Rotherham Metropolitan Borough Council

Risk Management Guide

(Revised November 2026)

Contents **Page**

Risk Management Guide

1.	Introduction	3
2.	Risk and risk management	3
3.	Objectives of risk management	4
4.	Approach to risk management	4
5.	Documentation	12
6.	Leadership, roles and responsibilities	12
7.	Risk assurance, monitoring and reporting	14
8.	Communication	14
9.	Performance management	15
10.	Corporate governance	15
11.	Guidance and training	15
12.	Further information	17

Appendices

A.	Risk Register template	18
B.	Risk scoring guidance	19
C.	Risk numbering protocol	21
D.	Fraud risk list	22

Rotherham Council: Risk Management Guide

1. Introduction

1.1 The Council recognises that risk management is a principal element of good corporate governance. Effective risk management supports and underpins achievement of the key objectives set out in the Council Plan, which in turn aims to improve the quality of life and services for all local people.

1.2 Members and employees are expected to play an active and positive role in embedding risk management in all activities and in the organisation's culture.

1.3 This Risk Management Guide provides a step-by-step approach to the Council's delivery of effective risk management. The guide should be read in conjunction with the Risk Management Policy 2023.

1.4 The Guide introduces the concept of risk and risk management, explains the general principles and clarifies the approach to and ownership of risk management within the Council.

1.5 This Guide shows how risk management should be approached by each service area. It provides guidance on completing the individual stages of the risk management process to help services to identify, evaluate, manage, monitor, and review risks.

2. Risk and Risk Management

2.1 A risk can be broadly defined as an event that, should it occur, will impact on the delivery of strategic or service objectives. Risks can be identified by posing three questions:

- What could go wrong?
- Would it prevent you from delivering your objectives?
- What would the impact be on your service?

An opportunity can be defined as an uncertainty that could have a favourable impact on objectives or benefits.

2.2 Risk management is the process by which we identify, evaluate and manage risks and opportunities. It is a positive process that can help the Council achieve positive outcomes from the decisions it makes. All members of staff should be involved in the risk management process. Risks and opportunities emerge and evolve continually, and the Council needs to be alert to these changes, responding in a timely and appropriate way to ensure the successful achievement of the Council Plan, Year Ahead Delivery Plan and Service Plans.

2.3 Risk management should not simply be a process of identifying the negatives of why a decision, action or opportunity should not be taken as this can lead to a failure to pursue opportunities. Risk management, if used effectively, can help the Council to pursue innovative opportunities with higher levels of risk because exposure to risk is better understood and managed down to acceptable levels.

2.4 Every organisation manages risk on a daily basis but not always in a way that is visible, repeatable and consistently applied throughout the organisation. A

risk management process tries to ensure that the organisation undertakes cost- effective actions that focus efforts and resources to the areas that pose the greatest threat or potential benefit to its ambitions, through everyone following a well-defined and structured process. The aim of risk management is to enable better decision making, by having the best understanding of the potential problems before they happen and to enable pre-emptive action to be taken.

3. Objectives of Risk Management

3.1 The Council's risk management objectives are to:

- Promote a culture of risk management at all levels to inform all strategic and operational decision making and planning.
- Ensure that risks are aligned to corporate objectives and priorities.
- Ensure the Council successfully manages risks and opportunities corporately, operationally and within projects and partnerships.
- Make an effective contribution to corporate governance and a satisfactory Annual Governance Statement.
- Ensure that all parties understand their roles and responsibilities in the implementation of effective risk management.
- Provide simple, intuitive processes to assist in the identification and prioritisation of risks and opportunities and the appropriate allocation of resources.
- Incorporate the principles of effective risk management into all planning and management processes to achieve consistency of approach.
- Provide appropriate training and guidance for all parties involved in risk management roles, to enable them to competently fulfil their responsibilities and ensure the benefits of good corporate governance are realised.
- Encourage the identification and sharing of information on potential or emerging risks so that risk prevention and/or mitigation measures can be formulated as necessary.
- Regularly consult with Members and officers in order to maintain a continuous review of the effectiveness of risk management processes.

3.2 The Council recognises it is not always possible, nor desirable, to eliminate risk entirely, and so has comprehensive insurance cover that protects the Council from significant financial loss following any damages or losses.

4. Approach to Risk Management

4.1 The risk management approach is based on good practice and can be applied at all levels of the organisation. It describes the key steps for identifying and managing risks within the Council. The approach intends to promote risk management as a positive process. It can bring value and benefit to each service area within the Council, by helping to identify and deal with issues before they happen.

4.2 The Council utilises a five-step approach in the identification and treatment of risks:

- **Step 1 Identify Risks**: Managers, together with their teams, identify risks and record them on the appropriate risk register.
- **Step 2 Evaluate Risks**: Assess the likelihood and severity of identified risk and their effect on the achievement of objectives or delivery of service plans.
- **Step 3 Manage Risks**: put in place control measures and allocate risk manager.
- **Step 4 Monitor Risks**: ensure the controls measures are working effectively or amend accordingly, on an ongoing basis.
- **Step 5 Review and Report**: Review risks and controls at agreed timescales and report to appropriate stakeholders.



4.3 Step 1: Identify Risk – the identification of risk and its consequences.

4.3.1 The Council maintains risk registers to record risks and opportunities that may affect the achievement of objectives. Managers should work with their teams to identify risks and opportunities and record them on the appropriate risk register.

4.3.2 Managers should be aware that risks and opportunities can emerge from a range of sources and should be routinely considered through activities such as:

- Horizon scanning, which can identify changes in the external environment that may affect the delivery of strategic and operational objectives.
- Service planning, which can identify opportunities and risks that may affect the delivery of strategic and operational objectives, priorities and performance measures.
- Performance management discussions, which can identify risks that may impact service delivery, outcomes or performance.
- Team meetings, project boards and programme updates, which can help identify new and emerging risks, changes to existing risks and issues affecting delivery.
- Performance Development Reviews (PDRs) and one-to-one meetings, which provide an opportunity to discuss risks, challenges and opportunities relating to individual roles and responsibilities.
- Customer feedback and complaints, which can provide valuable insight into existing and emerging risks and opportunities for improvement.
- Findings from accident and incident reports.
- Findings from internal and external audit reviews and inspections.
- Findings from insurance claims.

4.3.3 Risk Categorisation

Risks can be grouped into four categories for the purpose of analysis and reporting:

- Risks to the delivery of the Council Plan (strategic risks)
- Risks to the operational delivery of Council services (operational risks)
- Risks to the Council's financial sustainability (financial risks)
- Risks to compliance with legal and regulatory requirements.

4.3.4 Fraud Risk

Local councils manage substantial public budgets, deliver a wide range of services and administer complex tax and benefit systems. These responsibilities expose them to risks arising from internal control failures and external criminal activity.

The Council takes a proactive approach to fraud and requires risk assessments to be undertaken to identify where fraud could occur within services. The findings of these assessments should inform whether identified fraud risks need to be included in Directorate risk registers. A list of established fraud risks is included in **Appendix D**. The list is provided as a guide to potential known fraud risks; however, it is essential that Council Services respond and assess new fraud threats, to prevent losses and to

protect vulnerable people.

4.3.5 When recording risks on the relevant risk register, each risk should be clearly linked to an outcome in the Council Plan (if a strategic risk) or a service plan objective (for directorate or service risks) to assist in the categorisation.

4.3.6 Care should be taken when setting out a risk as, if a risk is not well described (including its origin/cause, the risk event expected to occur and the likely consequences of that event) it could lead to miscommunications and misunderstandings. These could subsequently affect the decisions and/or course of action taken to manage the risk.

4.3.7 Each risk should also be allocated its own unique reference number when it is entered in the relevant risk register (see **Appendix C** for numbering conventions to be used). At this stage the risk register (an example of a risk register is included at **Appendix A**) should include:

- The unique risk number.
- A description of the outcome we are trying to achieve (preferably linked to the Council Plan).
- A description of the risk itself.

4.4 Step 2: Evaluate Risk – the assessment of the risk, based on probability of occurrence and potential impact.

4.4.1 Evaluate each risk to understand their effect on the achievement of objectives or delivery of service plans and to identify those that are most important and merit most attention.

4.4.2 Assess the risk along two dimensions, and allocate a score:

- The **likelihood** (or probability) that the risk will occur
- The **impact** (or severity) that the risk will have if it occurs.

4.4.3 First, undertake an evaluation on the 'inherent risk': the risk before any control measures have been put in place. This gives an uncontrolled/gross/worst case scenario for each risk and illustrates the scale of the risk if all controls were not implemented or were to fail.

4.4.4 The risk is then re-evaluated with the existing controls in place, which provides the 'Residual Risk' as it is now.

4.4.5 It is important at this stage to make sure any existing controls that have been considered have actually been implemented and are working as anticipated to minimise the risk.

4.4.6 It should be remembered that risk by its very definition is uncertain and calculating the level of risk in any situation is at best an estimate. However, if everyone in the Council uses the same scoring criteria it should aid a consistent approach and the most important risks should rise to the top, enabling controls to be prioritised accordingly.

Risk scores are calculated using the following equation:
Likelihood score x Impact score

The Council has adopted a 5 x 5 risk matrix, as defined below.

LIKELIHOOD						
	Almost Certain 5	5	10	15	20	25
	Very Likely 4	4	8	12	16	20
	Likely 3	3	6	9	12	15
	Possible 2	2	4	6	8	10
	Unlikely 1	1	2	3	4	5
		Insignificant 1	Minor 2	Significant 3	Major 4	Catastrophic 5
	IMPACT					

4.4.8 The Council's definitions of the risk scores are included at **Appendix B**. These definitions should be used as a guide to enable risks to be scored consistently across the Council.

4.4.8 High impact risks could include hidden or underestimated threats that can cause serious damage such as fraud, cybercrime, social media, IT failures and problems caused by third parties.

4.4.9 The Council's risk register at **Appendix A** includes the following items which should be assessed at Step 2:

- The consequences of the risk should it happen.
- The control measures that are already in place.
- The target risk score (i.e. the score after existing controls have been applied.

4.5 Step 3: Management – the identification of control measures required and the allocation of appropriate action managers.

4.5.1 The Council determines the appropriate approach to addressing identified risk with reference to its risk appetite. This enables individual employees or departments to understand the limits of risk that the Council is willing to take in any particular aspect of its activities. The Council has clarified its current risk appetite (see below). Risks that have a score equal to or lower than the appropriate risk appetite will be tolerated and monitored. Risks that exceed the risk appetite will be subject to further controls/action.

4.5.2 The Council has a general policy to "accept" and monitor risk that is currently scored as less than "8" on the scoring matrix. Action should be taken on any risk with a score of more than "8" in line with the table shown below:

LEVEL OF RISK	OVERALL RATING	HOW THE RISK SHOULD BE TACKLED/ MANAGED
High Risk	**15-25**	**IMMEDIATE MANAGEMENT ACTION. Effectiveness of risk mitigation should be monitored monthly and mitigation should aim to reduce the risk to at least amber within the next three months.**
Medium Risk	**9-12**	**Plan for CHANGE. Effectiveness of risk mitigation should be monitored at least once every two to three months and mitigation should aim to reduce the risk level to 8 or less within a "reasonable" timescale (ideally six to twelve months).**
Low Risk	**1-8**	**Continue to MANAGE. Monitoring should continue and risk should be monitored at least every six months.**

4.5.3 Risk owners have ultimate responsibility (accountability) for the risk. The owner should be included in the risk register by both name and job role. The owner may differ depending on the level at which the risk is managed. For example, a service-level risk may be owned by a Head of Service or manager, whereas the equivalent risk on the Corporate Strategic risk register will be owned by an Executive Director. The role of the owner involves regularly monitoring the risk status and adjusting risk scores, accordingly, based on current information/intelligence and knowledge.

4.5.4 Mitigating actions (control measures) need to be developed to effectively manage the risk, allocated to appropriate managers and monitored regularly for compliance / implementation by the risk owner. Additional actions should include a timescale for their completion/implementation, and this should be included on the risk register.

4.5.5 It is also possible that risks in one service area can have an impact on other areas of the organisation. It is important to be aware that actions to manage a risk in one area may create or increase a risk in another area. Consideration and communication of any possible impacts on other areas is essential.

4.5.6 At this stage the risk register will have in addition:

- The additional management action planned to bring the risk within the Council's appetite.
- Target score once the additional action is implemented.
- Cost of the risk and the cost of the controls.
- The name and job role of the designated risk owner.

4.6 Step 4: Monitor Risk – ensure the controls measures are working effectively or amend accordingly.

4.6.1 Risk owners should monitor risks on an ongoing basis to ensure that the identified control measures are working effectively. In doing so, it may be useful to ask the following questions:

- **Have the chosen control measures been implemented as planned?**
  - Are the identified control measures in place?
  - Are these measures being used properly?

- Do those who implement and use the controls understand why the controls are necessary?

- **Are the chosen control measures working?**
  - Have the changes made to manage exposure to the assessed risks resulted in what was intended?
  - Has exposure to the assessed risks been eliminated or adequately reduced?
  - Have there been any 'near misses' and have any 'lessons learned' been applied?
  - Do any new controls need to be introduced?

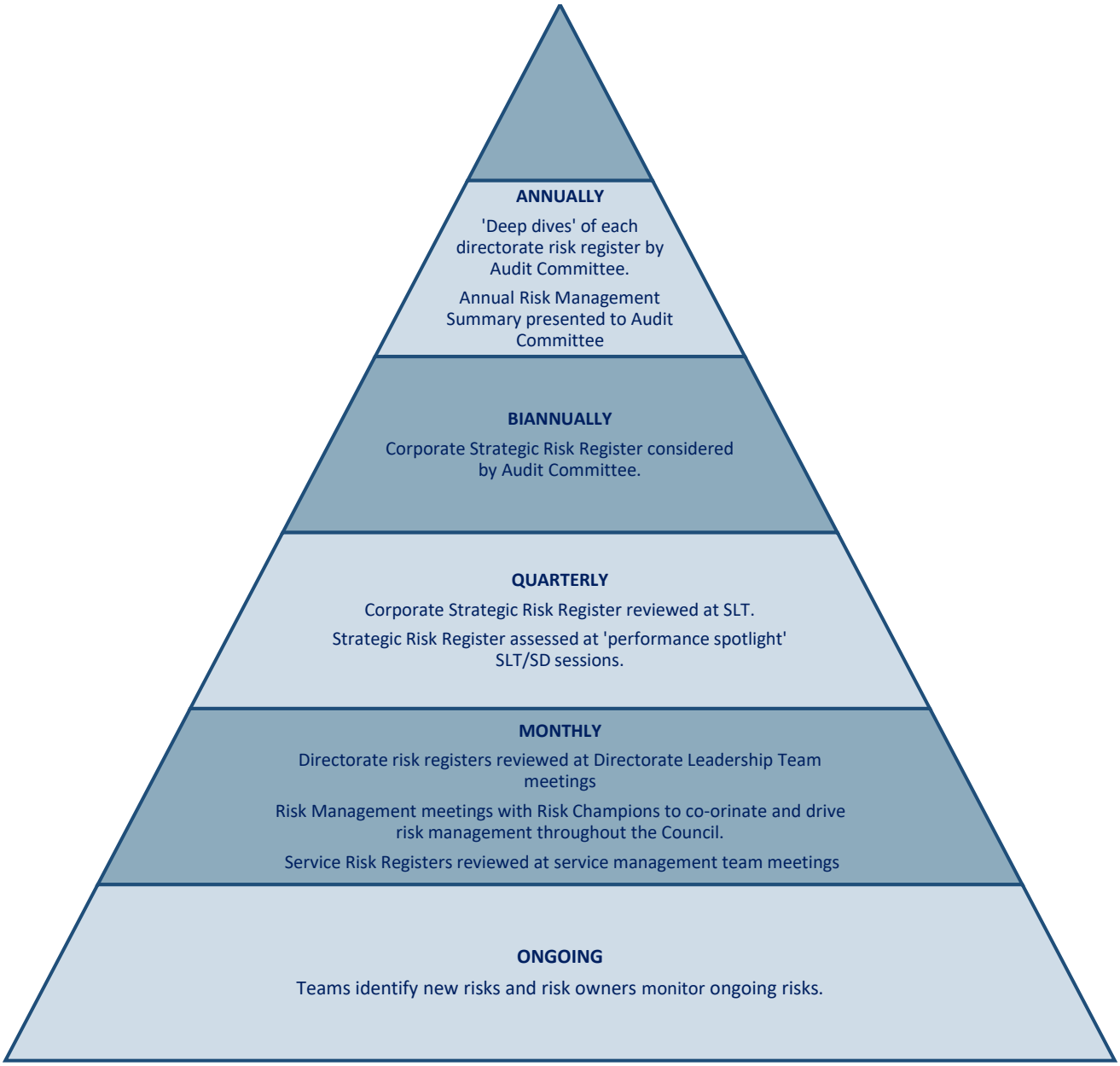
- **Are there any new problems?**
  - Have the implemented control measures introduced any new problems?
  - Do the existing controls need to be reviewed and updated?

4.6.2 It is necessary to monitor the progress in managing risks so that the achievement of objectives is maximised, and losses are minimised. In addition, the effectiveness of risk management controls to reduce the likelihood/impact of adverse risks occurring needs to be assessed and alternative controls introduced if the identified controls are proving ineffective.

4.6.3 When monitoring registers/risks, risk scores should be checked to ensure they are still accurate e.g. are the red rated risks still red and the green rated risks still green? The focus should always be on all risks and not just on red or amber rated risks with the aim of identifying and preventing any risks from becoming a high (red) risk issue.

4.7 Step 5: Review & Report – regular review of risks by risk owners to ensure continued validity of risk registers. Report risks to the appropriate level of management and/or forum to ensure important risk issues are communicated, understood and considered in decision making.

4.7.1 Additionally to the ongoing monitoring of risks, there are timelines in place to review and report risks at the relevant levels (see timeline triangle overleaf).



4.7.2 Changes, including those in corporate and service priorities, may affect risks and opportunities which, therefore, need to be reviewed regularly by asking the following questions:

- Are my risks still the same?
- Are there any new risks arising?
- Has the risk been controlled effectively by the action taken to reduce or eliminate it?
- Has the action (or lack of actions) affected the overall impact or likelihood (score) of the risk?
- Has the inherent risk diminished and can some of the controls be relaxed?
- Are there any other controls required? If so, what are they?

4.7.3 The risk register form at **Appendix A** includes a column to record the next planned review date. Review dates should be in line with the Council's risk appetite (see at 4.5.2). Risk management should be included as an agenda

item on every Directorate Leadership Team meeting so that the team is able to reflect on the risks that they have discussed and amend the risk register if appropriate.

4.7.4 The Corporate Strategic Risk Register is reviewed at least quarterly. Increasing or emerging risks may also be escalated to strategic level from directorate risk registers so that the Council can react effectively to changes in priorities. Risks that might normally be considered for “escalation” to the Corporate Strategic Risk Register include those that need to be managed by more than one directorate, risks that cannot be sufficiently mitigated to their target level using available resources and those that have a ‘red’ risk score. Risks that should not normally be escalated to the Corporate Strategic Risk Register include those risks assessed as ‘amber’ or ‘green’ or those with an impact score of three or less.

4.7.5 Where appropriate, risk owners are responsible for escalating risks and issues through the relevant governance structure to ensure they are appropriately considered for inclusion in the directorate risk registers and, where applicable, the Corporate Strategic Risk Register.

4.7.6 Risks may also be de-escalated from the directorate risk registers and the Corporate Strategic Risk Register when the impact is being effectively managed and risk controls are operating as intended. Where the risk score has reached its target level and the appropriate controls are in place, de-escalation can be considered by the Directorate Leadership Team and the Strategic Leadership Team as appropriate. Reaching the target score alone does not automatically result in de-escalation. Any such decision should consider the wider context, ensuring it remains proportionate and aligned with the Council’s risk appetite and objectives. Any risk that is de-escalated and subsequently removed from a risk register must be formally documented, with the rationale for the decision retained for audit and record-keeping purposes.

4.7.7 Risk Champions play a key role in supporting directorates to maintain and review both the Corporate Strategic Risk Register and directorate risk registers.

4.7.8 The review process includes annual “deep dives” of each directorate’s risk register by the Council’s Audit Committee. The Corporate Strategic Risk Register itself is considered biannually by the Audit Committee, who also receive a year end position on risk management.

4.7.9 The review process will inform the contents of reports to the Strategic Leadership Team and the Audit Committee.

4.7.10 Risk management is a continuous cycle designed not only to identify, evaluate, manage, monitor and review risks, but also to inform and support the budget setting and strategic planning processes.

5. Documentation

5.1 Risks will be recorded on standardised risk register templates in electronic format and held on the central SharePoint site, which can provide access to all risk owners and managers and ensure one version of each risk register is maintained and can be easily updated. It is up to each directorate to decide who should have access to their own risk register.

5.2 Risk Registers are retained once they have been amended. This is done by adding the register to the archive folder in SharePoint to ensure evidence of

risk changes and actions are retained.

6. Leadership, Roles and Responsibilities

6.1 Risk management should not be perceived as the responsibility of a small number of people. Where risk management is fully integrated into the culture and day to day working, everyone has a role to play, and this is what the Council aims to achieve.

6.2 The expectations of members and officers are set out in the diagram overleaf.

COUNCIL

Approve the Council Plan.

CABINET

Approve the Council's Annual Year Ahead Delivery Plan.

Approve the Council's Risk Management Policy.

Overall responsibility for ensuring the Council has in place effective risk management arrangements.

Lead in promoting a risk management culture within the Council and, where appropriate, with partners and stakeholders.

AUDIT COMMITTEE

Approve the Council's Risk Management Guide.

Approve an annual statement on the effectiveness of the Council's risk controls as part of the Annual Governance Statement.

Monitor the effective development and operation of risk management in the authority.

Monitor progress in addressing risk related issues reported to the committee.

Consider the Council's framework of assurance and ensuring that it adequately addresses the risks and priorities of the Council.

POLICY, IMPROVEMENT AND RISK MANAGER

Provide facilitation and support to promote and embed a proactive risk management culture throughout the Council, including clear guidance and processes and annual training programme.

Assist SLT and Service Directors in identifying, mitigating and controlling risks.

Maintain the Corporate Strategic Risk Register.

Ensure that risk management records and procedures are properly maintained, decisions are recorded and an audit trail exists.

Review external and internal audit recommendations relating

SENIOR LEADERSHIP TEAM (SLT)

Champion risk management arrangements and issue direction.

Lead and manage the identification of significant strategic risks and quarterly review of the Corporate Strategic Risk register.

Ensure that there is a robust framework in place to identify, monitor and manage the Council's strategic risks and opportunities.

Ensure that measures to mitigate these risks are identified, managed and completed within agreed time- scales, ensuring that they bring about a successful outcome.

Promote a risk management culture within the Council and, where appropriate, with partners and stakeholders.

Ensure risk is considered as an integral part of service planning; performance management; financial planning; and the strategic policy-making process.

Consider risk management implications in reports, business cases and major projects, including completion of risk assessments where required.

Ensure that appropriate advice and training is available for all Members and staff.

COUNCILLORS

Consider and challenge risk management implications as part of their roles and areas of responsibility

RISK CHAMPIONS

Raise awareness and promote the development of risk management.

Support the development and monitoring of directorate risk registers and any others within the directorate.

Provide updates in line with the reporting timetable.

Support the Policy, Improvement and Risk Manager in the development of risk management across the Council.

Promote consistency across directorates.

DIRECTORATE LEADERSHIP TEAMS (DLT) AND SERVICE DIRECTORS

Lead and manage the identification of significant operational risks from all service areas through monthly reviews of Directorate Risk Registers.

Ensure that the measures to mitigate these risks are identified, managed and completed within agreed timescales, ensuring that they bring about a successful outcome.

Escalate risks/issues to the relevant Executive Directors, where appropriate.

Consider risk management implications in reports, business cases and major projects, including completion of risk assessments where required.

Lead in promoting a risk management culture within the directorate and embed within service areas.

Ensure compliance with corporate risk management standards and corporate risk management processes.

Ensure that all employees, volunteers, contractors and partners are made aware of their responsibilities for risk management and are aware of the

ALL EMPLOYEES

Understand risk and their role in managing risks in daily activities, including the identification and reporting of risks and opportunities.

Support and undertake risk management activities as required.

Attend relevant training courses focussing on risk management.

7. Risk Assurance, Monitoring and Reporting

7.1 Rotherham's risk management function is routinely exposed to full scrutiny and validation:

- In the Annual Governance Statement that is signed off by the Leader and Chief Executive and endorsed by the Audit Committee.
- Elected Members hold the Strategic Leadership Team (SLT) accountable for the effective management of principal risks.
- SLT, and the Audit Committee monitor the delivery of the Risk Management Policy by receiving regular reports and/or presentations. As part of this process SLT and Service Directors review their own risks and update them accordingly.
- Risk management arrangements across the Council are independently reviewed for effectiveness on an annual basis by Internal Audit, which informs the signoff process of the Annual Governance Statement.

7.2 Service and operational risks are monitored and reviewed at directorate level and may be escalated to corporate level if deemed necessary (see paragraph 4.7.4)

7.3 There is a formal reporting structure for advising SLT and elected Members of any risk management implications. The Council's report template requires the completion of a risks and uncertainties section in every report. Managers completing formal reports for Cabinet, Council (and its Committees) as well as SLT should ensure that risks included in this section are reflected on their risk register and that those risks are referenced in the report.

8. Communication

8.1 Effective communication is essential in underpinning every aspect of risk management, from the identification and clear description of risks through to deploying control measures, escalating issues and reporting on progress.

8.2 It is important for strategic leaders and managers to engage with staff across the Council to ensure that:

- Everyone understands the Council's risk policy, risk appetite and risk process in a way that is appropriate to their role. If this is not achieved, effective and consistent embedding of risk management will not be realised, and risk priorities may not be addressed.
- Everyone understands the benefits of effective risk management and the potential implications if it is not done or is done badly.
- Each level of management actively seeks and receives appropriate and regular assurance about the management of risk within their area of control. Effective communication provides assurance that risk is being managed within the expressed risk appetite, and that risks exceeding tolerance levels are being escalated.
- Any organisation providing outsourced services to the Council has adequate risk management skills and processes. Gaining assurance that a partner organisation has embedded risk management processes in place, and that responsibilities are clearly defined from the start, should help to avoid

misunderstandings and any serious problems.

9. Performance Management

9.1 Risk management forms a critical part of the Council's Performance Management Framework. Awareness of potential risks that could impact the achievement of Council priorities and objectives, and planning for such possibilities, will contribute to the successful achievement of the objectives.

9.2 Risks associated with the delivery of the Council Plan are included in the Corporate Strategic Risk Register where relevant.

10. Corporate Governance

10.1 Managing risk is integral to the Council's Corporate Governance processes. It is a key feature in the production of the Annual Governance Statement that is signed by the Leader and Chief Executive.

10.2 There is high level risk management representation on the SLT and at Member level. The Director of Policy, Strategy and Engagement and the Cabinet Member for Finance and Community Safety are the leads for risk management at their respective levels.

10.3 The Policy, Improvement and Risk Manager and the Head of Internal Audit are responsible for drafting the Annual Governance Statement and evaluating risk management assurances and supporting evidence. In this role they report to the Governance Group who have oversight of the process for the statement's production.

10.4 Each directorate has at least one Risk Champion who promotes and supports the development and monitoring of risks within the directorate. The Risk Champions, Director of Policy, Strategy and Engagement and the Policy, Improvement and Risk Manager form the Risk Management Group. This group is responsible for co-ordinating risk management across the Council.

11. Guidance and Training

11.1 All Council staff need to be able to identify and proportionately manage the risks associated with their work. This will mean using knowledge and experience to make decisions on risk. However, it is not a weakness to seek advice and guidance. Having access to guidance and training also helps the Council to implement a consistent approach to risk, a subject where there may be different views and perceptions.

11.2 The Council's Policy, Improvement and Risk Manager is responsible for providing advice and training in respect of the Council's risk management arrangements.

11.3 All members of SLT and their management teams should receive training in risk identification, analysis, and control of risk. Risk management training (including refresher training) is compulsory for all staff of M2 grade and above. Risk workshops can be used as a prime method of educating and training managers in identifying and managing risks to their objectives. This approach can assist in creating a 'risk aware' culture.

11.4 Bespoke risk management training from external providers can be provided free of charge via risk control days for targeted areas of risk.

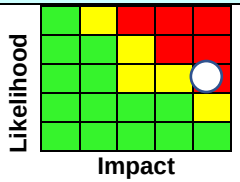
11.5 A risk management E-Learning package is accessible to all staff and Members on the Intranet.

12. Further Information

12.1 For further information on the Risk Policy and Guide or any risk management arrangements please contact either the Policy, Improvement and Risk Manger or your directorate Risk Champion. For contact details click here.

12.2 The risk register template and scoring guide are available on the intranet page, click here.

Appendix A: Risk Register template

	Risk Register Owner: Named SLT member								**Date completed:10/11/2026**					
Risk No	**Business Objective** ***(What is it you would like to achieve/need to deliver?)***	**Risk Detail What is the problem/hazard?** ***What is it that will prevent you from meeting your objectives?***	**Consequence /effect: (*What would actually happen as a result? How much of a problem would it be? To whom and why?***	**Existing actions/controls (What are you doing to manage this now?)**	**Risk Score with existing measures (See scoring table)**			**Current Risk Heat Map**	**Further Mitigations Actions (What would you like to do in addition to your existing controls?)**	**Target Score with further mitigations (See Scoring Table)**			**Cost (of Impact; of current controls; of further controls)**	**Risk Owner (Name and role of Officer responsible for managing risk and controls)**	**Risk Review Date**
					Impact	**Likelihood**	**Risk Rating (I x L)**			**Impact**	**Likelihood**	**Risk Rating (I x L)**			
CORP01	To deliver free and fair elections in which all participants are satisfied that the result is accurate and which allows no opportunity for challenge.	Inability to comply with legislative and statutory election duties.	Election Failure - legal challenge in high court and associated costs of re-running the election and reputational damage. Business continuity issues such as loss of ICT function and /or office accommodation / count venue and / or polling stations	Strong links with internal ICT teams to ensure ICT systems are restored immediately. Training and awareness programme for staff. BCP in Place.	5	3	15		Alternative manual systems have been developed as a back up and can be implemented at short notice. Training and awareness programme for staff. BCP in Place.	3	3	9	There are no costs associated with the controls. Costs will be incurred when actioned.	Manager	Dec-26

Appendix B: Risk Scoring Guidance

LIKELIHOOD	SCORE	*EXPECTED FREQUENCY*
ALMOST CERTAIN	**5**	Reasonable to expect that the event **WILL** undoubtedly happen/recur, possibly frequently and in the current year (next 12 months)
VERY LIKELY	**4**	Event is **MORE THAN LIKELY** to occur. Will probably happen in the current year and be likely to recur in the longer term.
LIKELY	**3**	**SOME LIKELIHOOD** of event occurring. Not likely in the current year, but reasonably likely in the medium/long term.
POSSIBLE	**2**	Event **NOT EXPECTED.** Do not expect it to happen in the current year, but possible in the longer term.
UNLIKELY	**1**	**EXCEPTIONAL** event. This will probably never happen/recur. A barely feasible event.

	IMPACT	SCORE	BENCHMARK EFFECTS
CRITERIA	**CATASTROPHIC**	**5**	• Multiple deaths of employees or those in the Council's care • Inability to function effectively, Council-wide • Will lead to resignation of Chief Operating Officer and/or City Mayor • Corporate Manslaughter charges. • Service delivery has to be taken over by Central Government. • Front page news story in National Press. • Financial loss over £10m
	MAJOR	**4**	• Suspicious death in Council's care • Major disruption to Council's critical services for more than 48hrs (e.g. major ICT failure) • Noticeable impact in achieving strategic objectives • Will lead to resignation of Executive Director and/or Executive Member • Adverse coverage in National Press/Front page news locally • Financial loss £5m - £10m
	SIGNIFICANT	**3**	• Serious Injury to employees or those in the Council's care • Disruption to one critical Council Service for more than 48hrs • Will lead to resignation of t Service Director/ Project Director • Adverse coverage in local press • Financial loss £1m - £5m
	MINOR	**2**	• Minor Injury to employees or those in the Council's care • Manageable disruption to internal services • Disciplinary action against employee • Financial loss £100k to £1m
	INSIGNIFICANT	**1**	• Day-to-day operational problems • Financial loss less than £100k

Note: The benchmark effects are provided as guidance and a risk does not need to satisfy every benchmark within a category to be assigned

that impact rating. For example, a risk that could result in a financial loss of more than £10 million may be assessed as having a catastrophic impact even if the other catastrophic benchmark effects would not occur. Professional judgement should be applied when determining the most appropriate impact score.

Appendix C: Risk Numbering Protocol

This protocol sets out how the numbering requirements in the Risk Policy and Guide are to be applied in practice.

1) Risk numbers should never be “reused”. If a risk is deleted from a risk register, the number should not be allocated to a new risk

2) All risks should follow an alpha numeric numbering system which should be set out as follows:
   - risks included on the Corporate Strategic Risk Register will be numbered sequentially in the following format – SLTxx – where xx is a sequential number
   - risks included on Directorate Risk Registers should follow the following formats:

Directorate	**Numbering format**
Children and Young People’s Services	CYPSxx
Corporate Services	CORPxx
Regeneration and Environment	R&Exx
Policy, Strategy and Engagement	PSExx
Adult Care, Housing and Public Health	ACHPHxx

3) Directorates may vary the alphabetical descriptor for risks that only appear on service risk registers if that eases operation of the risk register. However, the format should always be alpha numeric following the format above.

4) Directorate risk registers should also include an indication of whether a risk is also on the Corporate Strategic Risk Register. This can be achieved either by including on the directorate risk register the “SLT”xx" number or by including strategic risks on a separate tab in the directorate risk register. Directorates can choose which approach is used as long as the relevant register clearly shows which risks are on the register.

Appendix D: Fraud Risk List

Social Housing & Tenancy Fraud	**Illegal Subletting:** Council tenants renting out their social housing property to third parties for private profit. **Application Fraud:** Falsifying identity, income, or personal circumstances to jump the waiting list or illegally secure a tenancy. **Housing Benefit Fraud:** when a person or landlord intentionally gives false information or hides a change in circumstances (undeclared work, hidden savings, undeclared partner, fake rent, wrong address) to get Housing Benefit money they do not deserve. **Right to Buy Fraud:** Falsifying occupancy or sourcing illicit funds to buy council properties at steep, taxpayer-subsidised discounts
Procurement & Commissioning Fraud	**Bid Rigging and Collusion:** Contractors conspiring to artificially inflate prices or divide contracts during the local authority tendering process. **Management of Contracts (services, goods & works delivery):** Where contracts are not delivered as per agreed contract (incl. social value) i.e. poorly managed or oversight is weak, allowing opportunities for collusion, overcharging, substitution of inferior goods or services, false invoicing, duplicating invoices, or payment for work not completed.
Social Care Fraud	**Adult Social Care Fraud:** Misuse of direct payments intended for vulnerable individuals' care, care workers claiming money for time not worked, concealment of funds by resident to avoid paying residential or community provision, or care homes inflating the number of residents or care hours delivered. **Financial Abuse of Vulnerable Individuals:** The Council manages care for some vulnerable residents and for several clients administers their financial affairs. These care and support arrangements or guardianship orders (any arrangements where a child or young person is reliant on any individual), may be exploited by individuals for their own purpose **Grant Fraud:** Where grant funds are deliberately used for purposes other than those for which they were awarded, or where false or misleading information is provided to obtain or retain funding. **Immigration/No Recourse to Public Funds:** False entitlement to services or payments, including risks associated

	with sham marriages, misrepresentation of immigration status or residency and misuse of identity documents. Fraudulent claims of eligibility, identity or circumstances to access support from the authority where entitlement is restricted or highly dependent on accurate status information.
Revenue & Tax Fraud	**Council Tax Discretion Evasion:** Individuals falsely claiming Single Person Discounts (usually a 25% reduction) or other local council tax support discounts when they are not eligible. **Business Rates Evasion:** Deliberate withholding of information, shifting assets, or using shell companies to falsely claim Small Business Rate Relief or empty property exemptions
HR & Insider Fraud	**Payroll and Expenses:** Staff fabricating overtime, submitting false travel and expense claims, or creating "ghost employees" to siphon funds. **Recruitment Fraud:** Job applicants lying about their identities, right to work, qualifications, or criminal histories. **Bribery, Collusion and Corruption:** Council officers or elected councillors accepting kickbacks from property developers or suppliers to tilt planning permissions or contracts in their favour.
Cyber-Enabled & Emerging Fraud	**IT Attacks:** Criminal access to internal systems by 3rd parties for electronic data theft or harvesting. **AI-Generated Fabrications:** Fraudsters using artificial intelligence to create highly convincing digital identity documents or deepfake communications to claim localised grants or welfare and extort funds. **Mandate Fraud (Invoice Redirects):** Criminals impersonating a legitimate, major council contractor or supplier to convince finance teams to change bank details to a fraudster's account **Whaling:** When senior council officers are targeted and impersonated to obtain fraudulent payments or sensitive information.
Asset or Financial Fraud	**Money Laundering:** Where monies from criminal activities are cleaned by using them to buy legitimate Council assets or pass through a business so that the funds look like legitimate transactions. **Insurance Fraud:** includes any insurance claim that is proved to be false, made against the organisation or the organisation’s insurers e.g. for accidents or damage **Blue Badge Fraud:** Where someone applies for a disabled persons parking badge but isn't entitled to it, or where a

	legitimate blue badge is misused by a party or is used in circumstances in which they are not entitled to use it. **Theft of Assets via Abuse of Position:** Where existing or newly purchased assets are stolen/redirected by a Council employee and then sold for profit or used for themselves. This could be via direct access to stock/equipment or by manipulating the procurement system. This could include purchasing fuel using Council funds and using it for non-Council activity.