North Northamptonshire Council

Risk Management Policy and Strategy

February 2024

www.northnorthants.gov.uk

Document Version Control

Author (Post holder title): Chief Internal Auditor
Type of document: Policy and strategy
Version Number: 0.1
Document File Name:
Issue date:
Approval date and by who (CMT / committee):
Document held by (name/section): Rachel Ashley-Caunt, Chief Internal Auditor
For internal publication only or external also?: Both
Document stored on Council website or Intranet?: Both
Next review date: February 2025

Change History

Issue	Date	Comments
0.1	2nd May 2023	Draft for Audit and Governance Committee review and approval

NB: Draft versions 0.1 - final published versions 1.0

Consultees

Internal	External
Corporate Leadership Team	

Distribution List

Internal	External
Corporate Leadership Network	

Links to other documents

Document	Link
Corporate Plan 2021-25	Corporate Services - CORPORATE-PLAN--ADOPTED-BY-FULL-COUNCIL-01122021-.pdf - All Documents (sharepoint.com)

Contents

1. Foreword

1.1. The Council's vision statement for North Northamptonshire is: "*A place where everyone has the best opportunities and quality of life*." In order to achieve its vision and corporate objectives, the Council's leadership must be alert to the risks and opportunities that are posed in achieving those objectives. Decision making should be informed by this risk awareness and enable the management of risks as effectively as possible, whilst ensuring valuable resources are targeted in a prioritised and proportionate manner.

1.2. The Council's leadership is committed to effective risk management and see it as a key part of the Council's responsibility to deliver effective public services to the communities within North Northamptonshire.

1.3. There is a shared commitment to embedding risk management throughout the organisation, promoting a positive risk culture and making it a part of everyday service delivery and decision-making. This includes fostering an environment that embraces openness, supports integrity, objectivity, accountability and transparency in the identification, assessment and management of risks, welcoming constructive challenge and promoting collaboration, consultation and cooperation. We must invite scrutiny and embrace expertise to support decision-making, invest in the right resources and seek to continually learn from experience.

1.4. We seek to implement sound management of our risks and the threats – and, indeed, opportunities that flow from them. This places us in a stronger position to deliver our organisational objectives, provide improved services to the community, achieve better value for money and demonstrate compliance with the Local Audit and Accounts Regulations. Risk management will, therefore, be at the heart of our good management practice and corporate governance arrangements.

1.5. Effective risk management should enhance strategic planning and prioritisation, assist in achieving objectives and strengthen our ability to be agile to respond to the challenges faced. To meet our objectives, improve service delivery and achieve value for money for the residents of North Northamptonshire, risk management must be an essential and integral part of planning and decision-making.

Chair of Audit & Governance Committee Chief Executive

2. Introduction and scope

2.1. The aim of this Risk Management Policy and Strategy is to support the delivery of organisational aims and objectives through effective management of risks across the Council's functions and activities - applying appropriate risk management processes, analysis and organisational learning.

2.2. This document is aligned with the Council's key organisational strategies and plans and underpins the risk management framework. It explains the Council's approach and outlines the principles of risk management, as well as clarifying risk management roles and responsibilities across the Council.

2.3. This policy applies to all of the Council's core functions. Where the Council enters into partnerships the principles of risk management established by this policy and supporting guidance should be considered as best practice and applied, where possible. It is also expected that any significant contractors have risk management arrangements at a similar level, which should be established and monitored through commissioning processes and contract management arrangements.

2.4. This document and the risk management framework is informed by the Cabinet Office publication Management of Risk: Guidance for Practitioners; the HM Treasury publication "The Orange Book: Management of Risk – Principles and Concepts"; and the UK implementation of the international standard for risk management BS ISO 31000: 2018.

2.5. There are different but aligned risk management processes that are applied at various levels within the organisation. Risk specialists are embedded across the organisation in areas such as Health and Safety; Treasury Management; Emergency Resilience and Business Continuity; Insurance; Information Security and Governance; Counter Fraud etc. These specialist risk areas each have their own policies, procedures and processes that are built into the governance arrangements of the Council so that work is coordinated within the Council's overall risk management framework.

2.6. Risk is defined under BS ISO 31000:2018 Risk Management Guidelines as "The effect of uncertainty on objectives". The effect can be positive, negative or both and can address, create or result in opportunities and threats. Risk is usually expressed in terms of causes, potential events, and their consequences. A cause is an element which alone or in combination has the potential to give rise to risk. An event is an occurrence or change of a set of circumstances and can be something that is expected which does not happen or something that is not expected which does happen. Events can have multiple causes and consequences and can affect multiple objectives. The consequences are the outcome of an event affecting objectives, which can be certain or uncertain, can have positive or negative direct or indirect effects on objectives, can be expressed qualitatively or quantitatively, and can escalate through cascading and cumulative effects.

2.7. Risk management is defined as: "Co-ordinated activities to direct and control an organisation with regard to risk".

3. Policy and strategy outcomes

3.1. It is important to recognise that the Council is not seeking to eliminate all risk. This would not be a cost-effective use of scarce resources and as a body responsible for delivering statutory services, some risks simply cannot be eliminated. The Council will seek to manage risk in a proportionate manner relative to the severity of the risk.

3.2. It is the responsibility of the Audit and Governance Committee "to monitor the effective development and operation of risk management and corporate governance throughout the Council". Internal Audit will support the Committee in its role in providing a source of assurance over the Council's internal control framework and its effectiveness and adequacy.

3.3. Information and assurances from Internal Audit, and from other sources, will be used to inform recommended changes to the policy and framework at least annually. Any changes will be presented to the Audit and Governance Committee for approval before publication.

4. Risk Management Policy and Strategy

Context

4.1. The operating environment for local government has become increasingly challenging over the past decade, in terms of growing and complex service demand, additional statutory requirements and increasing public expectations, all set against a backdrop of local government funding restraint. This continuing trend requires greater collaboration, system-wide planning and a strong understanding of risk across public services.

4.2. The context specific to North Northamptonshire Council brings further challenges in the delivery of services as a recently established unitary authority, following vesting in April 2021. The continuing development of the unitary council must take place whilst managing the legacy risks, issues and opportunities arising from the former district, borough and county council services and the challenges of implementing cross-cutting systems and single, consistent processes and controls.

4.3. Furthermore, the impacts of the coronavirus pandemic and wider, major social and economic impacts have fundamentally changed the risk environment in which the Council operates. The macro-economic environment may remain volatile, complex and ambiguous for a number of years. The risks arising in this environment will often have no simple, definitive solutions and will require whole-system-thinking, aligned incentives, positive relationships and collaboration, alongside relevant technical knowledge, to support multi-disciplinary approaches to their effective management.

4.4. The operating environment will also require the Council to continually review its risk appetite, not only to ensure the right balance is struck between risk, innovation and opportunity, but to consider how much control can be exerted over risks, many of which cannot be directly mitigated by the Council alone.

4.5. In the context of continual and fast-paced change, elected Members will need to make challenging policy and budgetary decisions, while maintaining a longer-term view. As such, officers will need to provide the right balance of evidence, insight, advice and understanding of risk and opportunity.

Objectives and approach

4.6. In support of the Council's governance and internal control arrangements and achievement of North Northamptonshire Council's objectives, the Council is committed to:

- Managing risk in accordance with good practice and sound governance principles;
- Embedding effective risk management into the design, values and culture of the Council;
- Integrating the identification and management of risk into policy and operational decisions;
- Proactively anticipating and responding to changing social, economic, political, environmental, legislative and technological requirements that may impact on delivery of objectives;
- Eliminating or reducing negative impacts, disruption and loss from current and emerging events;
- Harnessing risk management to identify opportunities that current and emerging events may present and maximise benefits and outcomes;
- Managing risks in line with risk appetite;
- Promoting openness and transparency in risk management processes; and
- Raising awareness of the need for risk management by all those connected with the Council's delivery of services.

4.7. The Council will achieve these aims by:

- Integrating risk management practices into the Council's decision making, business planning, performance and management activities, particularly focusing on robust analysis, scrutiny and evaluation of mitigating controls and further actions;
- Providing a risk management training and development offer for both officers and elected Members;
- Embedding risk management arrangements within major change activities across the Council and developing an integrated approach to their assurance;
- Reviewing the Council's risk appetite to ensure it remains aligned with strategic objectives, whilst promoting a wide understanding of how it translates into tolerance levels within service or programme settings;
- Intelligence sharing and collaboration between risk management and assurance disciplines across all Council activities, consolidating ongoing learning, experience and knowledge;
- Ensuring understanding of how each of the "four lines of defence" contributes to the overall level of assurance required and how these can be best integrated and mutually supportive, including informing internal audit coverage;
- Operating sound and transparent risk management arrangements with partners and providers, underpinned by a culture that supports collaboration and the development of trust, ensuring clarity of risk and control ownership and striking a proportionate balance of oversight of partner / provider risks without being over-constrictive;
- Communicating relevant risk messages to the organisation in a timely manner, listening and responding to feedback received; and
- Subjecting the Council's risk management arrangements to regular review to determine their continued adequacy and effectiveness.

Risk management framework and principles

4.8. As an integral part of management systems, and through the normal flow of information, the Council's risk management framework harnesses the activities that identify and systematically anticipate and prepare successful responses.

4.9. The framework is designed to support a comprehensive view of the risk profile, aggregated where appropriate, in support of governance and decision-making requirements. It supports the consistent and robust identification and management of risks within desired levels across the organisation, supporting openness, challenge and innovation in the achievement of objectives.

4.10. There are five key principles of risk management that provide the basis on which the Council will manage risk:

- **Governance and leadership** – risk management shall be an essential part of governance and leadership, and fundamental to how the organisation is directed, managed and controlled at all levels.
- **Integration** - risk management shall be an integral part of all organisational activities to support decision-making in achieving objectives.
- **Collaboration and best information** – risk management shall be collaborative and informed by the best available information.
- **Structured processes** – risk management processes are recognised as iterative in practice, rather than sequential, and shall be structured to include:
  - Risk identification and recording – to determine and prioritise how the risks should be managed;
  - Risk analysis and evaluation – to establish the nature of the risk and its potential likelihood and impact;

- Risk appetite and escalation – to assess the risks against risk tolerances and ensure escalation, where appropriate;
- Risk treatment – the selection, design and implementation of risk treatment options that support achievement of intended outcomes and manage risks to an acceptable level;
- Sources of assurance – to recognise assurances available over the effectiveness of the risk treatment/controls;
- Risk monitoring – the design and operation of integrated, insightful and informative risk monitoring; and
- Risk reporting – timely, accurate and useful risk reporting to enhance the quality of decision-making and to support management and oversight bodies in meeting their responsibilities.

These processes are detailed further below (a) to (h).

- **Continual improvement** – risk management shall be continually improved through learning and experience.

Risk management processes

(a) Risk identification and recording

4.11. In broad terms, the Council's reported risks are split into four categories:

- Strategic – those risks, which if they occurred, would have a major impact on the organisation or delivery of its priorities. Strategic risks also include cross-cutting risks that impact across multiple directorates;
- Directorate – key risks that could affect the Council's control and ability to successfully and continually deliver or commission services;
- Project – risks that could affect the Council's ability to successfully complete the desired transformational outcomes or deliver predefined outputs that enable us to deliver outcomes and realise benefits; and
- Fraud – risks that could expose the Council to potential fraud by those internal or external to the organisation.

4.12. Each of the categories above should be captured within the relevant risk registers. All Strategic risks should be recorded on the Strategic Risk Register; all Directorate risks should be captured in the respective directorate risk register; and each project should maintain a risk register. All of these registers must apply the same risk framework, terminology and scoring – in accordance with this policy and strategy. Development of Fraud Risk Registers is being led by the Internal Audit and Counter Fraud team and applies the same scoring methodology and terminology – and the management and oversight of these registers is covered in more detail within the Counter Fraud Strategy.

4.13. The aim of risk identification is to recognise and articulate the risks that may help or prevent the Council to achieve its objectives. It is particularly relevant to consider new or emerging risks alongside business planning and strategy formulation processes.

4.14. The following factors, and the relationship between these factors, should be considered when identifying risks:

- Changes in the external and internal context;
- Causes and events;
- Consequences and their impact on objectives;

- Threats and opportunities;
- Vulnerabilities and capabilities – including those highlighted by internal audit / inspections;
- Uncertainties and assumptions within options, strategies, plans or initiatives;
- Indicators of emerging risks;
- Limitations of knowledge and reliability of information; and
- Time-related factors.

4.15. Risks should be recorded whether or not their sources are under the Council's direct control, as they have the potential to impact on achievement of objectives, causing great damage or creating significant opportunity. Where risks relate to partner organisations, the Council should work together with partners to seek and establish sources of assurance.

(b) Risk analysis

4.16. The aim of risk analysis is to build understanding of the nature of risk and its characteristics including, wherever possible, the level of risk. It involves consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness. Analysis techniques can be qualitative, quantitative or a combination of these, depending on the circumstances and intended use.

4.17. Risk analysis considers factors such as: the likelihood of events and consequences occurring;
- the type and scale of consequences;
- complexity, connectivity and volatility;
- time-related factors;
- the effectiveness of existing controls; and
- sensitivity and confidence levels.

4.18. The Council applies a common set of risk criteria to foster consistent interpretation and application in defining the level of risk, based on the assessment of the likelihood of the risk occurring and the consequences should the event happen. The Council's Risk Matrix used to determine risk ratings is provided as Appendix A to this strategy document, where the likelihood score is multiplied by the impact score in order to achieve an overall rating of between 1 and 25.

4.19. Providing sufficient information is known, during assessment each risk is to be assigned an inherent and current risk rating. The inherent risk rating refers to the level of risk that the Council would be exposed to, if no action were taken to manage/control the risk. The current risk scoring takes into account all mitigating controls already in place and their effectiveness.

(c) Risk evaluation

4.20. Once analysed, risks will be evaluated to compare the results against the nature and extent of risks that the organisation is willing to take or accept to determine where and what additional action is required.

(d) Risk appetite, tolerance and escalation

4.21. The Council recognises that risk is inherent in delivering and commissioning services and does not seek to avoid all risk, but instead aims to have a pro-active approach to risk, appropriately balancing risk against reward, with risks managed in a proportionate manner.

4.22. This will require an approach that allows flexibility and support for well-informed and considered risk taking, promoting transparency and effective risk management, whilst maintaining accountability. While risks defined as “high” are to be managed down to a tolerable level wherever possible, it is important that risks across the Authority are not over-controlled.

4.23. It is not realistic for the Council, with its diverse range of services and duties, to have a single definitive application of risk appetite across the entire organisation. Instead, risk appetite should be set with reference to the strategy for service delivery in each particular area/objective. However, examples of risk exposure that would be seen as intolerable without management would include any that are reasonably expected to:

- Endanger the safety of service users, residents or employees;
- Severely damage the Authority’s reputation;
- Lead to breaches of laws and regulations;
- Endanger the future operations of the Council (i.e. by exceeding the risk capacity of the organisation – the amount of risk that the Authority can bear); or
- Adversely impact the financial security or resilience of the Council.

4.24. In addition, to aid managers in understanding risk tolerance, the Council’s appetite for risk is implicitly defined within the framework for determining risk levels (see Appendix A). Risks rated as ‘High’ are deemed to have exceeded tolerance levels and must be subject to monthly review and discussion at the relevant management level for review and action, as follows:

- Strategic risks rated “High” – reviewed by Risk Owner monthly and by Corporate Leadership Team quarterly. Reported to Audit and Governance Committee six monthly;
- Directorate risks rated “High” – reviewed by Risk Owner and Directorate Management Team monthly. Responsible Director to escalate to Corporate Leadership Team if considered to represent a Strategic risk, for inclusion on Strategic Risk Register;
- Project risks rated “High” – reviewed by Project leads monthly and escalated to Assistant Director for discussion at Directorate Management Team.

4.25. Upon escalation, discussions should take place as to whether the risk requires escalation to the next level of risk register. This may include consolidation or aggregation of some risks.

4.26. The target rating for risks is expected to be “medium” or lower. In the event that this is not deemed realistic in the short to medium term, this shall be discussed as part of the escalation process, and this position regularly reviewed with the ultimate aim of bringing the level of risk to a tolerable level.

(e) Risk treatment

4.27. Risks can be mitigated in the following ways:

- **Tolerate** (do nothing as the risk impact is low or the cost of mitigation is not proportionate to the cost of the risk occurring);
- **Treat** (implement controls);
- **Transfer** (for example purchase insurance to transfer the cost of occurrence); or
- **Terminate** (stop the activity if it is too risky).

4.28. Potential benefits derived in relation to the achievement of objectives are to be balanced against the costs, efforts or disadvantages of implementation. Justification for the design of risk treatments and the operation of internal control is broader than solely financial considerations and should consider all of the organisation's obligations, commitments and stakeholder views.

4.29. The controls in place to manage a risk should be recognised on the respective risk register entry.

(f) Sources of assurance

4.30. For each risk entry, owners should consider the sources of assurance available to evidence the effectiveness of the current controls. In considering sources of assurance, risk owners should refer to the "four lines of defence" model and ensure that a suitable range of assurances are available and proportionate to the risk. Any gaps in the assurance framework should be discussed at the respective management team level and actions taken to address this – which may include discussions with the Chief Internal Auditor and inclusion in audit planning.

4.31. Under the "first line of defence", management have primary ownership, responsibility and accountability for identifying, assessing and managing risks. The first line 'own' the risks, and are responsible for execution of the organisation's response to those risks through executing internal controls on a day-to-day basis and for implementing corrective actions to address deficiencies. Through a cascading responsibility structure, managers design, operate and improve processes, policies, procedures, activities, devices, practices, or other conditions and/or actions that maintain and/or modify risks and supervise effective execution. There should be adequate managerial and supervisory controls in place to provide assurance over compliance and to highlight control breakdown, variations in or inadequate processes and unexpected events, supported by routine performance and compliance information. Sources of assurance at this level may include management/supervisory checks or management review of performance information. Assurance comes directly from those responsible for delivering specific objectives or processes. It may lack independence, but its value is that it comes from those who know the business, culture and day-to-day challenges.

4.32. The "second line of defence" relates to review by management or specialists that is separate from day-to-day operations. It includes risk and compliance reviews, financial controls over operational areas and oversight of operations by senior management. It can also include quality control reviews that are additional to day-to-day quality checks, for example one-off checking of a range of items where there have been customer complaints. assurance provided is separate from those responsible for delivery, but not independent of the management chain. This would typically include compliance assessments or reviews carried out to determine that standards, expectations, policy and/or regulatory considerations are being met in line with expectations across the organisation. This may include "audits" performed within the service area or routine internal inspections or spot checks on processes/controls.

4.33. Internal audit forms the organisation's "third line of defence". An independent internal audit function will, through a risk-based approach to its work, provide an objective evaluation of how effectively the organisation assesses and manages its risks, including the design and operation of the first and second lines of defence. It should encompass all elements of the risk management framework and should include in its potential scope all risk and control activities, in line with the Internal Audit Charter. Internal audit may also provide assurance over the management of cross-organisational risks and support the sharing of good practice between organisations, subject to considering the privacy and confidentiality of information. Management should not rely upon internal audit to identify or expose risks and vulnerabilities, but any findings assessed as "high" organisational impact by internal audit should be reflected upon to ensure those risks have been suitably noted in the relevant register entries.

4.34. Sitting outside of the organisation's own risk management framework, are other sources of assurance that support an organisation's understanding and assessment of its management of risks and its operation of controls. These can be referred to as the "fourth line of defence" and may include external auditors, who have a statutory responsibility for certification audit of the financial statements; independent inspection bodies, such as Ofsted, the Care Quality Commission or the Information Commissioner's Office, external system accreditation reviews/certification (e.g. ISO) or peer reviews.

4.35. Careful coordination is necessary to avoid unnecessary duplication of efforts, while assuring that all significant risks are addressed appropriately, with the appropriate range of assurances. Coordination may take a variety of forms depending on the nature of the organisation and the specific work performed by each party. It is important to adopt the Council's risk management framework and definitions consistently across all "lines of defence" to ease understanding, for example, in defining risk categories, risk criteria and what is an acceptable level of control or a significant control weakness.

4.36. Internal audit and external audit should work effectively together to the maximum benefit of the organisation and in line with international and public sector standards. The Internal Audit Charter provides further detail on the delivery of the internal audit service.

(g) Risk monitoring

4.37. The frequency of risk assessment, analysis and review should be a function of how fast risks are emerging and the level of their materiality rather than determined by traditional institutional administrative cycles.

4.38. As a minimum, risks should be reviewed by their owners every three months, with risks rated as "High" subject to more detailed and frequent monitoring, as above. It is expected that in addition to the timely reviewing of individual risks by risk owners, key risks are subject to structured collective discussion by management teams, focusing on changes to the existing risk profile, trends and any emerging risks.

4.39. Ongoing monitoring should support understanding of whether and how the risk profile is changing and the extent to which internal controls are operating as intended to provide reasonable assurance over the management of risks to an acceptable level in the achievement of organisational objectives.

(h) Risk reporting

4.40. Senior Officers and elected Members must receive unbiased information about the organisation's principal risks and how management is responding to those risks.

4.41. Reporting will take into account differing stakeholders and their specific information needs and requirements; cost, frequency and timeliness of reporting; method of reporting; and relevance of information to organisational objectives and decision-making.

4.42. As a public service body, it is imperative that the Council demonstrates transparency and accountability for managing the risks that impact on staff, service users and residents. Therefore, the Strategic Risk Register shall be reported in public session for the Audit and Governance Committee.

4.43. The Strategic Risk Register is to be presented to Executive annually, in addition to any occasion where it is the view of the Corporate Leadership Team that there has been a significant change to the Council's overall risk profile.

4.44. The Strategic Risk Register is reported to the Audit and Governance Committee at least six monthly for assurance purposes.

4.45. Strategic Risk Register entries are subject to rolling assurance reviews by Internal Audit. The outcomes of which are reported to the Audit and Governance Committee to provide real time assurance over the existence of the controls stated in the risk entry, whilst maintaining Internal Audit's independence from the risk management activity.

5. Links to Council Values and Behaviours

5.1. The Council's risk management approach must align with its values and behaviours and is the responsibility of all officers. An effective risk management strategy needs to be suitably embedded within those cultural behaviours and directly links as with the following:

- Customer focused – Take ownership and do the right thing.
- Customer focused – Think 'One Team' and act Council-wide.
- Respectful – Listen to and value the contribution of others.
- Efficient – Challenge and innovate.
- Efficient – Be collaborative and share learning.
- Supportive – Build an open and sustainable culture.
- Trustworthy – Act with honesty and integrity.
- Trustworthy – Be open and transparent.

Appendix A: Risk scoring

Figure 1: Risk scoring matrix

Very high (V)	5	10	15	20	25
High (H)	4	8	12	16	20
Medium (M)	3	6	9	12	15
Low (L)	2	4	6	8	10
Negligible	1	2	3	4	5
Impact / **Likelihood**	**Very rare**	**Unlikely**	**Possible**	**Likely**	**Very likely**

Red (risk scores 16 to 25):	Requiring regular review and active management
Amber (risk scores 5 to 15):	Likely to cause the Council some difficulties, ongoing reviews needed
Green (risk scores 1 to 4)	Monitor as necessary to note any change

Appendix B: Impact descriptors

The following descriptors are designed to assist the scoring of the impact of a risk:

	Negligible (1)	Low (2)	Medium (3)	High (4)	Very High (5)
Legal and Regulatory	Minor civil litigation or regulatory criticism	Minor regulatory enforcement	Major civil litigation and/or local public enquiry	Major civil litigation setting precedent and/or national public enquiry	Section 151 or government intervention or criminal charges
Financial	<£0.5m	<£1m	<£5m	<£10m	>£10m
Service provision	Insignificant disruption to service delivery	Minor disruption to service delivery	Moderate direct effect on service delivery	Major disruption to service delivery	Critical long term disruption to service delivery
People and Safeguarding	No injuries	Low level of minor injuries	Significant level of minor injuries of employees and/or instances of mistreatment or abuse of individuals for whom the Council has a responsibility	Serious injury of an employee and/or serious mistreatment or abuse of an individual for whom the Council has a responsibility	Death or abuse of an employee or individual for whom the Council has a responsibility or serious mistreatment or abuse resulting in criminal charges
Reputation	No reputational impact	Minimal negative local media reporting	Significant negative front page reports/editorial comment in the local media	Sustained negative coverage in local media or negative reporting in the national media	Significant and sustained local opposition to the Council's policies and/or sustained negative media reporting in national media

Appendix C: Roles and responsibilities

Individual or group	Role and responsibilities under the Risk Management Strategy and Policy
Audit and Governance Committee	On behalf of the Council, ensure that risk management and internal control systems are in place that are adequate for purpose and are effectively and efficiently operated. To review the effectiveness of risk management activity.
Executive	Responsibility for the operation of the risk management framework.
Chief Executive (Head of Paid Service)	Responsibility for the overall monitoring of strategic risks across the council, including the endorsement of priorities and management action. Responsible for ensuring sufficiency of risk management resources.
Executive Director of Finance and Performance	Active involvement in all material business decisions to ensure immediate and longer-term implications, opportunities and risks are fully considered. Owner of Risk Management Policy and Strategy.
Executive Director of Customer and Governance	Active involvement in all material business decisions to ensure immediate and longer-term implications, opportunities and risks are fully considered, including potential legal/regulatory compliance implications.
Corporate Leadership Team	Adopt and embed the Risk Management Policy and Strategy, ensuring the Council manages risks effectively and that risk assessment is factored into all decision making. Actively consider, own and manage key strategic risks affecting the Council through regular review of the Strategic Risk Register (at least three monthly and monthly for “High” risks). Promote and demonstrate the behaviours and values that support well-informed and considered risk decision-making. Promote the integration of risk management principles into the culture of the Council and its partners. Review and updating of sources of assurance on strategic risk entries. To flag any areas of gaps in sources of assurance (against the four lines of defense) in discussions with the Chief Internal Auditor as part of annual audit planning / as required in year. Ensure inclusion of risk management in relevant roles to embed within project methodology.
Corporate Leadership Network (includes Directors and Assistant Directors)	Ensure that effective risk management arrangements are in place in their areas of responsibility to ensure the Council’s exposure is at an acceptable level. Promote and demonstrate the behaviours and values that support well-informed and considered risk taking, while maintaining accountability.

Individual or group	Role and responsibilities under the Risk Management Strategy and Policy
	Encourage open and frank conversations about risks, ensuring appropriate reporting and escalation as required. Review and updating of sources of assurance on strategic risk entries. To flag any areas of gaps in sources of assurance (against all four lines of defense) in discussions with the Chief Internal Auditor as part of annual audit planning / as required in year. To play a key role in embedding risk management at a project level and escalating risks to directorate/strategic risk registers, as appropriate.
Directorate Management Teams	Responsibility for the effective management of risk within the directorate and maintenance of directorate risk registers, including regular review (at least three monthly and monthly for 'High' risks). Risk escalation and reporting to the Corporate Leadership Team, as appropriate for consideration in the Strategic Risk Register. Review and updating of sources of assurance on risk entries. To flag any areas of gaps in sources of assurance (against all four lines of defense) in discussions with the Chief Internal Auditor as part of annual audit planning / as required in year. Identify and assess any project related risks which require escalation to the directorate risk register.
Chief Internal Auditor	Facilitate maintenance of an up-to-date Strategic Risk Register and provide regular reports on the Strategic Risk Register to Audit and Governance Committee and the Corporate Leadership Team. Independently assess the effectiveness of the risk management framework and the control environment in mitigating risk. This will be informed by the outcomes of the risk based audit plan and rolling risk register reviews. To ensure audit plans are focused on areas of key risk and take into consideration the sources of assurances available under the first, second and fourth lines of defense – to target resource and assurance work accordingly. **Note** – it is important to acknowledge that the Chief Internal Auditor must remain independent of risk management processes, in order to provide an annual opinion on the effectiveness of risk management. Whilst Internal Audit will provide advice and facilitation on maintaining risk registers, all risk entries, management of risks and associated actions remain solely the responsibility of officers.
Project teams / sponsors	Identify, record, assess and manage risks associated with projects and escalate 'High' risks to members of Corporate Leadership Network, as appropriate, for review and potential inclusion on directorate or strategic risk registers.
All officers – including temporary, agency and volunteers	Identify risks and contribute to their management as appropriate. Report inefficient, unnecessary or unworkable controls. Report loss events or near-miss incidents to management.

Individual or group	Role and responsibilities under the Risk Management Strategy and Policy
	To build a culture whereby risk management is embedded in decision-making and operations.

Appendix D: Template risk register

Inherent Risk								Residual Risk					Actions			
Risk No.	Risk Description	Cause	Effect	Owner	Likelihood	Impact	Score & RAG	Key controls	Sources of assurance over controls	Likelihood	Impact	Score & RAG	Actions	Owner	Target Date	Action RAG