's that risks within their service are being managed effectively by:

- Ensuring that risk management within their area of responsibility is implemented in line with the Council's Risk Management Strategy (i.e. identify, assess, manage and monitor).
- Managing risks on a day-to-day basis.
- Adhering to the risk scoring mechanism (original, current and target risk scores) outlined in the Strategy to ensure risks are managed to add value by aiming to achieve the balance between undermanaging risks (unaware and no control) and over-managing them (over-control).
- Communicating the results of their service risk assessment to the DMT via their Risk Champion, demonstrating effectiveness of controls in place to mitigate/reduce service risks.
- Managing risks from their areas of responsibility that have been included within the departmental risk register. Where further actions/additional controls are necessary, ensure they are completed by the planned completion date.
- Identifying new and emerging risks or problems with managing known risks and escalating to the Risk Champion where appropriate.
- Assessing fraud risk within their service areas as part of the Fraud Risk Assessment process.
- Ensuring that they and their staff are aware of corporate requirements, seeking clarification from their Risk Champions when required.
- Identifying risk training needs of staff and informing this to Risk Champions.
- Using the Risk Management Toolkit and guidance.

Programme/Project/Partnerships

Providing assurance that project, programme and partnership risks and their impact are managed and communicated effectively by:

- Ensuring risk management is a regular item on Partnership/Programme/Project Board agendas.
- Reviewing and monitoring risks identified on programme/project/partnerships risks, ensuring that suitable controls are in place and working, or that plans are being drawn up to strengthen existing controls or put in place further controls.
- Identifying new and emerging risks or problems with managing known risks, ensuring communication of these through appropriate channels.
- Escalating appropriate Project, Programme or Partnership risks to the relevant Departmental Portfolio, or Corporate Risk Register where those risks may impact at a Departmental, Portfolio or Corporate level – ultimately the project or programme SRO/Sponsor is accountable for ensuring this happens.
- Ensuring any ongoing risks or issues identified at Project/Programme closure are transferred to the relevant business owner and where appropriate are escalated to Departmental or Corporate Risk Registers.

Risk Champions

- See Corporate section

Staff

- Taking responsibility for gaining an understanding of the risks facing their area of accountability.
- Report promptly perceived failures in existing control measures that could increase risk.
- Take due care to understand and comply with the risk management processes and guidelines of the Council.

Assurance Services

Risk Management function (in conjunction with the Director of Corporate Resources):

Provide assurance that the flow of risk information throughout the Council is working and effective to produce and maintain the Corporate Risk Register by:

- Leading in the development and implementation of the risk management framework and promoting use of the Risk Management Toolkit.
- Meeting with departments as per the risk management timetable to review and challenge risk registers and emerging risks.
- Identify any potential future internal audit requirements to the Head of Internal Audit & Assurance Service.
- Coordinating risk management activity across the Council with the support of Departmental Risk Champions/Representatives.

- Collating the changes to departmental risks and ensure that the Corporate Risk Register is amended to reflect current position.
- Regular scanning (in conjunction with Chief Officers, DMT Risk Champions and the Head of Internal Audit & Assurance Service) of information from relevant publications and minutes from key meetings to provide a basis for including additional risks on the Corporate Risk Register.
- Reporting progress on the Corporate Risk Register and other risk management related initiatives to the Chief Officers, the Committee and Cabinet as per the risk management timetable.
- Supporting Departmental Risk Champions/Representatives in their risk management role.
- Communicating corporate risk management information and requirements.
- Reviewing the Risk Management Policy Statement and Strategy at least annually to reflect best practice and initiate improvements.
- Arranging for the review of risk management maturity; benchmarking scrutiny and challenge.

•Establishing links with external groups and organisations to gain knowledge and share best practice on risk management issues.

- Agreeing mechanisms for identifying, assessing and managing risks in key partnerships.
- Supporting the development and delivery of relevant risk training.

Assurance function (Internal Audit Service)

Review and challenge the effectiveness of the risk management framework, providing independent assurance about the quality of controls that managers have in place, by:

- Creating a risk-based audit plan that is aligned wherever possible to the Corporate Risk Register and the Departmental Risk Registers and other drivers, e.g. biennial Fraud Risk Assessment.
- Testing and validating existing controls, with recommendations for improvement on identified control weaknesses.
- Reporting outcomes to Directors and the Committee.
- Monitoring changing risk profiles based on audit work undertaken, to adapt future audit work to reflect these changes.
- Conduct relevant audits of the risk management framework and maturity but overseen by a manager independent to the Service.
- Take account of any commentary/improvements recommended by the External Auditor in its annual review of Value for Money arrangements.

Annex 4 – Action Plan

This Strategy sets out the developments/actions the Council proposes over the short-term future to further improve risk management maturity. These developments include the following actions:

Action	Frequency	Target Implementation Date
To review and revise the Council's Risk Management Policy Statement and Strategy and related guidance with endorsement from Chief Officers and the Committee.	Annual	23 January 2026
Encourage DMTs and Risk Champions to re-align Risk Registers to their 2026-27 business planning objectives.	Annual	March/April 2026
Update and communicate through Manager's Digest, the Council's intranet Risk Management pages to include: - • Revised Risk Management Policy & Strategy • All relevant guidance on methodologies and processes, including the revised Risk Assessment Criteria and Map • Who to contact and details of the risk management "network", • Links to further information and guidance e.g. ALARM website	Annual	February 2026
Review findings and recommendations from objective internal audit undertaken. Plan to implement any actions e.g. risk appetites for individual risk categories, identifying and managing risks and issues separately	One off	February 2026
Arrange an independent Risk Maturity Assessment and implement an Action Plan to address any recommendations	Triennially	c/f - Spring 2026
Develop options for Collaboration Office 365 space by Department for updates to Departmental Risk Registers.	Ongoing	c/f – Spring 2026
Work with ALARM and the East Midlands Regional Group to develop guidance for identifying and managing new & emerging risks	Quarterly	As part of EMRMG meetings.
Introduce and continuously develop key performance indicator(s) for risk management activity to maintain and improve the maturity rating.	Ongoing	c/f – Summer 2026
Develop a training matrix to define required training levels by role. Consider delivery options (e.g., face-to-face, external courses) and review training offered by the Council's insurance providers.	Ongoing	c/f – Summer 2026
Develop E Learning for Risk Management	Ongoing	c/f – Summer 2026

Action	Frequency	Target Implementation Date
To review and revise the Council's Risk Management Policy Statement and Strategy and related guidance with endorsement from Chief Officers and Corporate Governance Committee.	Annual	24 January 2025
Encourage DMTs and Risk Champions to align Risk Registers to their 2025-26 business planning objectives.	Annual	April/May 2025
Update and communicate through Manager's Digest, the Council's intranet Risk Management pages to include: - Revised Risk Management Policy & Strategy All relevant guidance on methodologies and processes, including the revised Risk Assessment Criteria and Map Who to contact and details of the risk management "network", Links to further information and guidance e.g. ALARM website	Annual	February 2025
Arrange an independent Risk Maturity Assessment and implement an Action Plan to address any recommendations.	Triennially	c/f to Spring 2025
Develop options for Collaboration Office 365 space by Department for updates to Departmental Risk Registers.	Ongoing	c/f to Spring 2025
To liaise with ALARM and East Midlands Regional Group to develop and implement guidance to ensure new & emerging are identified and managed	Quarterly	As part of EMRMG meetings.
Introduce and continuously develop key performance indicator(s) for risk management activity to maintain and improve the maturity rating.	Ongoing	c/f to Summer 2025
Develop a training matrix to identify the levels of training that need to be attained by staff at different levels in the organisation. Explore differing options e.g. Face to face, external training. Explore training offering from the Council's Insurance providers.	Ongoing	c/f to Summer 2025
Develop E Learning for Risk Management	Ongoing	c/f to Summer 2025