Herefordshire Council

Draft Risk Management Strategy

AUTHOR(S):
Director of Finance
Head of Corporate Performance and Intelligence

DATE
September 2024

NEXT REVIEW DATE
September 2025

Contents

Introduction

In an ever-evolving landscape marked by economic uncertainty, regulatory changes and shifting public expectations, Herefordshire Council (‘the council’ hereinafter) recognises the need to adopt a robust risk management strategy to safeguard public interests, enhance service delivery and ensure sustainable development. Effective risk management is not just a regulatory requirement; it is a critical tool for resilience, enabling the council to anticipate potential threats, mitigate adverse impacts and maximise opportunities. Moreover, mitigating against the risk of missed opportunities and non-action can be just as important as mitigating against the risks of actions that could cause potential harm.

Risk is unavoidable. By integrating risk management into strategic planning and operational decision-making, the council can navigate complex challenges; from financial pressures and cyber threats to climate change and public health crises. A proactive risk management strategy will not only protect public assets and services but will also provide valuable assurance to residents, partners, and stakeholders that effective risk management arrangements are in place. This approach ensures that the council remain agile, responsive and prepared to thrive amidst uncertainty, delivering value and improving outcomes for the communities they serve.

Aims and Objectives

A proactive and responsive risk management strategy will support organisational resilience; safeguarding public interests whilst maintaining service quality and operational efficiency.

Aims

- Protect public interests: ensure the safety, health and well-being of residents, visitors and businesses across the county through the identification, assessment and effective management of risks.

- Enhance service delivery: maintain and improve the quality and continuity of public services by minimising the impact of risks that could disrupt operations or reduce service standards.

- Safeguard public assets and resources: protect the council’s physical, financial and human resources, including infrastructure, data and intellectual property, from potential threats and losses.

- Promote good governance: embed a culture of risk awareness and management across the council; ensuring accountability, transparency and compliance with statutory obligations.

- Support strategic objectives: align risk management practices with the council’s strategic priorities and objectives, fostering resilience and adaptability in a changing environment.

Objectives

- Develop a comprehensive risk management framework: establish a clear, systematic approach to risk identification, assessment, mitigation, monitoring, and reporting that is integrated into all levels of the council.

- Identify and assess risks: regularly identify and evaluate risks that may affect the council’s ability to achieve its objectives, including financial, operational, reputational, environmental and regulatory risks.

- Implement effective mitigation measures: develop and implement appropriate risk mitigation strategies, including risk avoidance, reduction, transfer and acceptance, tailored to the nature and severity of each risk.

- Promote risk awareness and training: provide regular training and guidance to employees and elected members to ensure a thorough understanding of risk management principles, practices and their roles in managing risks.

- Monitor and review risk management processes: regularly review and update risk registers, management plans, and controls to ensure they remain effective, relevant, and aligned with the council’s evolving risk profile.

- Enhance decision-making: integrate risk management into the council’s decision-making processes, ensuring that risks are considered when developing policies, projects, and partnerships.

- Ensure compliance and accountability: ensure compliance with relevant legislation, regulations, and standards while promoting a culture of accountability where risk management is seen as everyone’s responsibility.

- Foster resilience and business continuity: develop and maintain robust business continuity and emergency response plans to ensure the council can respond effectively to incidents and crises.

- Risk reporting: establish a robust hierarchy of risks, and regularly report on the risks to all levels of the organisation, including service managers, directorate leadership teams, Corporate Leadership Team and elected members.

What is risk management?

Risk is ‘the effect of uncertainty’, and risk management is ‘the coordinated set of activities and methods that is used to direct [the council] to control the risks that affect its ability to achieve the objectives’.[1] Risk management for the council involves identifying, assessing, managing and mitigating risks that could impact the delivery of services, projects or statutory duties. The council is responsible for a wide range of services, such as social care, education, housing, waste management, and public safety. Good risk management helps ensure these services are delivered effectively, safely and within budget, while also maintaining public trust.

Examples of risks include (not an exhaustive list):

- Financial risks: budget/funding reductions or unexpected costs.
- Reputational risks: negative media coverage, public dissatisfaction or failure to meet statutory duties.
- Operational risks: disruption of services, technological system failures, data breaches or infrastructure damage.
- Compliance risks: non-compliance with laws, regulations or statutory duties.
- Political and social risks: changes in central government policy, demographic shifts or social trends that affect long-term planning.
- Environmental risks: extreme weather events, climate change impacts or sustainability challenges.

Regulatory and Best Practice Frameworks
The council is guided by frameworks and standards such as:

- The Chartered Institute of Public Finance and Accountancy (CIPFA) Delivering Good Governance in Local Government Framework: offers guidance on good governance and risk management practices.
- The Public Sector Internal Audit Standards (PSIAS): provides standards for internal audit functions, including the assessment of risk management processes.
- ISO 31000: an international standard for risk management, which many local authorities adopt to structure their approach.

[1] *Source: ISO 31000 ‘Risk Management – Principles and guidelines’*

Types of Risks

The council will identify the type of risk under four broad categories as below. It is possible for a risk to apply to more than one category.

Type of risk	Description	Examples
Internal	These are risks over which the organisation has some control, for example risks that can be managed through internal controls and, where necessary, additional mitigating actions. This often involves traditional risk management, such as risk registers, controls and assurance.	Fraud, health & safety, legal & regulatory, information security, data protection, safeguarding, contracts, people capability & capacity.
External	External risks represent significant events/perils and their impact on organisational resilience. The approach to managing external risks is through considering the impact those external events could have on infrastructure, finance, people, operations and reputation. A common example is a business continuity plan.	Economic downturn, central government cuts, terrorist attack, extreme weather, cyber-attacks.
Strategic	Strategic risks represent risks to the timely achievement and delivery of priorities and objectives of the council's Council Plan and associated Delivery Plan.	These can be immediate impact risks to the organisation's ability to continue operating, e.g. loss of customer data; or slow-burning risks that grow and eventually prevent delivery of objectives, e.g. staff turnover or leadership capability.
Major programmes and projects	Major projects form such a critical part of the plans for the council and should have their own risk management arrangements in place aligned to the programme/project governance arrangements. Risks identified in respect of significant projects should be escalated as required.	These risks will be specific to the major project in question and could involve shifting requirements, budget overspend, slippage in delivery timeframes, failure to deliver. *Project and programme risks have separate guidance, available from the Project Management Office. Significant project and programme risks are escalated in the directorate risk registers.*

Roles and Responsibilities

Role	Responsibilities
Cabinet	• Has the ultimate accountability for risk and related control environment • Sets the direction in the Council Plan and articulate risk appetite to realise those objectives through the Council Plan's Delivery Plan in line with the risk management strategy • Oversees the effective management of risk by officers • Upholds the responsibilities within the risk management strategy • Reviews regular reports from the Audit and Governance committee • Considers the risks in all decision-making • Individual Cabinet members should also regularly review risks within their portfolio as part of Cabinet Member Briefings
Audit and Governance Committee	• Approves the risk management strategy • Approves the Corporate Risk Register on a quarterly basis and monitor its progress • Receives assurance that effective risk management arrangements are in place • Approves the Annual Governance Statement It is not a function of the committee to examine specific risks in detail, but satisfy itself that risk management in the council is operating effectively. Should the committee have a concern about the scoring or detail of the risk, it might refer back to officers attending the committee.
Corporate Leadership Team	• Owns the council's Corporate Risk Register • Monitors and review risks on the corporate risk register on a quarterly basis ensuring adequate response • Challenges one another in their delivery of activity which effectively mitigates identified risks • Articulates risk appetite • Champions and drives the effective management of risk across the council • Ensures the corporate risk function is supported in carrying out its role
Internal Audit	• Provides independent assurance on the effectiveness of the organisation's risk management arrangements • Shares good practice through comparative assessment across the local government sector
Risk Manager	• Proactively identifying, assessing, monitoring and reviewing corporate risks in collaboration with the Corporate Leadership Team and maintaining the registers associated with these risks • Assessing risks for inclusion on the corporate risk register from the directorate risk registers, strategic risks and external risks • Ensuring a consistent approach on the scoring of risk

	• Considering any risks identified in internal and/or external audit reports and challenging directorates on their inclusion • Undertaking a regular review of national risks and considering local implications • Ensuring there are plans in place to mitigate and control risks, and that they are being closely monitored, managed and reviewed • Reporting corporate risks to the Corporate Leadership Team and the Audit and Governance Committee • Undertake risk review requests on decision reports for Cabinet • Provide advice on operational risks as requested and during the service planning processes, and advise on when to escalate the risks • Adhering to, reviewing and updating the risk management strategy • Monitoring compliance with regulation and legislation • Promoting risk awareness across the council through clear communication and training, e.g. e-learning and workshops
Corporate and Service Directors	• Have clear understanding of the risks to the business • Assess risks and have a clear action plan on mitigating against risks depending on the level of council's risk appetite, and ensuring the implementation of the action plan • Monthly reviews of risks and maintaining a directorate risk register • Accountable for effective risk management within their directorate • Escalate risks to the corporate register as appropriate • Responsible for providing cabinet members of the oversight of significant risks within their portfolios
Heads of Service and Service Managers	• Accountable for effective risk management within their service • Identifying risks in the service delivery planning processes, and on an ongoing basis • Assessing and mitigating against risks according to the risk appetite of the council • Escalating risks to the directorate risk register as appropriate • Maintaining a live service risk register
Risk Owners	Risks owners are Service Manager or above
All Staff	• Responsibility to be risk aware; to identify, assess, manage and review risk effectively in their job • Report/ escalate potential hazards or risks to their managers • Work to mitigate risks and to work within the appropriate risk management guidelines

Risk Appetite

Risk Appetite Statement

Herefordshire Council is committed to delivering high-quality services to our community while ensuring the safety, wellbeing, and financial stability of the council. The risk appetite matrix outlines our approach to risk-taking, setting clear boundaries for the levels of risk we are willing to accept in pursuing our strategic objectives and will always be dependent on the specific circumstances of the risk. It provides guidance to staff and decision-makers on acceptable risks, ensuring that we balance innovation and service improvement with prudent management of resources.

If the risk values approach or exceed the specified appetite for risk, there must be escalation to the Corporate Leadership Team.

Risk Appetite Matrix

The four levels of risk appetite are as follows:

- Averse: Avoidance of risk and uncertainty wherever possible.
- Cautious: Tolerance for risk taking is limited to those events where there is little chance of any significant adverse impact.
- Aware: Tolerance for decisions with potential for significant risk, but with appropriate measures to minimise exposure and deliver benefits.
- Hungry: Eager to be innovative and to choose options offering potentially higher business rewards, despite greater inherent risk.

See Appendix B for the council’s risk appetite matrix.

Risk Management Process

Identifying Risks

All staff must systematically identify potential risks across all service areas, activities, projects and programmes. Considerations of risks in the national risk register and external factors must also take place during the monthly update of the service, project, directorate and corporate risk registers.

Risks can emerge at any point and from various sources and processes. Risks should also be given particular attention as part of service business planning, but it is not necessary that all risks must originate from a service risk register. External and strategic risks can be identified at directorate or corporate level that is not service-specific, such as, a pandemic.

The mechanism used to identify risks may vary, but might include SWOT (strength, weakness, opportunity and threat) analysis or PESTLE (political, economic, social, technological, legal and environmental) analysis. It is vitally important that the risk clearly identifies the impact it will have on achieving the council objectives, and the potential consequences.

Risks are often identified as a result of audit activity, and at this stage mitigating activity is typically agreed. Risks are also identified as part of decision reports. Risks emerging from decision reports and audits should be discussed by managers at all levels and an assessment undertaken as to whether they should be included in the relevant risk register.

Assessing Risks

After identifying risks, the next step is to assess the risks in terms of their likelihood and potential impact. This involves a scoring exercise from 1 to 25 utilising the assessment criteria below to assess the probability and the severity of potential consequences.

			IMPACT				
			Catastrophic	Major	Moderate	Minor	Minimal
			5	4	3	2	1
LIKELIHOOD	(Almost) certain	5	25	20	15	10	5
	Likely	4	20	16	12	8	4
	Credible	3	15	12	9	6	3
	Unlikely	2	10	8	6	4	2
	Highly unlikely	1	5	4	3	2	1

Risk Scoring – Likelihood

A timeframe within the next 12 months should be considered.

Score	Likelihood	Assessment criteria
5	(Almost) certain	The event is expected to occur or occurs regularly.
4	Likely	The event will probably occur (significant chance)
3	Credible	The event may occur (realistic chance)
2	Unlikely	The event may occur in certain circumstances (unlikely chance)
1	Highly unlikely	The event may occur in only rare circumstances (remote chance)

Risk Scoring – Impact

Score	Impact	Assessment criteria
5	Catastrophic	Potential to threaten the existence of a service Budgetary issues that cannot be resolved Death of employees or a member of the public Inability to function effectively, council-wide Central government intervention
4	Major	Widespread medium to long-term impact on operational efficiency, performance and/ or reputation Major disruption to council's critical services for more than 48 hours (e.g. major ICT failure) Breach of legal or contractual obligation attracting medium-term attention of legislative or regulatory bodies Adverse coverage in national press/ front page news locally Budgetary issues that can only be resolved by Section 151 Officer/ Chief Executive/ Members in accordance with the finance procedure rules Serious injury to employees or members of the public
3	Moderate	Significant loss, delay or interruption to services Disruption to one critical council service for more than 48 hours Non-delivery of corporate and service plan objectives during a quarter Significant stakeholder concern Attracting short-term media attention and potential for litigation/ prosecution from legislative or regulatory bodies Long-term regional damage to reputation Budgetary issues that can be resolved at directorate level in accordance with financial procedure rules Injury to employees or members of the public Significant complaints
2	Minor	Budgetary issues that can be resolved within service in accordance with the finance procedure rules Manageable disruption to services Noticeable internal impact, but the service would remain on course to achieve priorities for the year Localised reputational damage
1	Minimal	Day to day operational problems that can be dealt with relative ease

Addressing Risks

Following the assessment of a risk, the next step is to develop and implement strategies to manage and mitigate identified risks. Risk treatments include:

- Avoidance: taking steps to eliminate a risk entirely (e.g., discontinuing or not starting a risky activity)

- Removal: removing the risk source

- Reduction: implementing controls or measures to reduce the likelihood or impact of a risk (e.g., improving internal controls, enhancing staff training)

- Transfer: transferring the risk to a third party (e.g., through insurance or outsourcing)
- Acceptance: accepting the risk if it falls within the council's risk appetite, is deemed manageable and/ or by informed decision in pursuit of an opportunity

Where the risk is significantly outside our control, preparation for emergencies and contingencies will need to be made. This includes but is not limited to:

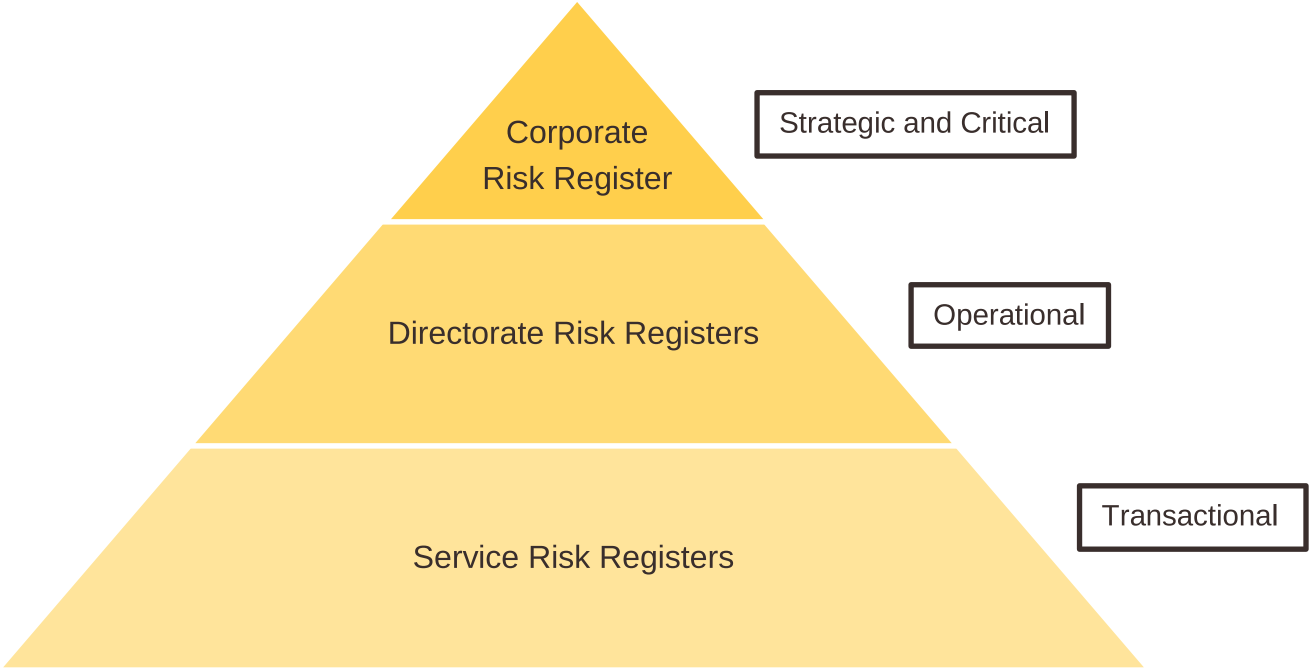
- Develop business continuity plans and disaster recovery plans to address risks associated with emergencies, such as natural disasters, cyber-attacks, or public health crises
- Conduct regular tests and drills to ensure readiness for unforeseen events

Monitoring and Reviewing Risks

Risk treatments, even if carefully designed and implemented might not produce the expected outcomes and could produce unintended consequences. Monitoring and reviewing risks need to be an integral part of the risk treatment implementation to give assurance that the different forms of treatment become and remain effective.

Risk registers are a documented list of identified risks, their assessments, and mitigation strategies (see Appendix A for a template of a risk register). Risk registers should be a live document, with a minimum of monthly reviews. This process ensures that risks are identified, managed and escalated in a timely manner.

There are 3 levels of risk registers in the council:



It is not necessary that all risks originate from the service risk register; risks can be identified at any level, and can remain monitored by that level even if the score is relatively low, for instance risks that affect more than one service can be included in the directorate risk register. Likewise, risks that are council-wide, such as cyber security threats, will be included in the corporate risk register.

The maximum score that is monitored at each level before escalation becomes mandatory is as follows:

Service Risk Register: 7
Directorate Risk Register: 14
Corporate Risk Register: no maximum

Closing risks
Whilst some risks will be ever-present, as work is done to mitigate risks, some risks will reach a point where they no longer need to be monitored. At this stage, the risk should be moved to a list of accepted risks in the risk register for 12 months.

Reporting Risks

Register	**Reviewer(s)**	**Minimum Frequency of Reporting**
Service Risk Register	All staff within the service; Heads of Service; and Service Managers	Monthly
Directorate Risk Register	Directorate Leadership Team	Monthly
Corporate Risk Register	Corporate Risk Team; Corporate Leadership Team; Audit and Governance Committee; Internal Audit	Monthly by the Corporate Risk Team; Quarterly for other reviewers

Herefordshire Council

Appendix A – Risk Register Template

(Corporate Risk Register to be completed at CLT workshop)

Risk reference number	Risk description	Date opened	Target risk score	Risk score before controls	Existing controls in place	Risk score after controls	Risk appetite	Further counter measures required	Residual risk trend (12 months)	Risk owner
R001	**Risk title** Short description *Outline potential consequences should the risk be realised* Type of risk	DD/MM/YY		Impact x Likelihood		Impact x Likelihood				

Appendix B – Risk Appetite Matrix

(to be completed at CLT workshop)

Risk Area	Definition	Appetite Level	Commentary
Financial Management			
Regulatory Compliance			
Operational Risk			
Staff Safety and Wellbeing			
Public Health and Safety			
Reputational Risk			
Environmental Impact			
Digital Transformation			
Cyber Security			
Partnership and Collaboration			
Economic Growth			