Appendix A

London Borough of Islington

Risk Management Strategy and Framework

Table of Contents

1. Introduction

Risk may be seen as an event or issue that may threaten our ability to deliver our vision and strategic objectives. Therefore, we recognise that managing risk effectively is key. However, we know that risk is inherent in any business and indeed it is essential to embrace risk to some degree if we wish to achieve our goals for Islington residents. Our priority must be to ensure that, as far as possible, our strategic objectives are not threatened by risks that have not been identified, managed or responded to effectively.

Effective risk management supports our ability to deal with emerging or growing risks and enhances our resilience. Additionally, both regulation and good practice require us to have an effective risk management framework in place.

2. Risk Management Strategy

The London Borough of Islington recognises and accepts its responsibility to manage risks effectively. We believe that risk management is a continuous process designed to identify, analyse, and mitigate risks, with the purpose of supporting the achievement of our objectives.

The vision of our risk management approach is to support the achievement of our strategic ambitions through the application of sound risk management principles. The vision is underpinned by four aims described below:

The risk management strategy is delivered through the application of the risk management framework set out in this document.

3. Purpose of a risk management framework

The purpose of a risk management framework is to support a robust and consistent process for managing risks and opportunities within the Council. It provides a common approach and terminology for all parts of the organisation. The framework has been designed to serve as an accessible and practical resource for teams to guide their risk

management activities and develop an understanding for root cause and consequence of risks.

Our risk management approach aims to embed a culture where risk management is integrated into the way we work. We want to ensure risk management feels dynamic and real. The framework is based on three interlinked principles:

1. **Resilience** - empowered and risk-based decision-making supports the resilience of an organisation;
2. **Agility** - risk management is forward-looking and supports the organisation to be agile, innovative and take calculated risk;
3. **Responsiveness** - risk management activities should be dynamic and responsive to emerging and changing risk.

Our risk management framework is informed by international risk management standards and best practice guidance (ISO 31000, the Institute for Risk Management).

3.1 Definitions

We have implemented the following definitions of risk and risk management:

Risk	Risk is the uncertainty of an event occurring that could affect the achievement of objectives. It is measured in terms of impact and likelihood, and the impact can be positive or negative.
Risk Management	Risk management is the process which help organisations to understand, evaluate and take action on risks with a view to increasing the probability of success and reducing the likelihood of failure.

3.2 Risk Culture

The Council is committed to developing a culture that supports openness, challenge, innovation and well-managed risk-taking. We expect staff to manage risk in line with this risk management framework. However, we also value feedback on its effectiveness to continuously improve and develop our risk management approach.

As with other organisations, the Council is on a continuing journey to developing our risk management. Our risk culture is risk-aware and proactive, with risk consistently considered as a key factor in all operational and strategic decisions.

4. Risk Appetite

Risk appetite is defined as the amount and type of risk that an organisation is willing to take in pursuit of its objectives. The Council's risk appetite varies depending on the type of risk. The Council is responsible for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives. Risk appetite is commonly expressed as a statement which explains what the Council sees as acceptable, taking into account organisational capability and capacity. The risk appetite statement is a fluid statement and is revisited regularly.

4.1 Risk Appetite Statement

We are an ambitious Council. To achieve our goals, we must continue to enhance our ability to collaborate, test new ideas and take risks. The Council recognises that the pursuit of strategic goals is not without risk and will not be afraid to take considered risks to learn and develop. A risk appetite that is defined in too rigid terms can hinder innovation. Appropriate risk-taking, underpinned by sound risk management, will support the Council to deliver its objectives. The Council is not unduly risk averse and will take a balanced view on risks as they are identified. However, as a general rule, the Council:

- Will not tolerate taking risks which would result in harm to our residents and staff;
- Will not tolerate risks which would result in breach of laws or regulations;
- Will not tolerate risks which would result in the Council becoming financially unviable;
- Will not tolerate risks that score 15 and above in the risk matrix and will require robust and closely monitored mitigation plans for such risks.
- Has a low tolerance for risks which would result in a long-term impact on our reputation.

5. Roles and responsibilities

All Council staff have a role to play in managing risk. Some individuals or groups have specific roles and responsibilities which are set out below:

All staff	Manage day to day risks within their areas of responsibilities and report risk concerns to their line managers.
Risk owners	A risk owner is the lead officer for the area affected by the risk. It is the risk owner's responsibility to ensure that appropriate resources are allocated to manage risk and that action plans are being implemented. They may delegate day-to-day management of risks but they are responsible for seeking assurance that the risks they own are managed effectively.
Service Managers/Project managers	Responsible for effectively managing risks within their areas of responsibility, including identifying risk ownership. Identify, assess and document significant risks and escalate appropriately if required.
Heads of Service/Service Directors	Deliver effective risk management within their area of responsibility to deliver business objectives. Responsible for timely escalation of significant risks. Encourage staff to be open and honest in identifying risks and opportunities.
Corporate Directors	Ensure key risks are being identified and managed to aid delivery of the Council's priorities and objectives. Promote effective risk management and risk-based decision-making within their areas. Risk owners for principal risks.
Corporate Director for Resources	Responsibility for the risk management framework and its effectiveness and to promote it across the Council.

Corporate Management Board	Promotes an effective risk management culture across the Council. Responsibility for ensuring that principal risks are managed and reported appropriately.
Audit Committee	Consider the Council's arrangements for corporate governance and risk management and recommend necessary actions to ensure compliance with best practice.

6. Risk governance

The risk management framework is underpinned by ownership and accountability. Strategic objectives and risk tolerance levels are set by the Corporate Management Board, who are reliant on staff at every level of the organisation escalating risks though formal reporting structures in line with the organisation's risk appetite. The risk governance arrangements ensure appropriate oversight of risk management and assurance of its effectiveness.

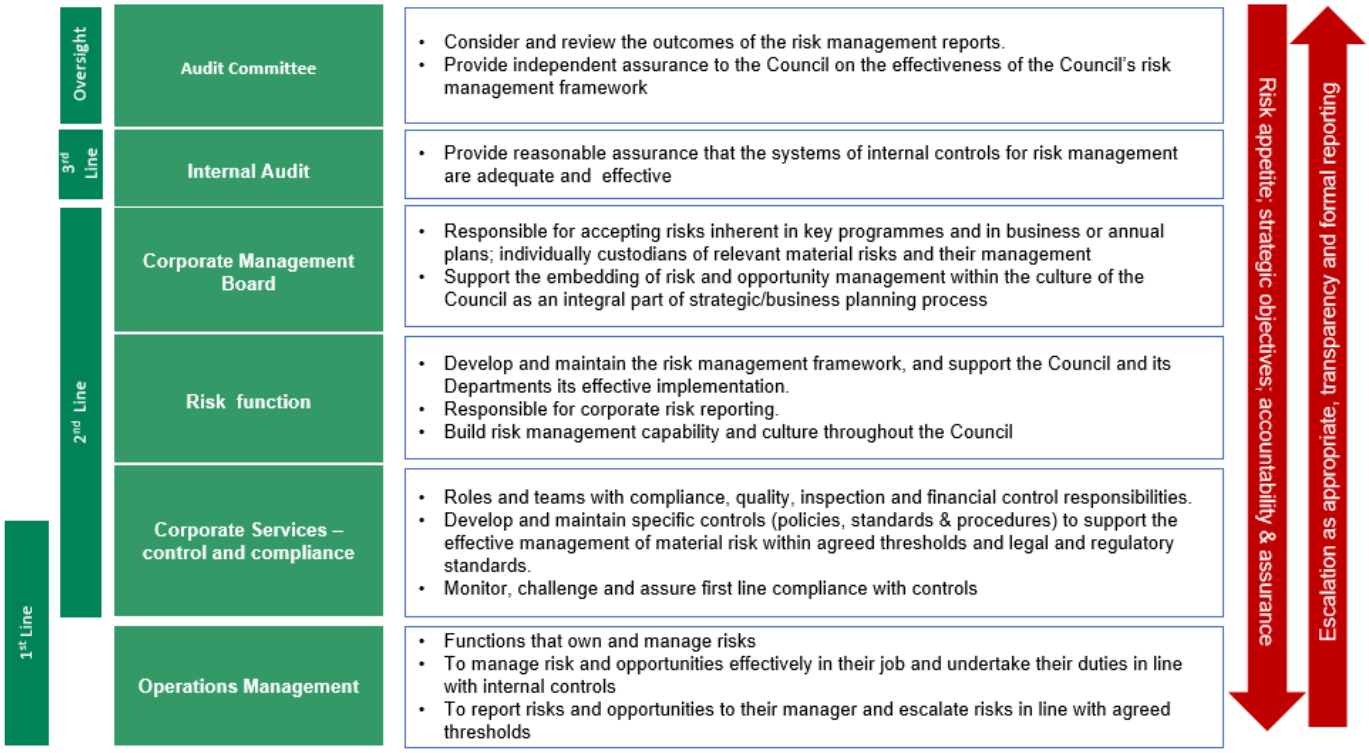


Figure 1: Risk governance structure

The governance structure aligns to the 'Three Lines of Defence' model which can be summarised as:

- *First line of defence:* Managing risks in day-to-day operations in line with internal controls (policies, procedures, and standards).
- *Second line of defence:* Roles and teams that put controls in place and monitor compliance, and the risk management function.
- *Third line defence:* Independent assurance that the controls are effective in managing risk.

6.1 Risk reporting

Risk owners need appropriate risk information to make business decisions and monitor business performance. They may nominate a risk lead to manage the day-to-day management of risks and will work with that person to determine what information is required. Each service and department should conduct risk assessments and keep a risk register to document the risks identified for their area, and the controls in place to manage them. Risk owners are responsible for regular monitoring of progress and updating the risk register. They may nominate a risk-coordinator to facilitate reporting of risks within their area of responsibility. Risk owners are also responsible for escalating risks to the next management level if risk exposure reach agreed trigger points.

The Council's Risk Manager is available to advise and support the development of a risk register. However, the service/department is responsible for the risk register, reflecting the fact that they own the controls and are responsible for monitoring and updating of risk and action items on their risk registers. Risk registers should follow the format of the template provided in **Appendix 3.**

The Principal Risk Report covers the Council's corporate level risks and is owned by the Corporate Management Board (CMB). The risk manager is responsible for working with risk sponsors and nominated risk leads to update all Principal Risks annually, and report to CMB and the Audit Committee. Figure 2 below shows the reporting flow of risk information.

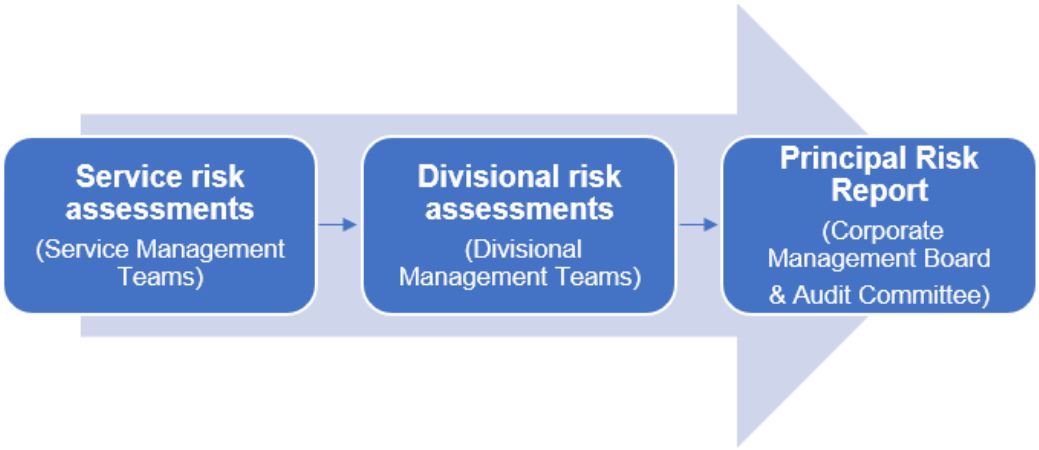


Figure 2: Risk reporting

6.2 Escalation triggers

The Council has defined thresholds to ensure risks are reported and managed at the appropriate level. These thresholds, or triggers, reflect management's tolerance for risk exposure at each governance level, and support appropriate escalation and delegation of risk. This ensures that risks are managed at the appropriate level of responsibility and authority depending on the risk exposure.

Figure 3 below illustrates how the risk assessment matrices align across the governance levels using financial metrics as an example. For example, the bottom threshold for the corporate risk matrix (£1m financial impact) sets the upper threshold on the department risk matrix, reflecting a delegation of risk. A service or departmental risk that is assessed as having an impact score in the highest category would automatically trigger an escalation to next management level for review and oversight. The lower threshold criteria provided for department and service level should be treated as illustrative, for it could vary to reflect different risk contexts. **Appendix 1** provides a guide to assessing the impact of risk for each of the three levels.

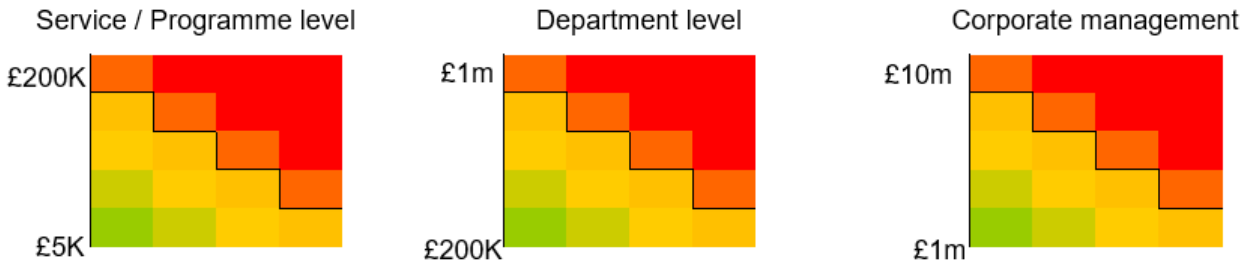


Figure 3: Illustrative example of differentiated but aligned risk matrices across governance levels.

7. Risk management process

The Council has implemented a six-stage process for managing risks. This comprehensive approach provides teams with a systematic way to manage all different types of risks. This section describes each step of the process.

The first stage involves understanding the team's or activity's objectives so that risks to achieving those objectives can be identified. The Council's strategic plan defines top level goals and objectives, and individual service areas should link their priorities to those.

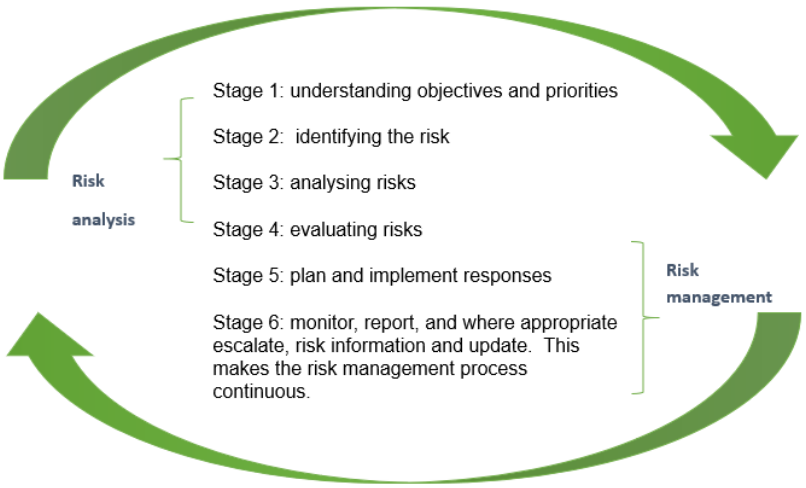


Figure 4: Risk management process

7.1 Risk identification

The aim of risk identification is to understand the overall risk profile. At this stage, it is useful to consider a wide range of risks that could have an impact on the ability to achieve objectives. A risk may have an impact on one or more objectives. Some risks may be outside of our direct control but should still be identified.

The table below presents examples of risk categories and areas that could be used as a starting point for identifying risks.

Category	Examples of risk areas
Political	Direction of Government policy now and possible changes in the future, tax policy, trade restrictions, political stability
Economical	Economic trends nationally, cost of living, wage rates, interest rates, inflation, exchange rates, credit availability
Social	Trends in demographics, consumer patterns, family life, community cohesion, residents' expectations, cultural norms and attitudes
Technology	Existing and emerging technology to deliver services, maturity of technology
Legal	Existing and future legislative and regulatory requirements, equal opportunities, health and safety, employment law, risk of legal claims
Environmental	Environmental factors that may hamper the delivery of objectives, adverse weather, changing climate
Governance	Clarity and transparency of decision-making and accountability, adequate monitoring, clarity of work plans
Operational	The design and efficiency of internal processes, value for money, quality and quantity of service or product, fraud
People	Leadership ability and effectiveness, staff engagement, culture and behaviours, industrial action, capacity and capability
Financial	Return on investment, quality of financial management, asset management, compliance with financial reporting, fraud
Commercial	Managing contracts and supply chains, poor performance, inefficiencies, value for money, meeting business requirements
Information	Quality of data and information, adequate use of available data, data protection, information governance, cyber attacks
Security	Managing access to premises and information, cyber security, staff safety and security
Reputational	Ethical considerations, poor quality of services, lack of innovation, repeated mistakes. Not managing risks appropriately can damage the reputation of individual departments as well as Council as a whole.
Project/Programme	Alignment of activities with strategic priorities, realising the indented benefits, delivering on time and within budget

Facilitated group workshops is the most effective method for risk identification as it draws on many different experiences and perspectives. Interactive workshops can often draw out previously unidentified risks through open and honest discussions.

Participants should represent a wide range of teams who may be affected by the risk area being discussed. This will generate a rich collection of risks to analyse further. Other risk identification methods include one-to-one conversations, and information gathering through surveys.

Once risks have been identified, they should be added to a risk register which will be used to document more details about each risk as the risk assessment process progresses. (**Appendix 3** includes a risk register template)

7.2 Risk analysis

After risks have been identified, they need to be analysed further to better understand how to manage them. The purpose of risk analysis is to articulate what would cause the risk to occur and what the consequences would be if it happened.

Once we understand cause and consequence, we can analyse the controls we have in place to manage the risk and their effectiveness. Proactive controls are designed to reduce the likelihood of the risk happening. Reactive controls will reduce the impact, or consequence, if the risk were to become reality.

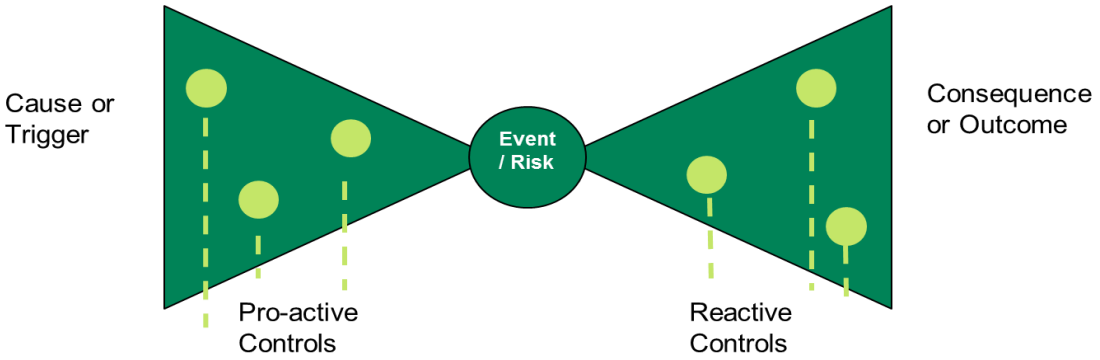


Figure 5: Analysing cause and consequence

7.3 Risk evaluation and scoring

The next stage in the risk management process is to evaluate the risk to establish the level of threat to our objectives. The evaluation process helps to identify the risks which can be tolerated, and which require additional action to reduce risk levels. It also facilitates prioritisation of risks.

We express total risk score in numerical terms of *likelihood multiplied by impact.* 'Likelihood' is defined as the probability of a risk occurring, whilst 'Impact' refers to the consequences if the risk it would occur.

Likelihood ratings is the same across the Council whilst impact ratings are differentiated by corporate, department and service level (see **Appendix 1**). We use a 'current' risk scoring method, meaning that we assess the likelihood (probability) and impact (consequence) of the risk in view of current controls in place.

Once risks have been evaluated and scored, they can be plotted on a heat map for an overview of the total risk profile (Figure 6). The Council has adopted a 5x4 risk score matrix.

The heat map will visually identify highest ranking risks and the cumulative risk level. This will assist the Council to consider its overall risk exposure and appetite (see **Appendix 2** for a heat map template).

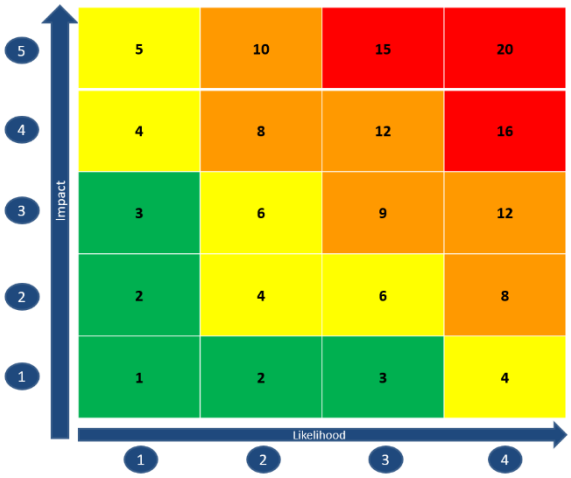


Figure 6: Heat map with risk scores

7.4 Taking action

The options of responding to a risk are referred to as the 4 T's:

- **Treat**: Applying proactive and reactive controls, and other actions to reduce risk levels to acceptable levels.
- **Tolerate**: The risk exposure may be tolerable if no future action is taken, or the ability to treat the risk is limited, or the cost disproportionate to the benefits.
- **Transfer**: Transfer all or some of the consequences to another party, most commonly through insurance.
- **Terminate**: Cease the activity that is giving rise to the risk.

The most common response is to treat the risk by increasing or modifying controls and mitigating actions.

7.5 Monitoring and review

All risk information should be documented in the risk register (see **Appendix 3** for a risk register template). This facilitates regular monitoring of implementation of mitigating actions and assessment of their effectiveness in reducing the risk level. New risks can be added as they are identified. High scoring risks should be monitored more frequently to ensure appropriate action is being taken. It is the risk owner's responsibility to monitor that action is taken forward and risk information is being updated.

Department and service level risk registers are dynamic risk management tools that should be reviewed on an ongoing basis, with formal management reviews at least bi-annually. Principal risks are reviewed bi-annually and updated annually.

7.6 Risk communication

Accurate and timely communication of risk information is crucial if we are to realise the benefits or risk management activities. Open, honest and transparent risk

communication is a sign of a strong risk culture. The Council's risk communications take many forms, including:

Formal communications

- Risk reporting – Department Management Teams, Corporate Management Board and Audit Committee receive regular updates to provide assurance that risks are being effectively identified and managed across the Council.
- External risk communication – engagement with residents and members to present risks associated with new projects and services.

Informal communications

- Staff intranet - sharing the risk framework and resources with staff and other ad hoc communications to raise awareness of risk management.
- Training sessions on risk management and the framework.
- Facilitated workshops with teams to support them to improve their risk management processes.

8. Managing risk in projects and programmes

The principles of the risk management process in this framework can be applied to project and programme risks as well. However, project and programme management have its own governance models and reporting structures. Risk management in this context is focused on risks to the successful delivery of the intended benefits of the project or programme.

For large and/or high-profile projects, risks may be of such strategic importance that they should feature on the corporate risk register. Programme/project sponsors should consider the impact criteria in **Appendix 1** when assessing if a risk meets the criteria for corporate oversight.

The Corporate Project Management Office (PMO) can provide specialist guidance on project and programme risk management – search PMO on Izzy for more information.

9. Guidance and training

The Risk Manager is responsible for designing and delivering training to support the Council's risk management activities. This may take many forms, for example:

- One-to-one guidance – talking through specific risks, or aspects of risk management, related to a member of staff's responsibilities.
- Resources on intranet – providing templates, guides and risk management tools on the Council's internal website.
- Team and member training – training sessions tailored to teams' service or risk areas, or members' responsibilities.
- Online training – Development of online training materials for staff who would like to gain risk management skills.

10. Conclusion

By establishing a robust risk management framework, the Council is able to manage risk as an integral part of governance and management. The benefits of the risk management framework include:

- A structured way of dealing with current and emerging risks;
- Creating the right culture so that the Council can learn from its mistakes and take advantage of opportunities;
- Helping to focus decision-making and actions of the priority issues for the Council, emanating from its objectives;
- Involving individuals at different levels in the Council and promote greater understanding of the objectives and strategy.

Appendix 1: A guide to assessing risk scores

Likelihood scoring

Likelihood score	Description	Example	Probability	
1	Rare	Very unlikely that this will ever happen.	1%	1 in 100
2	Unlikely	Expected to occur in only exceptional circumstances.	10%	1 in 10
3	Possible	Expected to occur in some circumstances. Has happened elsewhere.	20%	1 in 5
4	Likely	Expected to occur in many circumstances. Has happened in the past.	50%	1 in 2

Impact scoring (Corporate/Department/Service)

Corporate Management Board: Principal Risks

Impact Ratings	Financial	Service Delivery	Health and Wellbeing	Reputation
5	Financial loss above £10m.	Major disruption to a number of critical services.	Multiple deaths or serious/life-changing non-recoverable injury(s)/extreme safeguarding alerts likely.	Long term damage – e.g., Adverse national or local publicity, highly damaging severe loss of public confidence. Widespread and high level of criticism. Impacts on staffing and recruitment.
4	Financial loss above £8m.	Major disruption of a critical service.	Multiple casualties with recoverable injuries. Major safeguarding concerns potentially affecting multiple people. Evidence of known sustained neglect or abuse without intervention.	Medium to long term damage – e.g., Adverse local, regional, or national publicity, major loss of confidence, a matter that is frequently referenced in relation to the council.
3	Financial loss above £6m.	Major disruption of an important service. Moderate disruption of a critical service.	Noticeable safeguarding risks – evidence of known neglect or abuse without intervention.	Medium term damage – e.g., Adverse publicity, local, regional, and national coverage, with significant follow-up stories
2	Financial loss above £4m.	Moderate disruption of an important service.	Single casualties with recoverable injuries. Noticeable safeguarding risks – evidence of neglect.	Short term damage – e.g., Adverse publicity, national follow-up stories on the same issue.
1	Financial loss above £1m.	Brief disruption of an important service. Repeated disruption of a core service.	Medical treatment required, semi-permanent harm, up to 1 year. Safeguarding concerns of neglect.	Short term damage – e.g., Adverse publicity, regional follow-up stories on the same issue.

Note: a service is defined as critical if it is life critical, important if it has an immediate long-term impact on resident's quality of life

Directorate Management Team (DMT)/Senior Leadership Team (SLT) Risk Scoring Guide:

Impact Score	Financial	Service Delivery	Health and Wellbeing	Reputation
5	Financial loss above £1m	Repeated disruption of a core/critical service.	Significant Medical treatment required, semi-permanent harm, 1 year or more. Safeguarding concerns of neglect.	Medium term damage (12 months or more) – e.g. Adverse publicity, regional follow-up stories on the same issue (or worse)
4	£800k-£1m	Major disruption to a critical service	Moderate Medical treatment required, semi-permanent harm, 9-12 months or more. Safeguarding concerns.	Ongoing adverse media coverage – regional (9-12 months)
3	£600k-800k	Moderate disruption to a critical service	Moderate Medical treatment required, semi-permanent harm, 6-9 months or more. Safeguarding concerns.	Ongoing adverse media coverage – regional (6-9 months)
2	£400k-600k	Minor disruption to a critical service	Moderate Medical treatment required, semi-permanent harm, 3-6 months or more. Safeguarding concerns.	Ongoing adverse media coverage – regional (3-6 months)
1	£200k-400k	Brief disruption to a critical service	Moderate Medical treatment required, semi-permanent harm, 0-3 months or more. Safeguarding concerns.	Ongoing adverse media coverage – regional (0-3 months)

Note: i) a service is defined as critical if it is life critical, important if it has an immediate long-term impact on resident's quality of life ii) the lower thresholds can be adjusted by each department depending on risk context

Service Risk Scoring Guide:

Impact Score	Financial	Service Delivery	Health and Wellbeing	Reputation
5	Over £200k	Long term disruption to non-critical service	Moderate Medical treatment required, multiple casualties. Safeguarding concerns.	Adverse media coverage - regional
4	£100k-200k	Major disruption to a non-critical service.	Moderate medical treatment required. Single Casualties	Ongoing adverse media coverage - local
3	£50k-100k	Moderate disruption to non-critical service	Minor medical treatment required. Multiple number of casualties, recoverable injury.	Adverse one-off media coverage - local
2	£25k-50k	Minor disruption to non-critical service	Minor medical treatment required. Low number of casualties, recoverable injury.	Ongoing reputational damage within the local community
1	£5k-£25k	Brief disruption of non-critical service	Minor medical treatment required. Single casualty, recoverable injury.	Short term reputational damage within the local community

Note: that the upper thresholds can be adjusted by each department, and the lower threshold can be adjusted by each service depending on risk context.

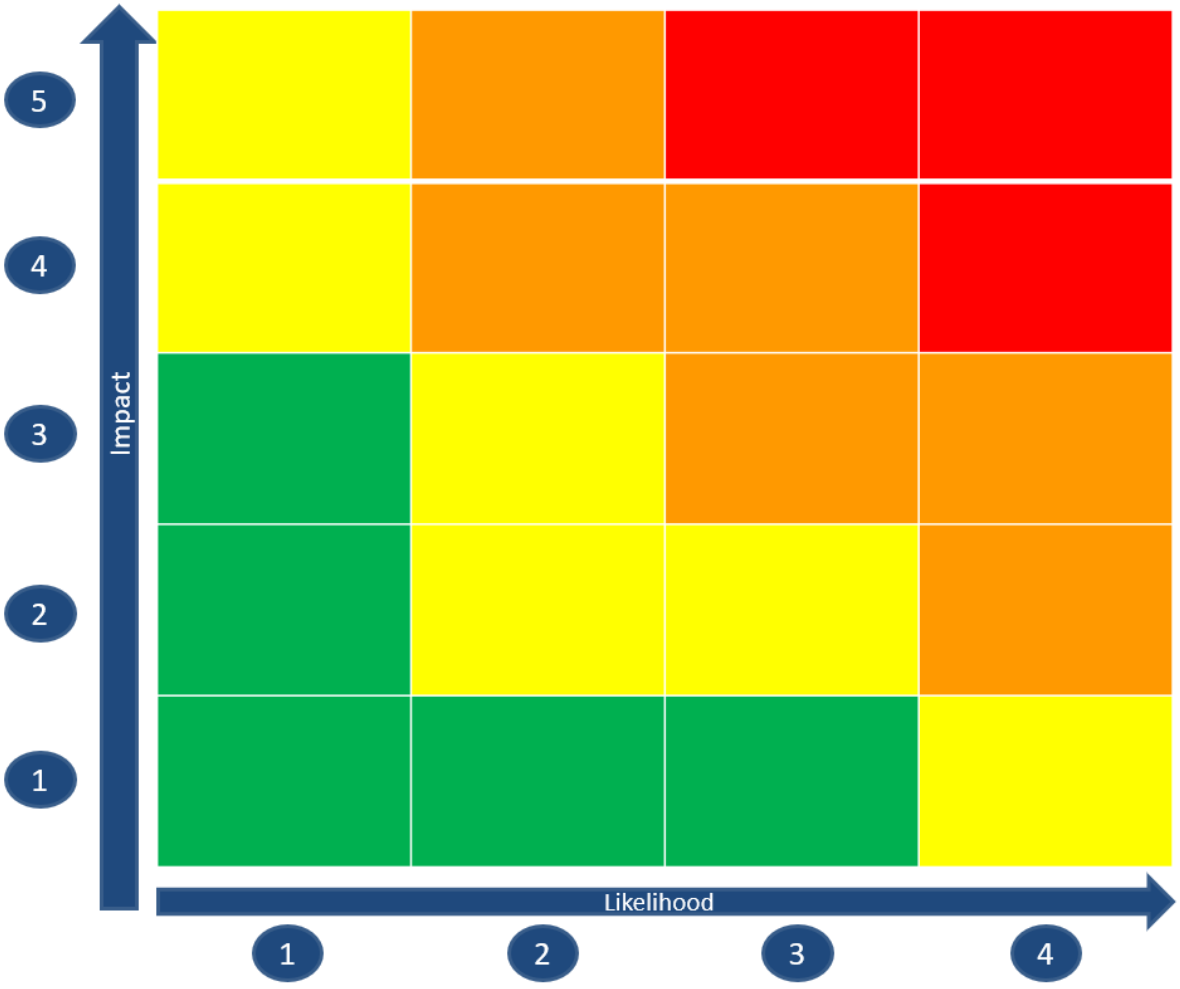
Appendix 2: Risk heatmap template

The heatmap can be used to visually present risks from a risk register. A 5x4 matrix is used (impact multiplied by likelihood).

The colours provide visual representation of risk severity:

- Green – Low risk
- Yellow – Medium risk
- Orange – High risk
- Red – Critical risk

The higher the risk severity, the more attention is needed to ensure robust mitigation plans and monitoring.



Appendix 3: Risk register template (department/service)

Objective	RISK Identified	Cause	Consequence	Impact category	Risk owner	Current risk score based on controls in place			Current controls in place to manage risk	Risk response	Further actions to mitigate risk	Target date and action owner
						Impact 1=Low 5=High	Likelihood 1=Low 4=High	Total score				
Link the risks to the relevant objective for the team/ department/ council	A risk is an uncertain event which may hinder ability achieve objective. A risk is *not* a current issue	The cause that would trigger the risk to happen	The impact if the risk were to happen	Either: Financial, Health and Wellbeing, Reputation or Service Delivery	Service Director	4	4	**16** **(Score at previous review: 20)**	Define any existing controls	Transfer, Treat, Tolerate or Terminate	Define any additional actions which could reduce the risk	Assign a target date for completion of actions and an action owner.
Illustrative example:												
A well run Council	Payment fraud	Anti-fraud controls are not designed and implemented	Financial loss and reputational damage to the Council	Reputation / Financial	Head of Service	2	3	**6** **(Score at previous review: 6)**	1. Segregation of duties between ordering good and services and authorising payment; 2. Invoice approval in line with the scheme of delegation; 3. Budget monitoring	Treat	Proactive duplicate payments testing	Target date: October 2022 Action owner: Accounts payables manager

Note: The Risk Manager can be contacted for an Excel version of this template

Version control:

Action	Date
This version	June 2022
Next review	June 2025