Wiltshire Council

Wiltshire Council

Risk Management

Policy

February 2024

Document control

Reference Number	1.0	Status	Draft
Sponsor(s)	Corporate Governance Group	Author(s)	Catherine Pink
Document objectives	To establish a comprehensive and robust risk management structure across Wiltshire Council.		
Intended Recipients	Leaders, Councillors and staff of Wiltshire Council. Specifically, Cabinet, CLT and Heads of Service.		
Group/Persons Consulted (to 26/01/2024):		Audit and Governance Committee; Corporate Governance Group; Environment Directorate; Assets Directorate; Occupational Health and Safety; Executive Office.	
Ratifying Body	Cabinet	Date Ratified	XXXX
Date of Issue	XXXX		
Next Review Date		February 2025	
Contact for Review		Catherine Pink, Corporate Support Manager Martin Nicholls, Head of Executive Office	

Wiltshire Council Risk Management Policy

Table of Contents

Introduction

1. Wiltshire Council's vision is to ensure that the people of Wiltshire are empowered to live full, healthy and enriched lives; to ensure our communities continue to be beautiful and exciting places to live; to ensure our local economy thrives and is supported by a skilled workforce; and that we lead the way in how councils and counties mitigate the climate challenges ahead. We will achieve this through prevention and early intervention, improving social mobility and tackling inequalities, understanding our communities, and working together to design and deliver our services.
2. Wiltshire Council uses risk management alongside performance management, robust internal controls, service planning, and strong priority-based financial management to ensure that the work undertaken by the Council's services and partnerships is delivering the stated priorities of the Council, whilst maximising the use of available resources.

Definition of Risk Management

3. Risk is the effect of uncertainty on objectives, which may be either threats or opportunities. Risk management is the planned and systematic approach to identifying and addressing that uncertainty, with the goal of anticipating events, adapting to change, increasing the probability of success and reducing the probability of failure in achieving objectives. This is achieved by identifying and minimising threats, whilst also maximising any opportunities that arise.

Policy Statement

4. The Council recognises and accepts its responsibilities and statutory obligations to manage risks effectively, in order to protect its assets and employees, minimise uncertainty in achieving its goals and objectives, and maximise the opportunities to enhance the value of services to the community and achieve its Business Plan.
5. Risk management is an integral part of the Council's corporate governance arrangements, falling under both the first and second lines of defence of the Council's assurance framework, under the Local Code of Corporate Governance set out in Protocol 9 of the Council's Constitution.
6. The Council has committed to ensuring that risk management is built into decision making and business planning to provide a sound system of internal controls, part of its aim for delivering continuous improvement.
7. The Council is risk aware rather than risk averse, recognising that some risks can never be fully eliminated, and that avoidance of risk can mean that opportunities are missed.
8. This policy therefore provides a structured approach to risk management that does not seek to have zero or rapidly closed risks, but which proactively uses risk management to balance opportunity and risk, and is seen as adding value to service delivery and enabling change.

9. The Council will seek to minimise unnecessary risk and have an appetite to manage residual risk to a level commensurate with its responsibilities as a public body.

Scope

10. This policy applies to all Directorates, Services, and Departments run by the Council.

Aims and Objectives

11. The aim of risk management is to ensure that the Council has a good understanding of risks and opportunities and their likely impact, allowing for more effective decision making.

12. The objectives of this Risk Management Policy are to:

- Provide clear criteria to standardise the risk process operating at all levels across all services.
- Establish clear roles, responsibilities, and reporting lines for risk management within the Council.
- Raise awareness of the need for effective risk management, and integrate risk management into the culture of the Council.
- Minimise loss, disruption, damage, injury and reduce the cost of risk, thereby maximising resources.
- Enable decision makers to anticipate, identify and evaluate emerging threats and opportunities, allowing them to consider mitigating factors and adapt plans accordingly.

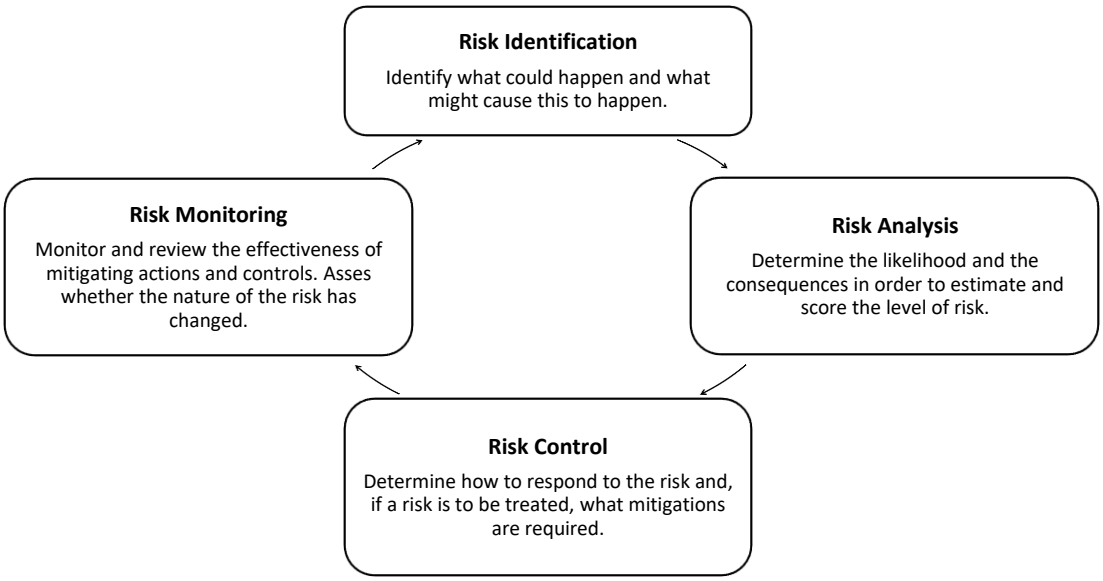
Benefits of Risk Management

13. Benefits gained from effectively managing risk include:

- *Improved strategic management* – Improved decision making and a greater ability to deliver against objectives and targets.
- *Improved operational management* – A reduction in managerial time spent dealing with the consequences of a risk event having occurred.
- *Improved financial management* – Better informed financial decision-making and a reduction in costly claims against the Council.
- *Improved services* – Identification of opportunities to implement improvements in service provision, acting as an enabler of change.
- *Improved transparency* – Clearly defined risk management processes ensure accountability, integrity, and trust in the Council's robust internal controls.
- *Improved customer service* - Minimal service disruption to customers and a positive external image as a result of all of the above.

Risk Management Cycle

14. There are four stages of risk management that form an ongoing risk management cycle:



15. Risk management is a planned and systematic process that starts with the identification and definition of a risk in relation to uncertainty in the Council's ability to achieve its strategic priorities and operational responsibilities, followed by analysis and evaluation of the potential likelihood and impact of the risk.

16. Once a response to a risk has been determined and a decision made to treat or transfer the risk, appropriate mitigating actions should be identified and implemented with the intention of reducing the risk score to a target level at or below the agreed appetite for the risk.

17. Risks should then be regularly reviewed, monitored and reported on. Importantly, this phase of the cycle should include regular assessment of the effectiveness of planned mitigations in terms of reducing the likelihood of a risk occurring or the impact should the risk occur.

18. The cycle is completed by regular horizon scanning to identify any emerging or new risks, and the impact of any changes to existing risks.

Roles and Responsibilities

19. Roles and responsibilities for managing risk are set out in the table below. In general:

- The overall monitoring and management of risk across the Council at the strategic level, including direct responsibility for the risks themselves, is owned by the **Corporate Leadership Team.**
- The accountability and responsibility for owning, identifying, recording, monitoring and managing risk sits with **Directors and Heads of Service**.
- Responsibility for holding the Corporate Leadership Team to account for effective management of risks and oversight of risk management processes rests with **Elected Members** sitting on specific committees.

Elected Members	
Leader of the Council	Identified in Part 3 (3.3.2.6) of Wiltshire Council's constitution as responsible within the Budget and Policy framework for probity and financial monitoring and risk management.
Cabinet member for Finance, Procurement, IT and Operational Assets	Identified in Part 3 (section C, appendix 2) of Wiltshire Council's constitution as responsible for Performance and Risk.
Cabinet	Holds the Corporate Leadership Team accountable for the effective management of risks by officers and of decision making based on performance evaluation. Approves relevant risk management policies. Reviews the Strategic Risk Register every quarter. Reviews any significant changes to corporate risks every quarter. Identified in Protocol 10 (area 7) of Wiltshire Council's constitution as having executive responsibility for governance reporting arrangements in relation to risk management.
Audit and Governance Committee	Identified in Part 3 (2.7.9.10) of Wiltshire Council's constitution as responsible for monitoring and reviewing the effective development and operation of corporate governance, risk, and performance management and internal control, and to receive progress reports as required. Identified in Protocol 10 (area 7) of Wiltshire Council's constitution as having non-executive lead responsibility for governance reporting arrangements in relation to risk management. Responsible for considering review findings from internal audits and ensuring that any identified weaknesses in arrangements for risk management are being properly addressed, in line with the 'third line of defence'.
Overview and Scrutiny Management Committee and any relevant Select Committees and/or Task Groups.	Review and scrutinise the quarterly Cabinet Risk reports to question members and officers about decisions and risks, providing independent checks and balance.
All members	Understand the principles of risk management and consider risk assessment as part of the decision-making process.
Corporate Officers	
Corporate Directors	Champion risk management across the Council.
Corporate Leadership Team (CLT)	Take responsibility for the Risk Management Policy and related guidance, in line with the 'second line of defence'.

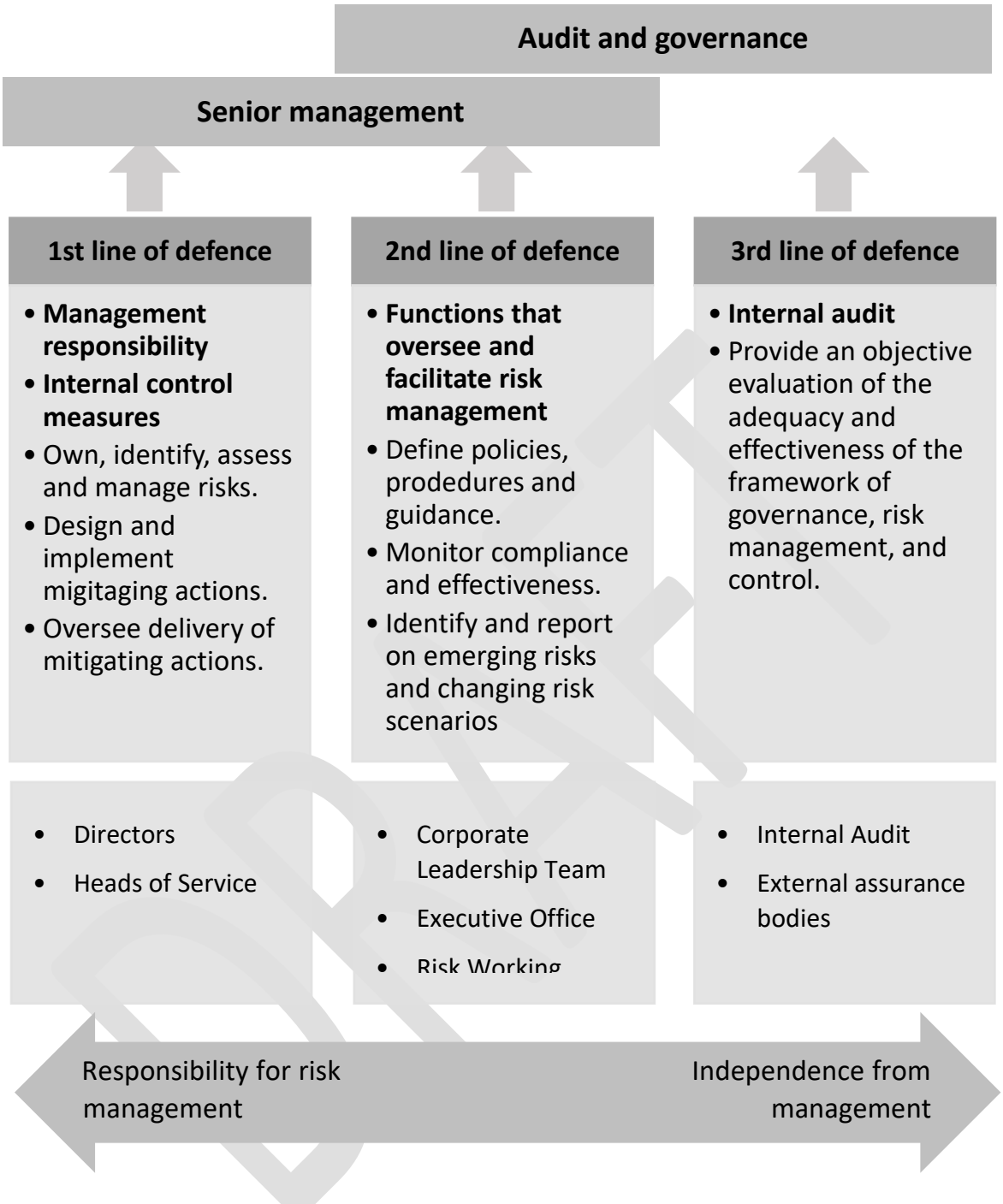
	Ensure a consistent approach to risk management across the council. Consider regular reports on the Council's risk management arrangements and major changes in risks with exception reports as appropriate. Own and approve changes to the Strategic Risk Register.
Chief Finance Officer	Identified in Part 9 (5.3.8) of Wiltshire Council's constitution as responsible for risk management in consultation with the Director of Legal and Governance and the Director with responsibility for Human Resources and Organisational Development. Identified in Part 9 (24.1) of Wiltshire Council's constitution, as part of risk management, as responsible for ensuring that proper insurance exists where appropriate, and that the Council has sufficient funds to meet potential liabilities and costs.
Director of Legal and Governance	Identified in Part 9 (22.1) of Wiltshire Council's constitution as responsible for managing and maintaining the Council's Risk Management Policy Statement and Strategy, reviewing its effectiveness, advising the Chief Executive and Corporate Directors, Directors, Cabinet and promoting robust and effective risk management throughout the Council. Identified in Part 9 (24.1) of Wiltshire Council's constitution, as part of risk management, as responsible for ensuring that proper insurance exists where appropriate, and that the Council has sufficient funds to meet potential liabilities and costs.
Directors for Finance and Corporate Functions & Digital	Responsible for the effective reporting of Performance and Risk Management in combination with Financial Management.
Directors	Have primary ownership, responsibility and accountability for identifying, assessing and managing risks, in line with the 'first line of defence'. Take ownership of directorate risk registers. Identify individuals to act as lead contact with the Executive Office. Make risk management a key part of the management process.
Officers	
Heads of Service and Managers	Have operational management for owning and identifying risks, implementing mitigating actions, and reporting appropriate information on key risks and control indicators to Directors.

	Identify training requirements for their service areas and actively promote risk management, ensuring that the guidance is followed. Recognise risk management and mitigating actions as integral parts of the service planning and performance management process, and crucial to the achievement of outcomes.
Executive Office	Responsible for the effective integration and delivery of risk management arrangements into the way the Council works in order to support performance improvement. Maintain the corporate and strategic risk registers. Provide expertise, guidance and support for officers to help ensure that risks are effectively managed, in line with the 'second line of defence'. Review and challenge services on their risks as a critical friend. Produce reports on current risk scores and mitigations for CLT, Cabinet, Overview and Scrutiny Management Committee and Performance Outcome Boards. Support and inform CLT, Cabinet, and oversight committees to ensure risk processes are appropriate and followed. Promote a risk aware culture and an awareness of the Council's risk policy and appetite.
All Staff	Identified in Protocol 9 (Principle 6) of Wiltshire Council's constitution - the Local Code of Corporate Governance - as responsible for managing risks as an integral part of all activities, for considering risk management in all aspects of decision making, and for ensuring that responsibilities for managing individual risks are clearly allocated. Understand the nature of risk and support managers in the identification, assessment and reporting of risk associated with their area of activity. Report emerging risks to line managers.
Other roles	
Internal Audit	Provides independent review on the effectiveness of the risk management policy and processes to ensure that the Council has an effective risk management process in place, in line with the 'third line of defence'. Identified in Protocol 9 of Wiltshire Council's constitution, through the Local Code of Corporate Governance, as responsible for ensuring additional assurance on the overall adequacy and effectiveness of the framework of governance, risk management and control.
Council Boards	Oversee and scrutinise any risks relevant to the remit and outcomes of the Board.

External assurance bodies	Provide the expertise needed to gain assurance that risk processes are being complied with and that mitigating controls are being implemented on a day-to-day basis.

20. These responsibilities align with the three lines of defence approach recommended by CIPFA and set out in Protocol 9 of the Council's Constitution, summarised in the diagram below:

21.



Strategic Risk Working Group

22. The risk working group takes the strategic lead on the Council's risk management processes, ensuring that they operate effectively and meet national standards of best practice.

23. It oversees the Council's strategic risks, and identifies emerging strategic risks and issues.

24. It ensures regular reviews of the Risk Management Policy are undertaken, in line with the 'second line of defence', and that updates proceed through review and approval

processes, including reviews by the Audit and Governance Committee and final approval by Cabinet.

25. The working group is chaired by the Director of Legal and Governance, with membership drawn from across the Directorates and Terms of Reference reviewed annually and approved by CLT.

Risk Registers

26. Risk registers are tools used to capture and manage information about risks throughout the risk management cycle. The information held in a risk register is then used for reporting on risks.

27. Registers of corporate and strategic risks should be maintained centrally, whilst service, programme, and project level risk registers can be maintained locally.

28. Risk registers must be able to capture all of the information described in this policy, including, but not limited to: risk identification codes; a risk description; risk owner; risk categories and appetites; risk scores for original, current and target risks; mitigating actions and progress made against them; and review details.

29. Although risk registers are living documents, an audit record of changes to corporate and strategic risk registers should be maintained for 7 years, in line with the Council's Disposal Schedule.

Tiers of Risk

30. The Council manages its risk across several different tiers, based on the significance of the risk to the Council's strategic and statutory ambitions, the level of risk that can be managed at a particular level, and where responsibility for the risk sits.

31. Each risk tier is typically managed using a separate risk register.

32. Risk tiers used by the Council are:

Tier	Description
Strategic risks	Strategic risks are significant and/or long-term risks that would impact the wider council, are the responsibility of the wider council to mitigate, or would significantly impact the Council's ability to achieve its stated aims. They typically arise from fundamental business decisions that senior management takes concerning the Council's strategic objectives.
Corporate risks	Corporate risks are risks associated with decision making, internal processes, business systems or activities. They are substantial risks that can no longer be managed at a service or project level, or that would impact a whole directorate or service.
Service risks	Service risks are specific to the operations of a service. They are risks that service levels are degraded, faulty or fail to perform, exposing the Council to complaints, liability claims, litigation, loss of revenues, or reputational damage. Responsibility for these risks may

	rest with Heads of Service rather than Directors or Corporate Directors.
Project / programme risks	Project or programme risks are an uncertainty of outcome through either positive opportunities or negative threats, that may impact one or more project objectives, or the outcome of a project.
National risks	National risks focus on large external events and perils. They are typically set and scored at the national level by central government and cascaded to local authorities via Local Resilience Forums. Within the Council mitigating actions for national risks are managed primarily through business continuity plans.

33. Where one or more corporate risks are related to a strategic risk, there should be a parent-child relationship between the strategic and corporate risks respectively. Scoring of the parent strategic risk should take into account scores of the related child corporate risks.

34. The anticipated numbers of risks in each tier and their hierarchy are shown in the diagram below:

Risk identification, definition and ownership

35. Risks always exist. A failure to identify a risk means it is automatically accepted. Identifying a risk means it can be managed.

36. New risks can be added to risk registers at any time when they are identified through a number of routes, including but not limited to:

- Service planning
- New policies, legislation or statutory requirements
- Changes to or reviews of existing services

- Cabinet reports
- Analysis of previous losses, events, incidents and lessons learnt
- National reports and technical briefings
- Internal audits
- Horizon scanning

37. New risks should be defined using a three-stage process that enable all risks to be described in a single sentence:

    - "Because of [the cause], [the event] may occur, which would lead to [the effect]"

Risk definition	Description
Cause	Why something could go wrong. It is this information that is used to consider what needs to be done to prevent a risk becoming an issue. The cause contributes to scoring the likelihood of the risk occurring. Causes are typically described as 'inability to', 'failure to', 'lack of', 'inadequate', 'inappropriate', or 'opportunity to'.
Event	This is what could go wrong. This is where the uncertainty lies. A cause doesn't automatically lead to the event, but it makes the event possible. The event also contributes to scoring the likelihood of the risk occurring.
Effect	This is the potential outcome of the event. It is the impact on the service, the Council, or our residents. The effect is used to score the impact of the risk.

38. In addition to the detailed risk definition, all risks should be given a short name to aid review and reporting.

39. All risk must be owned, usually by a Director or Head of Service. Risks should be owned by a role, rather than a named officer. However, the names of risk owners and contributing officers should be stored alongside the risk, as those currently responsible for reviewing information held about the risk on the risk register.

40. All risks should be assigned a risk identification code. Risk IDs must be unique and permanent for the risk, moving with the risk between tiers of risk registers, and between emerging risk and issue logs, to enable long-term tracking and audit.

41. Once defined, the addition of new risks to the relevant risk registers requires approval:

    - Strategic risks should be approved by both the Strategic Risk Working Group and CLT.
    - New corporate risks should be approved by the relevant Director and their creation reported to the relevant Performance Outcome Board.
    - New service-level risks should be approved by the relevant Director or Head of Service and their creation reported to the relevant Performance Outcome Group.

- New portfolio, programme or project risks should be approved in line with the agreed governance structures.

Emerging risks

42. Emerging risks arise where there are high levels of uncertainty about the likelihood and/or impact of an event arising from changes in the organisational or external environment that has not previously been properly assessed.

43. It may not yet be possible to fully understand the onset, likelihood or impact of emerging risks, preventing them to be accurately scored.

44. Unlike known risks, which can be managed, emerging risks can only be monitored to aid better understanding.

45. Emerging risks should still be added to the relevant risk register and assigned a risk ID, adding as much information as possible, even if incomplete. Waiting for complete information may delay monitoring of the risk and prevent timely implementation of mitigating actions once the risk is formalised.

46. Emerging risks should be escalated to full service, project, corporate or strategic risks once it is confirmed that the risk may impact the Council's strategic objectives or operational activities.

47. New emerging risks should be identified through similar processes to the identification of new risks.

48. A register of emerging corporate and strategic risks should be maintained and reported as per the process for reporting full risks described below.

Opportunities

49. Most risks are focused on reducing or avoiding threats. However, if only risks that disrupt or delay objectives or damage reputation are managed, then the Council is unlikely to identify opportunities to implement improvements in service provision.

50. Opportunity risk management is the proactive search for the positive upside of risks in order to find innovative solutions to the provision of services and improve on outcomes rather than just achieving them.

51. Opportunity risk management is best considered during the planning stages of any project, allowing new risks and opportunities to be identified and a decision taken on whether to take the opportunity.

52. Identification and capture of opportunities improves the chances of success, producing benefits for the Council that might otherwise have been over overlooked.

53. Opportunity risk management encourages people to think creatively about 'what if' questions to identify better, simpler, faster, or more effective ways of working, whilst removing the negative perception of risk management as scaremongering and intrinsically discouraging risk taking.

54. Opportunities arising from risk identification should be captured on risk registers with a risk response of 'take opportunity'.

Risk scoring

55. All risks are assessed to determine how much attention is given to managing a risk. This is achieved by scoring a risk based on the likelihood of the event occurring and the impact if the event were to occur.

56. The Council uses a 5-point scale, and the product of the likelihood and impact gives the risk score.

57. Scoring is done by suitably qualified and experienced officers, using the guidance and reaching a consensus to help avoid bias in scoring.

Original, current, and target scores

58. All risks are scored three times:

- **Original score**: The untreated risk score if no mitigating actions were to be implemented. This may also be described as the inherent risk. For treated risks, the original score should be hypothetical as mitigating actions should be in place.
- **Target score:** This is the score aimed for if all mitigating actions were to be successfully implemented. It is the risk score to be aimed for by a specific date.
- **Current score**: The risk score with existing controls in place. It is the risk score as it is now with the mitigating actions in their current state of implementation, which may not be complete. This may also be described as the residual risk.

Risk likelihood scoring criteria

59. Wiltshire Council uses a 5-point scale to assess the likelihood of a risk occurring:

Likelihood Score	Probability	Indicator
1 Very unlikely	Less than 20%	• **Very unlikely** to occur. • Has **not** happened within the last **5 years** or more. • Is **unlikely** to happen within the next **5 years** or more. • No similar instances in recent local government history except in exceptional circumstances.
2 Unlikely	Between 21% and 40%	• **Not expected** to occur. • Has **not** happened within the last **3 years**. • Is **unlikely** to happen within the next **3 years**.

		• There is rare but not unheard of occurrence in local government history.
3 Possible	Between 41% and 60%	• **Might** occur. • **Has** happened in the last **2 years**. • Is **likely** to happen within the next **2 years**. • Is **expected** to happen or be more severe in the future **if action is not taken** in the next 2 years. • There is a history of occasional similar occurrences in local government.
4 Likely	Between 61% and 80%	• **Strong possibility** of occurring. • Has **happened** in the **last year**. • Is **expected** to happen in the **next year**. • Is **expected** to happen or be more severe in the future **if action is not taken** in the next year. • There is a history of regular similar occurrences in local government.
5 Very likely	More than 80%	• **Very likely** to occur. • Has **happened** in the past **6 months**. • Is **expected** to happen in the next **6 months**. • Is **expected** to happen or be more severe in the future in **if action is not taken** in the next 6 months. • There is a history of frequent similar occurrences in local government.

Risk impact scoring criteria

60. Wiltshire Council uses a 5-point scale to assess the consequences should the risk event happen.

61. Brief indicators for each impact score are given in the table below. More detailed examples of the impact at each level for each category of risk is provide in the risk impact scoring matrix in Appendix 2.

Impact Score	Selected Example Indicators
1 Negligible	• Brief service disruption for less than a day affecting a project or team. • Incident occurred but no time lost. • Legal action against the Council unlikely. • Possible financial impact manageable within service budget. • Limited systems downtime with some services unavailable for a few hours.
2	• Loss of service for 1-2 days affecting one or more services.

Moderate	• Slight injury to one or more people but no time lost. • Legal action against the Council possible. • Financial impact managing within existing Service budget. • Brief downtime of non-critical systems for 1-2 days.
3 Substantial	• Loss of service for 2-3 days affecting a single directorate. • Temporary injury to one or more people requiring limited time off work. • Legal action against the Council likely. • Financial impact manageable within existing Directorate budget. • Downtime of core systems for 2-3 days.
4 Critical	• Loss of service for 3-5 days affecting most directorates. • Severe injury to one or more people requiring sustained time off work over 3 months. • Legal action against the Council expected. • Financial impact manageable within existing Council budget. • System failure with critical systems unavailable for 3-5 days.
5 Catastrophic	• Loss of service for more than 5 days affecting the whole council. • Death or life-changing injuries to one or more people. • Legal action against the Council underway or almost certain. • Financial impact not manageable within existing funds. • Significant system failures with critical services unavailable for more than 5 days.

Risk score levels

62. Risk scores for each risk are calculated by multiplying the likelihood score and impact score.

63. Risk scores are divided into five levels. These are used to determine the RAG rating when reporting risks:

Risk level	Score	RAG rating	Description
Very low risk	Scores 1-2	White	• The Council is content to carry these risks. • Risks are more likely to be tolerated rather than treated as the costs of maintaining controls may outweigh the benefits. • No action is required but risks should be regularly monitored.
Low risk	Scores 3 - 6	Blue	• The Council is uneasy about carrying these risks.

			• Immediate action may not be required, but any controls should be maintained and regularly reviewed to maintain the rating.
Medium risk	Score 6 - 12	Grey	• The Council is concerned about carrying these risks. • Manageable risks but action is required to reduce the rating within a specific timescale. • Mitigating actions to reduce the rating should be mindful of the costs vs. benefits of implementing them, and should be reviewed on a regular basis.
High risk	Score 15 - 16	Red	• The Council is very concerned about carrying these risks. • Significant risks that require urgent action to reduce the likelihood and/or impact through mitigating controls. • Controls should be monitored frequently to ensure they remain effective at reducing the risk.
Very high risk	Scores 20 - 25	Black	• The Council wants to actively prevent carrying these risks. • The activity should stop and immediate action should be taken to reduce the risk. • Ongoing reporting is required to ensure that controls remain effective at reducing the risk.

Risk ranking matrix

64. The Council's agreed criteria for scoring likelihood and impact gives rise to an overall risk scoring matrix that can be assigned to the five levels of risk:

Impact	**5 Catastrophic**	**5**	**10**	**15**	**20**	**25**
	4 Critical	**4**	**8**	**12**	**16**	**20**
	3 Substantial	**3**	**6**	**9**	**12**	**15**
	2 Moderate	**2**	**4**	**6**	**8**	**10**
	1 Negligible	**1**	**2**	**3**	**4**	**5**
Wiltshire Council Risk Matrix		**1 Very Unlikely**	**2 Unlikely**	**3 Possible**	**4 Likely**	**5 Very Likely**
		Likelihood of Occurrence				

Risk Categories

65. Risk categories broadly group risks into similar types and can be used to better understand the Council's risk profile. They can be used to identify potential new risks and to determine the level of risk appetite that the Council is willing to tolerate in achieving its ambitions.

66. All risks should be assigned a primary risk category. Many risks fall into more than one risk category, and so a secondary risk category should also be set.

67. Risk categories can be defined as:

Risk Category	Example situations in which the risk may arise
Procurement and Commissioning	Weaknesses in the management of commercial partnerships, supply chains and contractual requirements, resulting in poor performance, inefficiency, poor value for money, fraud, or failure to meet business requirements or objectives.
Environment	A failure to consider climate and environmental impacts, resulting in a loss of biodiversity, pollution and/or climate change and the increasing vulnerability of residents and Council services to climate impacts.
Financial	Not managing finances in accordance with requirements and financial constraints resulting in poor returns from investments; failure to manage assets or liabilities; failure to obtain value for money from the resources deployed; or non-complaint financial reporting.

Risk Category	Example situations in which the risk may arise
Governance	Unclear plans, priorities, authorities, and accountabilities; or ineffective or disproportionate oversight of decision making or performance.
Health and Safety	Failure in processes, policies, environment, or equipment that create unsafe working conditions causing a person to suffer harm.
Information	A failure to produce robust, suitable and appropriate data or information and to exploit this to its full potential.
Legal	Failure to take appropriate measures to meet legal or regulatory requirements or to protect assets; a legal event occurring that results in a liability or other loss; a defective transaction, claim being made, or defence to a claim or counterclaim.
Operations / Service Delivery	Inadequate, poorly designed, or ineffective/inefficient internal processes resulting in error, impaired customer service, non-compliance, or poor value for money.
Reputational	Adverse events, including ethical violations, a lack of sustainability, systemic or repeated failures, poor quality, or a lack of innovation, leading to damages to reputation and/or destruction of trust and relations.
Security	A failure to prevent unauthorised or inappropriate access to key systems and assets, including people, platforms, information, and resources. This encompasses the subset of cyber security.
Staffing/People	Ineffective leadership and engagement; suboptimal culture; inappropriate behaviours; the unavailability of sufficient capacity and capability; industrial action; non-compliance with relevant employment legislation; or policies resulting in a negative impact on performance.
Technology	Technology not delivering the expected services, benefits or quality due to inadequate or deficient system/process development and performance, or inadequate resilience.

Risk appetite

68. Risk appetite is defined as the amount and type of risk that an organisation is willing to pursue or retain in order to achieve its priorities[1].

69. It helps to define the level of exposure that can be justified and tolerated when balancing the benefits of taking the risk with the cost of mitigation.

70. Levels of risk appetites can be defined as:

[1] ISO 31000, Guide 73 definition.

Risk Appetite Level	Overall risk Score	Description
Averse	1-2	Avoidance of risk and uncertainty in any objective.
Minimalist	3-6	Preference for safe options that have a low degree of original/uncontrolled/inherent risk.
Cautious	8-9	Preference for safe options that have a low degree of current/treated/residual risk.
Receptive	10-12	Willing to consider all options and choose one that is most likely to result in successful delivery.
Eager	15 or higher	Eagar to be innovative and to choose options that based on maximising opportunities and accept greater uncertainty, even if those activities carry a very high residual risk.

71. All risks will be assigned a risk appetite score, based on the lowest, more risk averse appetite from the primary and secondary risk categories the risk is classified as.

72. Risk appetites are set for each of the categories of risk using the risk scoring appetite matrix in Appendix 3.

73. Risk appetites will be reviewed annually by the Audit & Governance Committee, and approved by Cabinet, following recommendations from the Risk Working Group and CLT.

74. Risk appetites for each of the risk categories used by the Council are:

Risk Category	Risk appetite	Risk appetite score	Risk appetite description for the category (from Appendix 3)
Procurement and Commissioning	Receptive	12	Innovation supported with demonstration of benefit/improvement in service delivery. Responsibility for non-critical decisions may be devolved.
Environment	Cautious	8	Seeks to balance carbon reductions and environmental protections with minimising residual financial loss. Trade-off between climate outcomes and performance returns.
Financial	Receptive	12	Prepared to invest for benefit and to minimise the possibility of financial loss by managing the risks to tolerable levels.
Governance	Cautious	9	Willing to consider actions where benefits outweigh risks. Processes, and oversight / monitoring arrangements enable cautious risk taking. Controls enable fraud prevention, detection and deterrence by maintaining appropriate controls and sanctions.

Health and Safety	Minimalist	6	Legislation adhered to. Training in place. Regular reviews of risk assessments and processes for all activities involving higher degree of equipment usage.
Information	Cautious	9	Accepted need for operational effectiveness. Careful management of information and data through access controls and some monitoring for most information and data.
Legal	Cautious	9	Would want to be reasonably sure we would win any challenge.
Operations – Minimalist	Minimalist	6	Innovations largely avoided unless essential. Decision making authority held by senior management.
Operations – Cautious	Cautious	9	Tendency to stick with the status quo. Innovations generally avoided unless necessary. Decision making authority generally held by senior management. Management through leading indicators.
Operations - Open	Receptive	12	Innovation supported with clear demonstration of benefit or improvement in management control. Responsibility for non-critical decisions may be devolved.
Reputational	Eager	15	Appetite to take decisions that are likely to bring additional Council scrutiny only where potential benefits outweigh the risks.
Security	Cautious	8	**Limited** security risks accepted to support business need, with appropriate checks and balances in place: • Vetting levels may flex with teams as required. • Controls **managing** staff access and **limiting** visitor access to information, assets and estate. • Staff personal devices may be used for limited official tasks with appropriate permissions.
Staffing/ People	Cautious	9	Seek safe and standard people policy. Decision making authority generally held by senior management.
Technology	Receptive	12	Systems or technology developments are considered to enable improved delivery. Agile principles may be followed.

Risk responses

75. After a risk has been identified and the original, untreated level of risk has been scored, consideration should be given about how to treat the risk.

76. The Council has five possible responses that determine what type of action should be taken:

Risk response	Description
Treat	Taking mitigating action to reduce or minimise the likelihood of an event occurring and/or to minimise its impact should it occur. This will require defined actions to be allocated to individuals, target implementation dates agreed and progress to be monitored.
Transfer	Transfer the risk to another party either by insurance or through a contractual arrangement. Responsibility for statutory functions cannot be fully transferred. The reputational implications of risks need to be managed since these cannot be transferred.
Tolerate	Make an informed decision that the risk is acceptable and make proper financial arrangements should it occur. This may occur where it is more appropriate to tolerate the risk than to spend resources attempting to further mitigate it. Current 'ongoing' controls or mitigating actions will need to be monitored.
Terminate	Where feasible, stop doing whatever it is that causes the risk and use alternative products or change processes.
Take opportunity	Consider other gains that may be made by applying the risk controls envisaged. These may have a positive impact beyond the activity being assessed.

Mitigating Actions

77. Mitigating actions should directly reduce the likelihood of the risk occurring or the impact if the risk were to occur.

78. Mitigating actions might include, but are not limited to:

- Implementation of policies or procedures.
- Use or development of systems.
- Insurance against financial impacts.
- Contracts to transfer risks to third parties. Note that responsibility for statutory functions cannot be fully transferred.
- Training and guidance procedures.
- Business continuity planning.
- Other control measures.

79. Mitigating actions can be either business-as-usual activities, transformation projects, or discrete service-level projects identified as part of the annual service planning process.

80. All mitigating actions should be recorded on the risk register and their effectiveness reviewed quarterly to ensure that they remain relevant, are being implemented or complied with, and are effectively reducing the current risk score. Progress with implementing mitigations should be captured and updated quarterly.

81. Mitigations where little progress is being made with implementation, or where the mitigations are having no impact on the current risk score, should be reported to Performance Outcome Boards and additional mitigations should be considered.

Issues

82. Issues are risks that have been realised, where there is no longer uncertainty about the likelihood of the risk occurring.

83. A register of corporate and strategic issues should be maintained and reported as per the process for reporting full risks described below.

84. Once a risk has been realised, mitigating actions should be reviewed and refocused on reducing the impact and ensuring that contingency plans and business continuity plans are implemented.

85. The issue should continue to be regularly monitored and reviewed so that, should circumstances change, the issue can be returned to a risk.

Risk reviews

86. Strategic and corporate risks should be reviewed by either the owner or contributing officer at least quarterly.

87. Reviews must ensure that named officers are still in relevant posts, update progress on the implementation and effectiveness of mitigating actions, and establish whether anything has changed that may affect current levels of risk.

88. Reviews should also consider whether the risk is still relevant, whether it has occurred and become an issue, or whether it should be closed.

89. Urgent attention should be paid to risks where:

- The current risk score exceeds its appetite;
- The current risk score is high or very high (a score of 15 or higher);
- The current risk score has increased since the previous review;
- Little progress has been made with implementing mitigating actions;
- Mitigating actions are not effectively reducing the current risk score.

90. For these risks, the review should determine whether additional mitigating actions are required to reduce the current risk score, and whether the risk should be escalated to a more senior officer for ownership or escalated to a higher risk register.

Risk Escalation and De-escalation

91. Risks should be escalated up the hierarchy of risk registers, from project/programme to service or from service to corporate, when any of the following criteria apply:

- The current risk score exceeds the appetite boundaries set for the risk.
- The current risk score remains high or very high, with a score of 15 or higher, even after control measures and mitigating actions have been fully implemented.
- The risk becomes unmanageable by responsible officers at the current level.
- The risk has operational impacts beyond the current project or service area.
- The risk has the potential to impact beyond the current project service area.

92. Risks should be de-escalated to a lower risk register when the criteria listed above no longer apply.

93. Escalation/de-escalation of a risk to the corporate risk register should be reviewed and agreed by the relevant Director or Head of Service, who will take responsibility for the decision.

94. Corporate risks that meet the escalation criteria above, or those that directly impact delivery of more than one mission in the Council's Business Plan, should be re-formulated into new strategic risks.

95. Where multiple similar corporate risks are identified across several service areas, a new parent strategic risk should be created so that the overall level of risk can be monitored and mitigated at the strategic level. The scoring of this strategic risk should be informed by the scores of the related child corporate risks.

96. Responsibility for approval of new strategic risks rests with the Strategic Risk Working Group and CLT.

Risk reporting

97. Risks do not remain static. Regular reporting on the Council's risks is essential for ensuring all stakeholders remain informed of changing conditions, current performance in managing risk, and plans for dealing with future risks. Reporting also ensures that serious risk are effectively managed and drawn to the prompt attention of the relevant level of management.

98. Risks are reported as they are at the time of the report, against their risk appetite, rather than at the end of any prior quarterly or annual reporting period, to ensure that the information reported is current and accurate, and recent updates to risk scores can be acted on.

99. All strategic risks should be reported to CLT, Cabinet, and the Overview and Scrutiny Management Committee on a quarterly basis as part of the Performance and Risk Report.

100. All current issues and emerging risks should be reported to CLT, Cabinet, and the Overview and Scrutiny Management Committee on a quarterly basis as part of the Performance and Risk Report.

101. Corporate risks should be reported to CLT, Cabinet, and the Overview and Scrutiny Management Committee on a quarterly basis by exception if:

- The current score exceeds the appetite level set for the risk.

- The current score, with existing mitigations in place, is high or very high (a score of 15 or higher)
- The current risk score has increased by a score of 5 or more since the previous review.

102. National risks and the Council's response to them will be reported to the Overview and Scrutiny Management Committee on an annual basis.

103. Performance Outcome Boards will receive 'deep dive' reports on relevant strategic and corporate risks on a quarterly basis.

104. Performance Outcome Boards will also receive quarterly exception reports for corporate risks using the same criteria as for Cabinet reporting, with additional exception reports for risks where little progress has been made in implementing mitigating action.

105. Note that although risks may be reported to Cabinet or Overview and Scrutiny Management Committee, elected members may not have direct responsibility for risks where they relate to separate statutory responsibilities held by officers, as set out in Article 12(4) of Part 2 of the Council's Constitution, such as the Returning Officer for elections.

106. The Audit and Governance Committee will receive an annual report on the effectiveness of the Council's risk management processes and any changes made over the previous 12 months.

Risk closure

107. Risks may be closed by the Risk Owner if they are assessed by and agreed by the service to no longer be relevant, such as if a time-limited event has passed or if the work has been completed or is no longer conducted.

108. Risks that have been successfully mitigated to reduce their risk scores must not be closed, but should remain on the relevant risk register for regular review, to ensure that the mitigating actions continue to be effective in reducing the likelihood or impact of the risk.

Acknowledgements

109. We thank colleagues at the City of London Corporation, Stafford Borough Council, and HMRC for sharing their risk management policies and strategies.

Appendix 1: Glossary

Appetite	The amount and type of risk that the Council is willing to pursue or retain in order to achieve its priorities.
Category	Groups of risks that are of a broadly similar type. Risk categories can be used to identify potential new risks and understand the overall risk profile. Risk categories are also used to determine the appropriate appetite level for the risk.
Cause	The cause is why something could go wrong. Used to consider what needs to be done to prevent a risk becoming an issue e.g. If [the cause] happens the risk will occur.
Child risk	One or more corporate risks that are related to a single parent strategic risk. Multiple services may have similar corporate risks that collectively influence the scoring of a single risk at the strategic level. For example, multiple services may have risks relating to staffing that are child risks of a single parent strategic risk on overall staffing across the Council.
Corporate risk	Risks associated with decision making, internal processes, business systems or activities. Corporate risks are substantial risks that can no longer be managed at a service or project level. Corporate risks typically impact a whole directorate or service.
Current risk score	The risk score with existing controls in place. The current risk score is the risk as it is now with the mitigating actions in their current state of implementation. Previously called the residual score.
De-escalation	The movement of risks down the hierarchy of risk registers based on criteria around decreasing risk scores, ability of risk owners to manage a risk, and a narrowing of how widely the risk applies across the Council.
Emerging risk	Where there may be high levels of uncertainty about a new event arising from changes in the organisation or external environment, that cannot yet be properly assessed.
Escalation	The movement of risks up the hierarchy of risk registers based on criteria around increasing risks scores, inability of risk owners to manage a risk, and a broadening of how widely the risk applies across the Council.
Event	The event is what could go wrong. This is where the uncertainty lies. A cause doesn't automatically lead to the event, but it makes the event possible. Use the cause and the event to score the likelihood of a risk occurring e.g. there is a risk that [event] will happen.
Effect	The effect is the potential outcome of the event. It is the impact on the service, the Council or our residents. The effect is used to score the impact of the risk e.g. the risk leads to the [effect] happening.

Impact	This scores what the impact would be if the risk did occur from 1 (negligible) to 5 (catastrophic).
Issue	Issues are risks that have been realised, where there is no longer uncertainty about the likelihood of the risk occurring.
Likelihood	The likelihood scores how likely the risk is to occur, from 1 (very unlikely) to 5 (very likely).
Mitigating action	A mitigating action is an activity aimed at reducing the likelihood of a risk occurring, or the impact if the risk were to occur. They can be business-as-usual activities or processes, discrete projects, or a transfer of the risk to a third party via a contract or insurance.
National risks	Risks that focus on large external events and perils. National risks are typically set and scored at the national level by central government, and cascaded to local authorities via Local Resilience Forums.
Opportunities	A risk where early identification of the uncertainty may present the opportunity to implement improvements in service provision.
Original risk score	The untreated risk score if no mitigating actions were to be implemented. Previously called the inherent score.
Owner	The person ultimately responsible for the risk, including ensuring that the appropriate response is implemented, where appropriate, to reduce the risk score.
Parent risk	A single strategic risk that is related to one or more child risks on the corporate risk register. Scoring of the parent strategic risk should take into account risk scores of all related child risks. For example, a parent strategic risk on staffing should consider the scores of any related staffing risks across multiple services.
Risk	The effect of uncertainty on objectives, which may be either threats or opportunities.
Risk ID	A unique identifier permanently assigned to a risk, allowing it to be tracked across different risk registers over time.
Risk level	The division of risk scores across five levels ranging from very low to very high. Risk levels can be used to produce colour-coded heatmaps for risk reporting.
Risk long name	A meaningful name used to identify the risk on reports and the Strategic Risk Summary for Cabinet.
Risk management	The planned and systematic approach to identifying and addressing uncertainty, with the goal of anticipating events, adapting to change, increasing the probability of success and reducing the probability of failure in achieving objectives, by minimising threats and maximising opportunities that arise.
Risk management cycle	An ongoing process that starts with the identification and definition of risks, followed by analysis and evaluation of the potential likelihood and impact of the risk. An appropriate response is then selected,

	which may include implementation of mitigating actions to reduce the risk score. The risk is regularly reviewed and monitored, including horizon scanning to identify new or emerging risks.
Risk register	A tool used to capture and manage information about risks throughout the risk management cycle. The information held in the risk register can be used for reporting on risks.
Risk scores	The risk score is calculated by multiplying the likelihood by the impact. Scores of 15 or above are high and very high risks. Scores of 6 or below are low or very low risks.
Risk short name	Used to identify a risk when completing the risk register or discussing risks with colleagues.
Service risk	Risks that are specific to the operations of a service, resulting in service levels being degraded, faulty, or failing to perform. Responsibility for these risks may rest with Heads of Service rather than Directors or Corporate Directors.
Strategic risk	Significant, long-term risks that would impact the wider council, are the responsibility of the wider council to mitigate, or would significantly impact the Council's ability to achieve its stated aims. Strategic risks typically arise from fundamental business decisions that senior management take concerning the Council's strategic objectives.
Target risk score	The target score aimed for if all mitigating actions are successfully implemented. It is the risk score aimed for by a specific date.
Tiers of risk	The level at which the risk applies, which might be Council-wide, within a Directorate, within a Service, or specific to a project or transformation programme. The tier determines which risk register the risk is recorded on (strategic, corporate, service, or project).

Appendix 2: Risk impact scoring matrix

110. The following matrix can be used to determine the appropriate impact score for different categories of risk.

	1 Negligible	2 Moderate	3 Substantial	4 Critical	5 Catastrophic
Procurement and Commissioning	All contracts represent excellent value for money and are below the allocated budget with all services included. Robust supply chains with certainty of supply procured under the allocated budget. Full return on investment in less than the proposed times scales.	Contracts represent good value for money and are on budget with all services included. Reliable supply chains procured within the allocated budget. Full return on investment in the proposed timescales.	Contracts represent good value for money but require compromises on non-key services included to remain within budget. Consistent supply chains but requiring additional budget to procure. Short extension required to proposed timescales in order to achieve full return on investment.	Contracts represent limited value for money remaining within budget but with key services not included. Unreliable supply chains. Full return on investment unlikely within extended timescales.	Contracts do not represent value for money with costs exceeding allocated budget or key services not included. Frequent disruption to supply chains. Return on investment remains unpaid despite extended timescales.
Environment	The risk or incident has a negligible negative impact on climate and	The risk or incident has a moderate negative impact on climate and	The risk or incident has a substantial negative impact on climate and the environment in the short or long term;	The risk or incident has a critical negative impact on climate and the environment in the short or long term;	The risk or incident has a catastrophic negative impact on climate and the environment in the

	1 Negligible	2 Moderate	3 Substantial	4 Critical	5 Catastrophic
	the environment in the short or long term. There is negligible impact on the vulnerability of local habitats, wildlife, agriculture, businesses, infrastructure or the delivery of critical Council services to climate change, environmental impacts or incidents.	the environment in the short or long term. There is moderate impact on the vulnerability of local habitats, wildlife, agriculture, businesses, infrastructure or the delivery of critical Council services to climate change, environmental impacts or incidents.	and can cause short term persistent contamination to the local area and may cause some short-term health impacts. There is substantial impact on the vulnerability of local habitats, wildlife, agriculture, businesses, infrastructure or the delivery of critical Council services to climate change, environmental impacts or incidents.	and can cause persistent medium-term contamination to the local area and may cause some loss of life or significant health impacts. There is critical impact on the vulnerability of local habitats, wildlife, agriculture, businesses, infrastructure or the delivery of critical Council services to climate change, environmental impacts or incidents.	short or long term; and can cause long terms or irreparable contamination to the local area and may cause widespread loss of life. There is catastrophic impact on the vulnerability of local habitats, wildlife, agriculture, businesses, infrastructure or the delivery of critical Council services to climate change, environmental impacts or incidents.
Financial	Possible financial impact manageable within service budget. Unbudgeted financial loss or unplanned increase on service budget up to £50,000	Financial impact manageable within existing service budget. Unbudgeted financial loss or unplanned increase on service budget up to £250,000	Financial impact manageable within existing Directorate budget. Unbudgeted financial loss or unplanned increase on service budget up to £500,000	Financial impact manageable within existing Council budget. Unbudgeted financial loss or unplanned increase on service budget up to	Financial impact not manageable within existing funds. Unbudgeted financial loss or unplanned increase on service budget over

	1 Negligible	2 Moderate	3 Substantial	4 Critical	5 Catastrophic
	or >1% (<10%) of monthly budget. Robust long-term treasury management with utilities and debts fixed at low rates, and investments fixed at high rates.	or >2% (<50%) of monthly budget. Treasury management secures beneficial rates for utilities, debt and investments over the medium term.	or >5% (<75%) of monthly budget. Treasury management reliant on variable rates, resulting in substantial exposure to changes in interest rates.	£1,000,000 or >10% (>75%) of monthly budget. Treasury management reliant on variable rates, resulting in critical exposure to non-beneficial changes in interest rates.	£1,000,000 or >15% of monthly budget. Significant failures in treasury management, with utilities and debt locked into long-term fixes at high rates, and/or investments fixed at low rates, with catastrophic financial impacts on procurement and investments.
Governance	No incidents of fraud against or within the Council. No decisions taken outside of processes and oversight / monitoring arrangements. All plans and priorities clearly defined with effective decision making and robust accountability.	Potential for fraud against or within the Council. Decisions rarely taken outside of processes and oversight / monitoring arrangements. Most plans and priorities well-defined with effective decision making and clear accountability.	Occasional incidents of fraud against or within the Council. Decisions occasionally taken outside of processes and oversight / monitoring arrangements. Defined plans and priorities with consistent decision making and some accountability.	Regular incidents of fraud against or within the Council. Decisions often taken outside of processes and oversight / monitoring arrangements. Vague plans and priorities with inconsistent decision making and unclear accountability.	Frequent incidents of fraud against or within the Council. Decisions frequently taken outside of processes and oversight / monitoring arrangements, resulting in ineffective decision making. Unclear plans and priorities with ineffective decision

	1 Negligible	2 Moderate	3 Substantial	4 Critical	5 Catastrophic
					making and no accountability.
Health and Safety	Incident occurred but no time lost. Outcomes not notifiable to an enforcement agency. Fully compliant with all employer/landlord responsibilities and robust maintenance contracts, ensuring the safety of all Council tenants.	Slight injury, harm or discomfort to one or more people. No time lost. Outcomes not notifiable to an enforcement agency. Gaps in compliance with some employer/landlord responsibilities and adequate maintenance contracts, but with no resulting safety breaches for Council tenants.	Injury or harm to one or more people of a temporary nature but does not require sustained on-going treatment. Limited time off work required. Outcomes notifiable to the relevant enforcement agency. Substantial gaps in compliance with employer/landlord responsibilities and/or inadequate maintenance contracts, with potential safety implications for Council tenants.	Severe injury or harm to an individual or several people. Sustained time off work above 3 months. Outcomes likely to attract the attention of the relevant enforcement agency. Substantial gaps in compliance with most employer/landlord responsibilities and failings in maintenance contracts, resulting in harm to one or a few Council tenants.	Death of one or more people. Significant life changing / threatening injuries to one or more people. Outcomes certain to require action by the relevant enforcement agency. No compliance with employer/landlord responsibilities and substantial failings in maintenance contracts, resulting in significant harm to Council tenants.

	1 Negligible	2 Moderate	3 Substantial	4 Critical	5 Catastrophic
Information	No data breaches. Data fully exploited for all decision making. Robust data retention policies and strong implementation results in low storage costs for retention of only essential data.	Data breach of non-confidential or non-personal data. Data exploited for most decision making. Data retention policies are implemented for most types of data, reducing data storage costs.	Data breach of confidential or personal data but where individuals do not need to be informed and with no action taken by the ICO. Data used to inform critical decision making only. Data retention policies are not routinely implemented, resulting in poor data management and retention of large amounts of non-essential data.	Data breach of highly confidential data or personal data, where individuals need to be informed and/or resulting in a fine from the ICO at the standard penalty level. Data only occasionally used to inform critical decision making. Data retention policies only cover statutory requirements and committees, resulting in uncontrolled retention of other types of data and high storage costs.	Significant breach of highly sensitive, special category, or personal data resulting in an ICO fine at the higher penalty level. Data not used to inform decision making. Uncontrolled data retention resulting in high storage costs.
Legal	Legal action against the Council unlikely. Localised service-level deviation from duties.	Legal action against the Council possible. Minor breach of duty resulting in disciplinary action.	Legal action against the Council likely. Moderate breach of duty resulting in disciplinary action.	Legal action against the Council expected. Significant breach of duty resulting in fines and/or disciplinary	Legal action underway or almost certain and difficult to defend. Catastrophic breach of duty resulting in fines and imprisonment.

	1 Negligible	2 Moderate	3 Substantial	4 Critical	5 Catastrophic
	Potential claim than up to £50,000 or potential costs up to £25,000. Properties with a capital value of up to £150,000.	Potential claim greater than £50,000 or potential costs greater than £25,000. Properties with a capital value of more than £150,000.	Potential claim greater than £150,000 or potential costs greater than £50,000. Properties with a capital value of more than £450,000.	action leading to gross misconduct. Potential claim greater than £300,000 or potential costs greater than £100,000. Properties with a capital value of more than £800,000 or contracts that have a significant impact on council services.	Potential claim greater than £500,000 or potential costs greater than £150,000. Properties with a capital value of more than £1,000,000 or contracts that have a critical impact on council services. Matters where there is significant political interest or involving issues concerning the reputation of the Council.
Operations / Service Delivery	Brief disruption of less than 1 day. Affects a project or team. Possible impacts to non-vulnerable groups.	Loss of service for 1-2 days. Affects one or a few services. Impacts to non-vulnerable groups.	Loss of service for 2-3 days. Affects a single Directorate. Definite impacts to non-vulnerable groups.	Loss of service for 3-5 days. Affects most Directorates. Impacts to small numbers of vulnerable people. Definite impacts to non-vulnerable groups.	Loss of service for more than 5 days. Affects the whole Council. Impacts vulnerable groups. Impacts upon property accessed by the public and officers.

	1 Negligible	2 Moderate	3 Substantial	4 Critical	5 Catastrophic
			Possible impacts upon property accessed by the public and officers.	Impacts upon property accessed by the public and officers.	
Reputational	Matter contained within section/ service. Minor adverse local publicity.	Negative local publicity. Negative local public opinion generating complaints.	Sustained negative local publicity. Negative publicity in municipal press affecting standing in professional local government community. High proportion of negative customer complaints.	Negative national publicity. Low public confidence in members and officers in ability to deliver services.	Sustained negative national publicity. Resignation or removal of Corporate Director or elected member. Breakdown of multiple partnership working
Security	All Council buildings, systems, information, and assets secured with access restrictions in place.	Failings or gaps in access restrictions to Council buildings, systems, information, or assets, but not resulting in intrusions, damage, loss or data breaches.	Unauthorised staff access to Council buildings, systems, information, or assets due to breaches of internal access restrictions, resulting in limited intrusions, minor damage, or loss of non-sensitive data.	Unauthorised public access permitted to buildings, systems, information, or assets resulting in intrusions, loss or minor damage to Council buildings or assets, or external data breaches.	Unauthorised access to the public to buildings, systems, information, or assets resulting in substantial loss or damage to Council buildings or assets, danger to the safety of people, or loss of critical

	1 Negligible	2 Moderate	3 Substantial	4 Critical	5 Catastrophic
					information and/or personal data.
Staffing/People	Some short-term vacancies in non-critical services with no impact on service delivery. Staff have the required skills and experience to perform their full duties.	Several short-term vacancies in non-critical services with minor impact on service delivery. Staff have most skills and experience required to ensure delivery of services.	Several long-term vacancies impacting on delivery of non-critical services. Staff lack relevant skills, resulting in an underperforming workforce.	Unable to fill key staff vacancies in critical services leading to inability to deliver critical services. Staff lack core skills and experience, leading to gaps in service provision.	Long-term inability to fill staff vacancies resulting in leading to an inability to deliver critical services with impacts on vulnerable people and/or public health implications. Lack of critical skills and experience, impacting on the workforce's ability to fulfil statutory duties.
Technology	Limited systems downtime with some services unavailable for a few hours. Workarounds possible and no operational impact. All systems can be restored from backup with no loss of data.	Brief downtime of non-critical systems for 1-2 days. Limited operational impact on non-critical services. All critical systems can be fully restored from backup, with minimal	Downtime of core systems for 2-3 days. Some operational impact on critical services. Critical data can mostly be restored from backup but with some loss of system data.	System failure with critical systems unavailable for 3-5 days. Substantial operational downtime impacting most services. Systems can only be partially restored from	Significant system failures with critical services unavailable for more than 5 days. Widespread operational downtime impacting all services. Systems can't be restored from backup resulting in permanent

	1 Negligible	2 Moderate	3 Substantial	4 Critical	5 Catastrophic
	All systems fully deliver required functionality.	loss of non-critical system data. Systems mostly deliver required functionality.	Only critical Systems deliver required functionality.	backup, resulting in partial loss of system data or loss of data integrity. Critical systems do not deliver required functionality.	loss of critical system data. Most systems do not deliver required functionality.

Appendix 3: Risk appetite matrix

111. The following matrix can be used to determine the appropriate appetite level for different categories of risk. It is based on risk appetite guidance provided by HM Treasury, including the UK Government's 'Orange Book' series.

112. Yellow highlighted boxes indicated where the Council's risk appetite for a given category currently sits.

Risk category	Risk appetite level and associated risk score				
	Averse	**Minimalist**	**Cautious**	**Receptive**	**Eager**
	Very low risk score acceptable 1-2	**Low risk score acceptable 3-6**	**Lower medium risk score acceptable 8-9**	**Higher medium risk score acceptable 10-12**	**High or very high risk score acceptable 15 or higher**
Procurement and Commissioning	Zero appetite for untested commercial agreements. Priority for close management controls and oversight with limited devolved authority.	Appetite for risk taking limited to low scale procurement activity. Decision making authority held by senior management.	Tendency to stick to the status quo. Innovations generally avoided unless necessary. Decision making authority generally held by senior management through leading indicators.	Innovation supported with demonstration of benefit/improvement in service delivery. Responsibility for non-critical decisions may be devolved.	Innovation pursued. Desire to 'break the mould' and challenge current working practices. High levels of devolved authority. Management by trust or lagging indicators rather than close control
Environmental	Zero appetite for not meeting net zero and environment aims. Decarbonising and environmental policies are main priorities.	Prepared to accept minimal climate or environmental impacts if essential to the delivery of other critical services. Preference to take	Seeks to transparently demonstrate a course of action is justified, based on a balanced consideration of carbon reductions and environmental	Willing to risk not meeting net zero and environment targets and the implications for climate change in order to achieve other objectives.	Willing to take the risk of uncontrolled climate change and environmental damage. Willing to risk increased carbon emissions in pursuit of

Risk category	Risk appetite level and associated risk score				
	Averse	**Minimalist**	**Cautious**	**Receptive**	**Eager**
	Very low risk score acceptable 1-2	**Low risk score acceptable 3-6**	**Lower medium risk score acceptable 8-9**	**Higher medium risk score acceptable 10-12**	**High or very high risk score acceptable 15 or higher**
	Avoiding making the causes and impacts of climate change worse, and taking actions to improve our climate and environmental impacts are key objectives.	mitigating actions on environmental impacts of Council operations, which may result in reduced performance outcomes or impact delivery of other objectives.	protections with implications for delivery of critical services and other strategic objectives.		other ambitions and performance. Willing to risk vulnerability to frequent and wide-ranging impacts of climate change.
Financial	Avoidance of any financial impact or loss is a key objective.	Only prepared to accept the possibilities of very limited financial impact if essential to delivery.	Seek safe delivery options with little residual financial loss only if it could yield upside opportunities.	Prepared to invest for benefit and to minimise the possibility of financial loss by managing the risks to tolerable levels.	Prepared to invest for the best possible benefit and accept possibility of financial loss (controls must be in place).
Governance	Avoid actions with associated risk. No decisions taken outside of processes and oversight/ monitoring arrangements.	Willing to consider low risk actions which support delivery of priorities and objectives. Processes, and oversight / monitoring	Willing to consider actions where benefits outweigh risks. Processes, and oversight / monitoring arrangements enable cautious risk taking.	Receptive to taking difficult decisions when benefits outweigh risks. Processes, and oversight/ monitoring arrangements enable	Ready to take difficult decisions when benefits outweigh risks. Processes, and oversight / monitoring arrangements support informed risk taking.

Risk category	Risk appetite level and associated risk score				
	Averse	**Minimalist**	**Cautious**	**Receptive**	**Eager**
	Very low risk score acceptable 1-2	**Low risk score acceptable 3-6**	**Lower medium risk score acceptable 8-9**	**Higher medium risk score acceptable 10-12**	**High or very high risk score acceptable 15 or higher**
	Organisational controls minimise risk of fraud, with significant resource focused on detection and prevention.	arrangements enable limited risk taking. Organisational controls maximise fraud prevention, detection and deterrence through robust controls and sanctions.	Controls enable fraud prevention, detection and deterrence by maintaining appropriate controls and sanctions.	considered risk taking. Levels of fraud controls are varied to reflect scale of risks with costs.	Levels of fraud controls are varied to reflect scale of risk with costs.
Health and Safety	No appetite for staff undertaking any activities that may carry a risk to health and safety. Stringent controls to comply with legislation.	Legislation adhered to and forms the minimum accepted level of control. Regular staff training and refresher courses. Regular reviews of risk assessments and processes.	Legislation adhered to and regular staff training in place. Regular reviews of risk assessments and processes for all activities involving a higher degree of equipment usage.	Legislation mostly adhered to but with occasional breaches. Training in place to ensure staff are aware of health and safety risks. Risk assessments written but not regularly reviewed.	Legislation not adhered to with frequent breaches. No controls or training in place. All staff able to exercise their own judgment on acceptable levels of risk.
Information	All information and data are locked down. Access is tightly controlled with high levels of monitoring.	Access to and the distribution of information and data is highly controlled	Accepted need for operational effectiveness. Careful management of information and data	Accepted need for operational effectiveness in the distribution and sharing of information	Levels of control minimised with data and information openly shared. No monitoring.

Risk category	Risk appetite level and associated risk score				
	Averse	**Minimalist**	**Cautious**	**Receptive**	**Eager**
	Very low risk score acceptable 1-2	**Low risk score acceptable 3-6**	**Lower medium risk score acceptable 8-9**	**Higher medium risk score acceptable 10-12**	**High or very high risk score acceptable 15 or higher**
		with monitoring in place.	through access controls and some monitoring for most information and data.	and data. Access controls and monitoring only for specific types of information.	
Legal	Avoid anything that could be challenged, even unsuccessfully.	Would want to be very sure we would win any challenge.	Would want to be reasonably sure we would win any challenge.	Challenge would be problematic. We are likely to win and the gain will outweigh the adverse impact.	Chances of losing are high but exceptional benefits could be realised.
Operations / Service Delivery (All)	Defensive approach to operational delivery – aim to maintain/protect, rather than create or innovate. Priority for close management controls and oversight with limited devolved authority.	Innovations largely avoided unless essential. Decision making authority held by senior management.	Tendency to stick with the status quo. Innovations generally avoided unless necessary. Decision making authority generally held by senior management. Management through leading indicators.	Innovation supported with clear demonstration of benefit or improvement in management control. Responsibility for non-critical decisions may be devolved.	Innovation pursued. Desire to 'break the mould' and challenge current working practices. High levels of devolved authority. Management by trust and lagging indicators rather than close control.
Reputational	Zero appetite for any decisions with a high chance of	Appetite for risk taking limited to those events where there is	Appetite for risk taking limited to those events where there is	Appetite to take decisions with the potential to expose	Appetite to take decisions that are like to bring additional

Risk category	Risk appetite level and associated risk score				
	Averse	**Minimalist**	**Cautious**	**Receptive**	**Eager**
	Very low risk score acceptable 1-2	**Low risk score acceptable 3-6**	**Lower medium risk score acceptable 8-9**	**Higher medium risk score acceptable 10-12**	**High or very high risk score acceptable 15 or higher**
	repercussion for the Council's reputation.	no chance of any significant repercussions for the Council.	little chance of any significant repercussions for the Council.	the Council to additional scrutiny, but only where appropriate steps are taken to minimise exposure.	Council scrutiny only where potential benefits outweigh the risks.
Security	No tolerance for security risks causing loss or damage to Council property, assets, information or people. Stringent measures in place including: • Staff vetting at the highest appropriate level. • Controls limiting staff and visitor access to information,	Risk of loss or damage to Council property, assets, information, or people minimised through stringent security measures including: • All staff vetted levels defined by role requirements. • Controls limiting staff and visitor access to information,	Limited security risks accepted to support business need, with appropriate checks and balances in place: • Vetting levels may flex with teams as required. • Controls managing staff access and limiting visitor access to information,	Considered security risk accepted to support business need, with appropriate checks and balances in place. • New starters may commence employment following partial completion of vetting processes. • Controls limiting visitor	Organisation willing to accept security risk to support business need with appropriate checks and balances in place: • New starters may commence employment, following partial completion of vetting processes. • Controls limiting visitor

Risk category	Risk appetite level and associated risk score				
	Averse	**Minimalist**	**Cautious**	**Receptive**	**Eager**
	Very low risk score acceptable 1-2	**Low risk score acceptable 3-6**	**Lower medium risk score acceptable 8-9**	**Higher medium risk score acceptable 10-12**	**High or very high risk score acceptable 15 or higher**
	assets, and estate. • access to staff personal devices restricted in Council sites.	assets and estate. • Staff personal devices permitted but may not be used for official tasks.	assets and estate. • Staff personal devices may be used for limited official tasks with appropriate permissions.	access to information, assets and estate. • Staff personal devices may be used for official tasks with appropriate permissions.	access to information, assets and estate. • Staff personal devices permitted for official tasks.
Staffing/ People	Priority to maintain close management control and oversight. Limited devolved authority. Limited flexibility in relation to working practices. Development investment in standard practices only.	Decision making authority held by senior management. Development investment generally in standard practices.	Seek safe and standard people policy. Decision making authority generally held by senior management.	Prepared to invest in our people to create an innovative mix of skills environment. Responsibility for noncritical decisions may be devolved.	Innovation pursued. Desire to 'break the mould' and challenge current working practices. High levels of devolved authority. Management by trust rather than close control.
Technology	General avoidance of system or	Only essential systems or technology	Consideration given to adoption of	Systems or technology developments are	New technologies are viewed as a key

Risk category	Risk appetite level and associated risk score				
	Averse	**Minimalist**	**Cautious**	**Receptive**	**Eager**
	Very low risk score acceptable 1-2	**Low risk score acceptable 3-6**	**Lower medium risk score acceptable 8-9**	**Higher medium risk score acceptable 10-12**	**High or very high risk score acceptable 15 or higher**
	technological developments.	development to protect current operations.	established or mature systems and technology improvements. Agile principles are considered.	considered to enable improved delivery. Agile principles may be followed.	enabler of operational delivery. Agile principles are embraced.

Based on:

113. Government Finance Function, 2021. *Risk Appetite Guidance Note v2.0*. London: HM Treasury. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1012891/20210805_-_Risk_Appetite_Guidance_Note_v2.0.pdf [Accessed 22 September 2023].

114. HM Treasury, 2006. *Thinking about risk. Managing your risk appetite: A practitioner's guide*. London: MH Treasury. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/191519/Setting_and_communicating_your_risk_appetite.pdf [Accessed 22 September 2023].