FOR PUBLICATION

DERBYSHIRE COUNTY COUNCIL

AUDIT COMMITTEE

20 July 2021

Report of the Director of Finance & ICT

Corporate Risk Management Strategy 2021-2025

1. Purpose

1.1 To agree the Corporate Risk Management Strategy 2021-2025 and refer it to Cabinet for formal approval.

2. Information and Analysis

2.1 The Corporate Risk Management Strategy describes the context, policy and process for risk management in the Council. The Strategy is thoroughly reviewed every four years to support delivery of the new Council Plan. Interim updates are made in the intervening years as necessary.

2.2 The proposed Corporate Risk Management Strategy for 2021-2025 is shown in Appendix 2. This builds on the previous Strategy, with an emphasis on improving performance so that the Council is among the best performing local authorities for risk management by December 2024.

2.3 The proposed Corporate Risk Management Strategy uses national and international standards, builds on the principles and aspirations in the existing strategy and uses recognised risk management practices. Risk management practice is kept under constant review. Best practice is shared between local authorities, ALARM and insurance companies on a regular basis and learning incorporated into the Council's business processes as appropriate

2.4 Effective risk management is vital for delivering the Council's strategic and operational objectives. Risk management reduces the uncertainties involved with delivery and increases the likelihood of achieving the intended outcomes described in the Council Plan and subsidiary service delivery plans.

2.5 The revised Strategy strengthens existing arrangements and sets out clearer expectations about risk management. Key changes are proposed in the following areas:

- Clearer definitions of strategic and operational (process and resources) risks, and introduction of the term 'major risk' to refer to risks assessed as 'Red' or 'Amber' requiring the most active management attention and regular oversight.
- The adoption of national and international standards for organisational resilience (BS6500:2014 and ISO 22301:2019), supplementing existing use of the risk management standard (BS ISO 31000:2018), to strengthen business continuity practices required to meet the Council's obligations under the Civil Contingencies Act 2004.
- Clearer steps to embed 'enterprise risk management' to improve understanding of corporate risk exposure, a focus on identifying and managing portfolios of risk related to specific areas of delivery, and consistency of practice across the Council.
- Improved support for corporate decision making, with business cases and Council papers clearly identifying major risks and corporate exposure for informed and balanced decisions about risk acceptability ('risk appetite').
- Deepening and strengthening the culture and governance of risk management at all levels of the Council to improve performance.
- Publication of a corporate risk register alongside the Council Plan and updated each year, beginning in 2022-23, setting out for the public the Council's strategic and operational risk environment and its approach to risk acceptance and management as an Enterprising Council.
- Improved service planning to identify, assess and manage portfolios of risk related to all services and deliverables described in service delivery plans.
- A greater focus on the potential impact when assessing the severity of risks and scoring reputational risk separately to provide greater visibility of this aspect for management and decision making.
- A clear process for risk management, based on the national and international standards, to provide a more systematic approach in

identifying, assessing and actively managing risk throughout the delivery lifecycle, including a consistent and robust approach to business continuity planning and management, and a more systematic review and incorporation of lessons learned to improve performance.

- Improved recording of corporate risks by expanding the Council's performance information system (APEX) to record risk data and allow improved analysis, monitoring and reporting.

2.6 An outline implementation plan is shown in Appendix 3. Leadership and oversight of the Strategy and progress in meeting performance targets will be provided by the Council's Corporate Management Team and Corporate Risk Management Group (CRMG). Progress will be reported regularly to the Audit Committee each quarter.

2.7 The Council's capability in risk management will be assessed using the CIPFA/ALARM[1] risk management maturity framework shown in Appendix 4. A self-assessment is currently being undertaken in all parts of the Council to set the baseline for measuring progress towards the December 2024 performance target. Progress will be reviewed and reported quarterly, with an external independent assessment provided each year.

2.8 InPhase provides the software for the existing APEX performance information system. The Council has exercised its option in the existing contract to add the InPhase risk management module as a fully integrated enhancement to the system. The Council has the option to extend its contract with InPhase on an annual basis to end on 31 October 2025 at the latest. Future options for APEX will be considered prior to the contract expiry date.

3. Alternative Options Considered

3.1 The CIPFA/ALARM methodology is widely accepted across the public sector and provides a benchmarking facility across other Councils. The Council approved the methodology for use as part of the current risk management strategy. An alternative would be to adapt the CIPFA/ALARM risk maturity framework or devise our own scoring mechanism. This would require further development work and undermine the current baseline benchmarking work already underway. Doing nothing would mean the Council has no means to measure its performance in a consistent way. We therefore recommend that the council continues to use the CIPFA/ALARM risk maturity framework.

[1] Chartered Institute for Public Finance and Accountancy (CIPFA)/Association of Local Authority Risk Managers (ALARM)

3.2 The InPhase risk management module is designed to fully integrate with the existing software used for APEX and was available as an option under the existing InPhase contract. Rather than using the InPhase Risk Management module, the Council considered in-house development and procuring a stand-alone system to report on risk management. This would potentially have increased costs as that system would need to integrate with InPhase to link risk with performance data; would potentially be more expensive as a standalone purchase; increase the draw on ICT resources and extend the implementation timescales. We therefore exercised the option to purchase the InPhase risk management module under the existing contract. Future options will be fully considered when the existing contract comes up for renewal.

4. Implications

4.1 Appendix 1 sets out the relevant implications considered in the preparation of the report.

5. Consultation

5.1 Internal consultation in preparing the strategy has been conducted with the Director of Finance & ICT, Director of Legal and Democratic Services and other members of the CRMG.

6. Background Papers

6.1 Derbyshire County Council Risk Management Strategy & Implementation Plan 2019-2021 (Version 2.7)

7. Appendices

7.1 Appendix 1 – Implications
Appendix 2 – Draft Corporate Risk Management Strategy 2021-2025
Appendix 3 – Outline implementation plan
Appendix 4 – CIPFA/ALARM risk management maturity framework

8. Recommendation(s)

That the Audit Committee:

a) Agrees the Corporate Risk Management Strategy 2021-2025 and refers it to Cabinet for formal approval; and
b) Notes the outline implementation plan.

9. Reasons for Recommendation(s)

9.1 The revised Strategy strengthens existing arrangements and sets out clearer expectations about risk management.

9.2 To ensure that the Council has robust risk management arrangements in place which drive up performance, improve decision making, strengthen business continuity arrangements, and fully embed the principles of 'enterprise risk management' across the Council.

Report Author: Jane Morgan
Risk and Insurance Manager, Finance & ICT Division
Contact details: jane.morgan@derbyshire.gov.uk

This report has been approved by the following officers:

On behalf of:	
Corporate Risk Management Group	Helen Barrington
Director of Legal Services and Monitoring Officer	Helen Barrington
Director of Finance and ICT	Paul Stone
Managing Executive Director	Helen Barrington
Executive Director(s)	Helen Barrington

Appendix 1

Implications

Financial

1.1 The cost of implementing the corporate risk management strategy and InPhase risk management module will be absorbed within existing budgets.

1.2 The Strategy is expected to deliver increased value for money through improvements to decision making, managing service delivery outcomes and contingency planning. Improved risk management is also expected to reduce financial liabilities arising from losses which are met from within the Council's insurance deductible (excess) and to help in controlling the authority's insurance premium.

Legal

2.1 The Strategy will help the Council to deliver its obligations as a Category 1 responder under the Civil Contingencies Act 2004 more effectively. Improved risk management is also expected to help to reduce the likelihood of legal claims against the Council and the number of occasions the Council would need to pursue legal action.

Human Resources

3.1 It is proposed to recruit a corporate business continuity management specialist to advise and support with development and updating of the Council's business continuity plans. The officer will be managed within the Council's Emergency Planning Team.

3.2 All other implementation of the Strategy will be met using existing human resources.

Information Technology

4.1 The risk management module is an extension to existing InPhase software already used to support APEX. The module is designed for full compatibility and integration with the other InPhase modules.

4.2 The InPhase software offers considerable user configuration to meet business needs, including bespoke dashboards and customised reporting formats.

Equalities Impact

5.1 An equality impact analysis has not been completed as there are no substantial proposals being made to alter a policy, service, or function in the delivery of risk management.

5.2 Implementation of the strategy will improve the identification and assessment of risks, including the impact on equality, reducing the potential for legal challenges under the Equality Act 2010.

Corporate objectives and priorities for change

6.1 CCP service plan 2021-2025 deliverable: Rolled out the revised Risk Management Strategy (April 2021-March 2022). Owner: Jane Morgan (Finance and Audit).

6.2 This also contributes to the CCP deliverable: Further developed and embedded the Council's performance management framework (April 2020-June 2021). Owner: Sarah Eaton (Strategy and Policy).

6.3 Implementation of the Corporate Risk Management Strategy will support the better delivery of all corporate aims and objectives.

Appendix 2

DERBYSHIRE
County Council

CORPORATE RISK MANAGEMENT STRATEGY

2021-2025

Version History			
Version	**Date**	**Detail**	**Author**
3.01	10.05.2021	First draft	Tony Kearsey
3.02	04.06.2021	Second draft	Tony Kearsey
3.03	11.06.2021	Third draft	Tony Kearsey
3.04	29.06.2021	Fourth draft	Tony Kearsey
3.05	13.07.2021	Audit Committee approval	Tony Kearsey

Contents

1. Introduction
2. Definition of risk management
3. The benefits of good risk management
4. Policy statement
5. Standards and performance
6. Enterprise risk management
7. Acceptable levels of risk
8. Culture
9. Governance and management
10. Corporate planning and delivery
11. Risk management process
12. Data protection
13. Risk management training
14. Implementation
15. Further support

Appendices

A. Risk assessment scoring tables
B. Glossary

1. Introduction

The Council is committed to improving its risk management performance to deliver better outcomes and greater public value for Derbyshire residents and businesses.

The Council's ambition is to be among the best performing local authorities for risk management by December 2024. This strategy sets out how we will deliver this transformational ambition using a 'one council' framework to actively manage risk at all levels of the organisation, from elected members and senior officers to managers and all those on the frontline delivering services to the public.

Feedback

This strategy is kept under constant review and feedback is always welcome. Any comments, best practice ideas and suggestions on how the Council can improve its risk management should be sent to: riskandinsurance@derbyshire.gov.uk

2. Definition of risk management

The Council has adopted the following definitions of risk and risk management:

(a) Risk

A 'risk' is an internal or external opportunity, event, issue, relationship, process or resource which presents a degree of uncertainty in delivering a desired outcome.

A 'strategic risk' is a risk which has a fundamental impact on the Council's purpose, constitution, strategic aims and objectives and ability to carry out its statutory and other major obligations.

An 'operational risk' is either a 'process' or 'resource' risk:

- 'Process risk' - a risk which concerns the policies, procedures, plans, practices and related vulnerabilities in successfully delivering the Council's strategic and operational aims and objectives.

- 'Resource risk' - a risk which concerns the human, financial, physical, information and intellectual resources of the Council required to successfully deliver its strategic and operational aims and objectives.

A 'major risk' is a risk which has been assessed as 'Red' or 'Amber' using the Council's corporate risk assessment criteria.

(b) Risk management

'Risk management' is the proactive identification, assessment, acceptance and management of risks to successfully deliver the Council's vision, aims, objectives and statutory obligations.

3. The benefits of good risk management

Good risk management offers the Council many benefits, including:

- Creating greater public value by reducing uncertainty, leading to the delivery of better services and outcomes.
- Protecting and enhancing the Council's reputation as a local authority.
- Ensuring statutory and other obligations are met.
- Achieving greater organisational and community resilience.
- Protecting the Council's assets, including property and information.
- Better decision making, management control, and resource allocation.
- Increasing value for money from public funds and the Council's other resources.
- Minimising liabilities, including legal action and claims against the Council.
- Improving assurance and public accountability.

4. Policy statement

The Council is committed to being among the highest performing local authorities in England for risk management. To deliver this ambition, the Council has adopted relevant risk management standards and an enterprise risk management (ERM) operating framework.

The Council overall has a moderate tolerance of risk. Acceptance of specific risks will be exercised flexibly according to business needs, benefits and priorities.

The Council will exercise a proportionate approach, focussing management attention on those risks with the highest potential impact on delivery and greatest uncertainty.

5. Standards and performance

The Council's strategy is guided by the principles and aims of risk management, resilience and business continuity management set out in the following standards:

- BS ISO 31000:2018 - Risk management - Guidelines.
- BS 65000:2014 – Guidance on organizational resilience

- ISO 22301:2019 – Security and resilience – business continuity management systems - requirements

Progress will be measured using the CIPFA risk management capability framework. The Council aims to achieve the following levels of performance in all framework categories by the dates shown below:

- Level 3 (Working) – by March 2022
- Level 4 (Embedded and Working) – by March 2023
- Level 5 (Driving) – by December 2024

All Departments are collectively and individually responsible for delivering the Council's ambition and targets.

Departments are accountable for progress to the Corporate Management Team (CMT) and Audit Committee, with advice and support available from the governance and corporate risk management groups, corporate risk and insurance team and internal audit.

6. Enterprise risk management

The Council's strategy is based on the 'enterprise risk management' (ERM) approach. This means greater public value is delivered as:

- The Council takes a 'one council' view of risk, focussed on the risks associated with corporate objectives and deliverables rather than Departmental boundaries.
- Risk management is an integral part of good management and decision-making, embedded in the structure, operations, and processes of the Council at strategic, operational, programme and projects levels.

This approach offers many benefits, including:

- A consistent approach to risk management across the Council.
- An overview of risks related to a service and deliverable, and their importance.
- Ensuring statutory and other obligations are met.
- Protecting and enhancing the Council's reputation as a local authority.
- Protecting the Council's assets, including property and information.
- Better decision making, management control, and resource allocation.
- Increasing value for money from public funds and the Council's other resources.
- Minimising liabilities, including legal action and claims against the Council.
- Achieving greater organisational and community resilience.
- Improving assurance and public accountability.

The key elements in delivering this approach are:

Culture

- Creating a risk-aware culture – embedding risk awareness and management at all levels of the Council (described further in Section 8 below).

Strategy and decision making

- Horizon scanning – regular horizon scanning for external risks likely to have a strategic impact on the Council's purpose and activities.
- Critical decision making - informed risk assessment and recommendations for all critical decisions taken by Cabinet, CMT and departmental management teams, including how major risks will be managed.

Management

- Portfolio risk management - identifying and managing all strategic, process and resource risks in the context of specific services and objectives (i.e. deliverables).
- Managing combined risk exposure – assessing and managing the exposure of all related risks across the Council.
- Benefits management – ensuring that desired outcomes are achieved, by actively managing significant hazard risks and having effective contingency arrangements in place.
- Minimising disruption – ensuring that unexpected disruption to delivery of critical objectives, services and core processes is minimised through effective business continuity management and planning.

Reporting and assurance

- Integrated performance reporting - corporate performance reporting on the delivery of objectives to include all directly related major risks and combined risk exposure.
- Assurance - structured assurance arrangements for CMT, the Audit Committee and Cabinet, focussed on risk portfolios for Council objectives and core processes.

7. Acceptable levels of risk

The Council accepts that risk is an inherent part of innovation, pursuing new opportunities and delivering high quality services. It also accepts that it is not possible, practical, or desirable to eliminate all risk from its activities.

The Council therefore seeks to manage all risk within acceptable levels (its ‘risk appetite’ or ‘tolerance’). While overall having a moderate tolerance of risk, the level of risk accepted will vary between the opportunities being sought, activities being delivered and the overall risk exposure from combined risk of a similar nature.

A flexible approach will be used, with balanced decisions made on a case-by-case basis to decide how much risk the Council will accept, taking account of the:

- General guide to the Council’s risk appetite, shown in Table 1.
- Potential benefits and disbenefits of accepting each risk.
- Related portfolio of risk (e.g. property, financial investments, client groups etc.).
- Impact on the Council’s aims, objectives, and reputation if the risk materialised.

Table 1 – Risk appetite guide

Acceptability (or ‘tolerance’)	**Examples**
Lower acceptability	• Statutory responsibilities. • Safeguarding of vulnerable adults and children. • Health and safety of the public and employees. • Community safety. • Safety critical maintenance. • Larger investments with smaller returns or limited public benefit.
Limited acceptability	• Unproven policy and service innovations with a significant risk of failure, but with the potential for substantial public or economic benefit (a limited number of such innovations will be pursued at any time).
Higher acceptability	• Smaller investments with higher returns or wider public benefit. • New opportunities, potentially with substantial public or economic benefit, which have an existing evidence base and offer more certainty of a successful outcome. • Organisation and service efficiency measures which offer significantly improved performance, including ‘spend to save’ measures, with a high likelihood of success.

8. Culture

Risk management is the responsibility of everyone in the Council. The Council therefore aims to promote a culture of active risk management at all levels of the organisation.

Building a strong risk-aware culture offers many benefits, including:

- A clear understanding by everyone that good risk management is fundamental in delivering the best outcomes.
- Much greater awareness of different types of risk, and how it impacts on the wider aims, objectives, and reputation of the Council.

- Routinely considering risk in all decision making, with more significant risks quickly identified and escalated for higher-level management attention as needed.
- Improved dynamic risk management, by developing an individual's judgement in routinely considering and managing risk in all day-to-day activities.
- Greater community satisfaction and fewer claims against the Council.

9. Governance and management

Responsibility and accountability for overseeing and delivering the risk management strategy, including promoting a risk-aware culture, are distributed throughout the Council. Specific roles and responsibilities are:

(a) Governance

Council Leader and Cabinet members

The Council Leader and Cabinet members have governance responsibility, including:

- Approving the Council's risk management strategy and framework.
- Receiving assurance from the Audit Committee on the Council's risk management strategy, performance and implementation
- Receiving the Managing Executive Director's annual risk management report.
- Receiving occasional reports on strategic risks affecting the Council.

Audit Committee

The Audit Committee has responsibility for detailed oversight and scrutiny of the Council's risk management arrangements and performance on behalf of the Council Leader and Cabinet members, including:

- Overseeing the corporate risk management strategy and framework and its implementation.
- Overseeing risk management by officers, including ensuring that risks are adequately considered when setting Council and departmental objectives and that only appropriate risks are accepted.
- Regularly reviewing the corporate risk register and progress with managing major risks.
- Monitoring the adequacy of the risk management arrangements and their implementation.
- Overseeing delivery of the Council's ambition to achieve Level 5 (Driving) on the CIPFA risk management capability framework, by December 2024.
- Providing assurance to the Council Leader and Cabinet members on all aspects of risk management.

(b) Management

Corporate Management Team

The Managing Executive Director is accountable to the Council Leader and Audit Committee for risk management in the Council. All members of the Corporate Management Team (CMT) have responsibility for:

- Promoting a strong risk management culture.
- Having a clear understanding of the external and internal risk environment, and the impact of this on the successful delivery of the Council and service delivery plans.
- Ensuring that major risks and overall risk exposure are fully assessed and reflected in advice and recommendations for the Cabinet to make informed decisions.
- Challenging risk management performance, including seeking assurance of satisfactory progress in managing all significant risks.
- Leading and driving delivery of the risk management strategy, including the Council's ambition to achieve Level 5 (Driving) on the CIPFA risk management capability framework, by December 2024.

Corporate Risk Champion - the Corporate Risk Champion is an Executive Director nominated by the CMT to actively promote the aims of the corporate risk management strategy in the Council.

Corporate Risk Management Group (CRMG)

The Corporate Risk Management Group (CRMG) has responsibility for:

- Providing oversight of corporate risk management issues, including delivery of the Council's corporate risk management strategy.
- Regularly reviewing strategic risks to the Council for the attention of CMT and Audit Committee, including those for potential inclusion in the annual update to the Council's corporate risk register.
- Promoting the principles of enterprise risk management in the Council.
- Maintaining an overview of the Council's business continuity and contingency planning arrangements, including its interface with the Derbyshire Local Resilience Forum.
- Considering corporate risk management training and development for Councillors and officers, including the development of specialist risk expertise.

Senior management teams

Each Executive Director is accountable to the Managing Executive Director for risk management in their department. All senior department, directorate and division management teams have responsibility for:

- Having a clear understanding of the external and internal risk environment, and the impact of this on the successful delivery of the service delivery plan.
- Ensuring that significant risks and overall risk exposure are fully assessed, regularly reviewed, and reflected in advice and recommendations for the CMT and Cabinet to make informed decisions.
- Regularly reviewing and challenging risk management performance, including seeking assurance of satisfactory progress in managing risks within the department and by each directorate and division.
- Conducting a periodic self-assessment of progress by their department and each directorate and division in meeting corporate risk management performance targets detailed in Section 5 above.

Managers

All managers have responsibility for:

- Understanding and implementing the corporate risk management strategy.
- Communicating and supporting good risk management practice in their teams.
- Keeping abreast of all risks related to their responsibilities.
- Ensuring that risks are actively managed, recorded and progress regularly updated on APEX and local risk action plans as necessary.
- Promptly escalating issues to senior managers as necessary.

All other employees

All employees have responsibility for:

- Managing risk effectively in their own jobs.
- Using risk assessments effectively and suggesting to a manager where an assessment would be beneficial.
- Reporting unassessed hazard risks to their manager.

10. Corporate planning and delivery

The consideration, understanding and informed acceptance of risks is an integral and vital part of corporate planning, delivery management and performance monitoring.

Sufficient time will be given for the CMT, Audit Committee and Cabinet to consider and agree their appetite for proposed activities and risks prior to publication of the Council plan, corporate risk register and service delivery plans.

Council plan

When preparing the four-year Council Plan, due consideration will be given to the risks to the Council in setting specific aims, objectives, and key deliverables. This will include, but is not limited to:

- The Council's vision, mission and values.
- The social, cultural, political, legal, regulatory, financial, technological, economic and environmental context at international, national, regional and local levels as appropriate.
- Key drivers and trends.
- External and internal stakeholders' relationships, perceptions, values, need and expectations.
- Statutory obligations, contractual relationships and commitments.
- The Council's strengths, weaknesses and capabilities, in terms of resources and knowledge.
- Any limits set by statute or government policy on what the Council can do.
- The overall portfolio of risk and risk exposure.

Corporate risk register

The corporate risk register will be compiled from the corporate planning process and published alongside the Council Plan from 2022-2023.

The corporate risk register will contain those strategic and operational risks that could materially threaten the Council's operating model, future performance, ability to deliver its statutory obligations and a balanced budget, may substantially affect its reputation, or which could prevent the Council pursuing and delivering its strategic objectives and significant new opportunities.

Both the Council Plan and corporate risk register are public documents. They are reviewed and updated annually.

Service delivery plans

Service delivery plans set out in greater detail how the aims, objectives and key deliverables described in the Council Plan will be delivered in each service area.

Following the principles of enterprise risk management, service delivery plans should refer to all major risks related to the delivery of core services, regardless of where responsibility for managing a risk rests within the Council.

The proposed core services and related resource requirements form the basis for risk identification and assessment. Many of the risk factors considered in preparing the Council Plan will be addressed in more detail, together with consideration of other factors. Risk factors will include, but are not limited to:

- The relative public value created by each activity in relation to the risk appetite.
- Relevant statutory requirements, standards, guidelines, and delivery models.
- Available data, information systems and information flows.
- Allocated capital and revenue budgets.
- Savings targets.

11. Risk management process

Risk management is a dynamic, collaborative, and structured process. The risk management process underpins decision making about service planning, including which new opportunities to pursue, through to the successful delivery and realisation of the intended outcomes and benefits.

Service delivery

All current services, programmes and deliverables should be supported by a full assessment of strategic, process and resource risks and a risk action plan.

New opportunities

The Council will pursue new opportunities where there is a justified benefit and the related risks are acceptable. All new proposals and business cases should include a full assessment of strategic, process and resource risks to support informed decision making by senior officers and members.

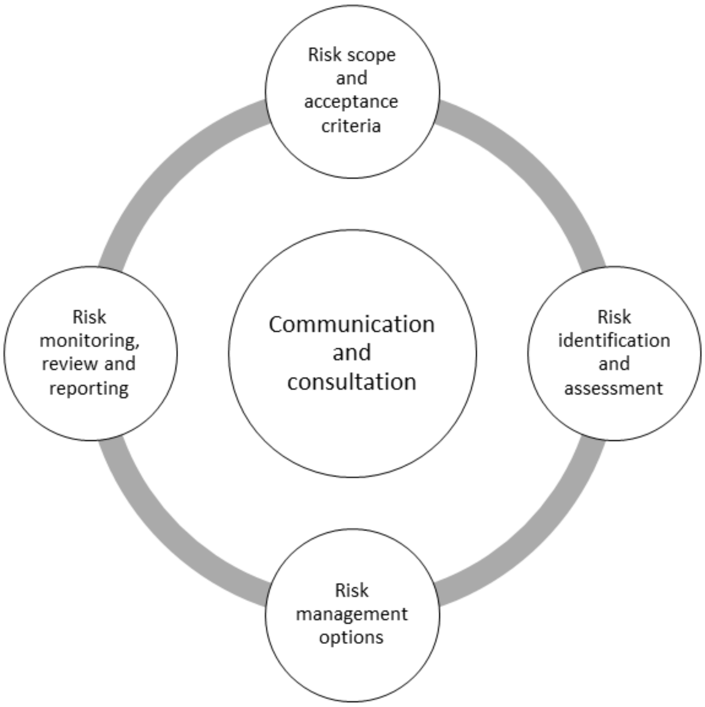
Risk management process

The key elements of the risk management process are:

- Communication and consultation.
- Risk scope and acceptance criteria.
- Risk identification and acceptance.
- Risk management options.
- Risk monitoring, review and reporting.

These are shown in Figure 1 and described further below.

Figure 1 – Risk management process


Risk scope and acceptance criteria
Risk identification and assessment
Risk management options
Risk monitoring, review and reporting
Communication and consultation

(a) Risk scope and acceptance criteria

New proposals, services, programmes, and key deliverables in service delivery plans will provide the focal point and context for risk identification and assessment.

The scope of risks covered will include:

- All relevant internal and external strategic, process and resource factors which contribute to the successful delivery of each outcome and deliverable.
- Wider considerations, including the potential overall exposure from related risks across the Council and significant impacts on the community, businesses, and partners.

The criteria for risk acceptance will include consideration of:

- The Council's risk appetite in relation to the new opportunity, service, programme or deliverable, weighing the intended benefits with hazard risks.
- The nature and type of uncertainties (both tangible and intangible) related to the intended outcome and deliverable.
- How wider impacts will be assessed.
- The Council's capacity to manage the risks during the period of delivery, including the robustness of management arrangements to deliver the intended benefits.

(b) Risk identification and assessment

All key risks which could prevent or disrupt achieving an objective or deliverable should be identified and assessed systematically. The best available information should be used, drawing on the knowledge and views of internal and external stakeholders as necessary.

Risk should be assessed using the scoring tables in Appendix A. The risk impact scoring criteria may be reworded for customised use within programmes and projects, provided the risk impact grading criteria remain consistent with Appendix A for corporate reporting purposes.

The complexity of the assessment needed will take account of the potential impact of a risk, both positive and negative, on the intended outcome and reputation of the Council.

Relevant quantitative and qualitative information should be used in assessing the severity of a risk, which may include:

- Tangible and intangible sources of risk.
- Potential changes in the internal and external context, including emerging risks.
- The potential for unintended, different or multiple impacts and outcomes.
- The actual and potential consequences for internal and external stakeholders, and their perception of the Council.
- The nature, value and availability of resources.
- Time-related factors.

Due care should be taken to understand the limitations in knowledge and information for decision making, including reliability, assumptions, biases, and beliefs.

Assessments will be documented and used in evaluating the acceptability of risks, obtaining approvals, managing the delivery of benefits, and for evaluating overall success in delivering the intended outcomes and organisational learning.

(c) Risk management options

Decisions to accept risks will depend on a range of factors, including the Council's overall risk appetite, obligations, discretionary goals and commitments, stakeholder views, financial and legal exposure, and reputational impact.

Risk acceptance

Risk appetite and acceptance will depend on how well a risk can be managed, considering:

- The balance of benefits and disbenefits of taking the risk, including the Council's overall exposure to similar risks.
- The benefits balanced with the cost, management effort, potential impact and likelihood of the risk occurring.
- Acceptability to stakeholders.
- Whether the risk has a higher or lower impact assessment.

- The severity of the risk, and if management action can contain the risk within the Council's risk appetite.

Management options

Four main options are available for managing risk (known as the '4T's').

Management action for risks with lower impact will tend towards:

- **Toleration** – accepting the risk with no active management action.
- **Treatment** – active management action to control or reduce the risk exposure to an acceptable level.

Action for risks with higher impact will tend towards:

- **Transfer** – transferring the risk to a third party, usually through a contract or insurance.
- **Termination** – not accepting the risk if it is judged too high, even after mitigation.

The most appropriate option or combination of management options will be used for each risk and recorded in APEX.

Risk management plans for major risks

More detailed risk management plans will be produced for major risks (assessed as Amber or Red). Plans will specify management action, how it will be implemented and used for communication and monitoring progress.

These plans should include the rationale for selecting risk management options, actions and intended impact, resources needed, any performance measures, constraints, when actions are expected to be undertaken and completed, and reporting and monitoring arrangements.

The risk management plans for major risks will be recorded in APEX.

Business continuity and contingency planning

A risk impact assessment should be completed for all core services, deliverables and supply chains, and appropriate business continuity and contingency arrangements put in place as necessary and maintained.

These arrangements should be effective in managing the potential impact of a risk and building organisational resilience for critical services and functions in both emergency and non-emergency situations.

The Civil Contingencies Act 2004

The Council's statutory responsibilities for business continuity are defined in The Civil Contingencies Act 2004. As a Category 1 responder, the Council must maintain plans to ensure it can continue to exercise its functions in the event of an emergency so far as is reasonably practicable.

The Council's duty under the Act relates to all the functions of a Category 1 responder, which include:

- Making provision for ensuring that ordinary functions can be continued to the extent required.

- Maintaining plans to deal with emergencies.
- Having arrangements to warn and inform the public in the event of an emergency.
- Having a training programme for those directly involved in the execution of the business continuity planning.
- Promoting business continuity management to businesses and voluntary organisations.

In developing business continuity and contingency plans, departments should work closely with the Council's emergency planning team as necessary, which is also responsible for co-ordinating with other Category 1 and 2 responders represented on the Derbyshire Local Resilience Forum.

(d) Monitoring, review and reporting

Management actions must be actively monitored and reviewed regularly to provide assurance that risks are being managed effectively. Changes should be made if actions are not working or have created new risks which need managing.

Risk recording

Corporate strategic and operational risks will be recorded and monitored using the Council's APEX performance reporting system being introduced during 2021-22.

The use of APEX for recording strategic and operational risks does not replace the need for specific local risk assessment, recording and monitoring arrangements where these are appropriate. This includes the safeguarding of individual vulnerable adults and children, legal cases, local health and safety assessments and similar examples.

The risk management component in APEX will be developed progressively during 2021-2024 to provide further analysis and management information as needed.

Management team risk reviews

Senior management teams should regularly review progress with risk management and identify any 'rising star' risks. Priority should be given to the most significant corporate risks, with reviews as follows:

- Red risks – at least every month
- Amber risks – at least every two months
- Green risks – at least every three months
- Blue risks – at least every six months

Corporate risk reviews and reports

The timetable for corporate risk reviews and reports to support formal governance and senior management oversight is published by the Corporate Risk and Insurance Team at the beginning of each financial year.

A summary of main reviews and reports, including their audience and frequency, is shown in Table 2.

Table 2 – Corporate risk reviews and reports

Report	Audience	By whom	Frequency
Corporate risk register (alongside Council Plan)	Public	Cabinet	Annually
Annual report on corporate risk management	Cabinet	Audit Committee and Managing Executive Director	Annually
Performance and Finance Reports (by Cabinet portfolio)	Cabinet Portfolio Holders	Lead Executive Director and Director of Finance & ICT	Quarterly
Service delivery plans (incorporating major service delivery risks)	Cabinet	Executive Directors	Annually
Review of corporate and major service delivery risks by department or service area	Audit Committee	Executive Director/Directors	Annually (each department or service area)
Corporate risks exception report	Audit Committee	Risk and Insurance Manager	Quarterly
Corporate risks review (APEX report)	CMT	Risk and Insurance Manager	Quarterly
Service delivery risk action plans (APEX report)	Senior management teams	Executive Directors, Directors, and heads of teams	Ongoing
Cabinet/CMT Papers (incorporating risk assessments)	Cabinet and CMT	Lead Executive Director/Director	As submitted
Corporate risk reports (specific topics)	Audit Committee and CMT	CRMG	As required

Lessons learned

Consideration of lessons learned should be included in regular management reviews to identify best practice, understand and learn from failures in all areas of activity, including projects, incidents, events, complaints, breaches, claims and accidents.

Lessons which may have relevance for the wider Council should be reported to the corporate risk and insurance team, which will also support significant post-incident lessons learned reviews as required.

12. Data protection

No personal data will be recorded in the corporate risk register or APEX.

Where personal data is required for risk management, this will be recorded locally in a confidential register maintained separately by the relevant department or team and managed in compliance with the Council’s information governance strategy and data protection legislation.

Other sensitive non-personal data can be recorded and protected within APEX.

13. Risk management training

The CRMG will consider and advise on risk management training and development for members (in consultation with the Governance Group), Directors, managers and other employees. This will include both general and specialist training and development needs and their delivery.

All managers should ensure that risk management performance, skills development and training is included in all employees’ ‘My Plan’ and discussed during reviews.

14. Implementation

An implementation plan to deliver the Council’s ambition and strategy will be approved and overseen by the CRMG, which will act as the programme board.

Regular reports on progress will be provided to the CMT and Audit Committee by the Director of Finance & ICT.

15. Further support

Further information, advice and support in implementing this strategy is available from the Corporate Risk and Insurance Team:

RiskandInsurance@derbyshire.gov.uk.

Appendix A – Risk assessment scoring tables

A risk is assessed by taking account of:

- Impact – the potential consequences if the risk materialised.
- Likelihood – the likely time period in which the risk could materialise.

Each risk is categorised according to its severity using the traffic light system shown in Table A1.

Greatest emphasis is given to impact scores to highlight those risks needing the most management attention.

Table A1 – Risk severity

Impact Score	Extremely high	4	Green	Amber	Red	Red	Red
	High	3	Green	Green	Amber	Red	Red
	Moderate	2	Blue	Green	Green	Amber	Amber
	Low	1	Blue	Blue	Green	Green	Green
	None	0	Blue	Blue	Blue	Blue	Blue
			1	2	3	4	5
			Rare	Unlikely	Possible	Probable	Almost certain
			Likelihood Score				

Tables A2 and A3 show the detailed criteria for assessing likelihood and impact.

Table A2 – Likelihood scoring

5	**Almost certain**	The event is expected to occur every year
4	**Probable**	The event could occur every year
3	**Possible**	The event could occur every two years
2	**Unlikely**	The event could occur every five years
1	**Rare**	The event could occur every 10 years or longer

Table A3 – Impact scoring

All relevant impact areas should be graded, with the highest scoring area (the ‘primary impact’) used to assess risk severity.

Note 1: Confidential risk assessment of specific individuals, legal action or claims should be undertaken separately and recorded locally by the relevant Division.

	Impact grading	Public and employee health, safety and wellbeing	Community	Economy	Environment	Service Disruption	Skills capability	Legal	Contracts and Partnerships	Information Security
4	**Extremely high**	Substantial level of harm to the health, safety and wellbeing of the community, members of the public or employees	Substantial disadvantage to large parts of the community and/or many vulnerable residents	Substantial negative impact on the County’s economy, including hard infrastructure	International and/or national environmental damage	Substantial external or internal disruption and/or loss of service (more than seven days)	Substantial under-performance from skills gaps and/or shortages	Substantial legal action, claims and/or and penalties against or by the Council	Substantial impact on service delivery from a contract and/or partnership failure	Substantial breach; Information Commissioner Office (ICO) fine; loss of ISO 27001 certification
3	**High**	Significant level of harm to the health, safety and wellbeing of the community, members of the public or employees	Significant disadvantage to large parts of the community and/or some vulnerable residents	Significant negative impact on the County’s economy, including hard infrastructure	Significant regional environmental damage and/or failure to meet all or most internal climate change targets	Significant external or internal disruption and/or loss of service (between three to seven days)	Significant under-performance from skills gaps and/or shortages	Significant legal action, claims and/or penalties against or by the Council	Significant impact on service delivery from a contract and/or partnership failure	Significant external breach with no loss of sensitive data; or minor external breach with loss of sensitive data

	Impact grading	Public and employee health, safety and wellbeing	Community	Economy	Environment	Service Disruption	Skills capability	Legal	Contracts and Partnerships	Information Security
2	**Moderate**	Moderate level of harm to the health, safety and wellbeing of the community, members of the public or employees	Moderate disadvantage to large parts of the community and/or some vulnerable residents	Moderate negative impact on the County's economy, including hard infrastructure	Moderate regional and/or major local environmental damage and/or failure to meet many internal climate change targets	Moderate external or internal disruption and/or loss of service (between 24 to 48 hours)	Moderate under-performance from skills gaps and/or shortages	Moderate legal action, claims and/or penalties against or by the Council	Moderate impact on service delivery from a contract and/or partnership failure	Significant internal breach with no loss of sensitive data; or minor internal breach with loss of sensitive data
1	**Low**	Minimal level of harm to the health, safety and wellbeing of the community, members of the public or employees	Minimal disadvantage to the community and/or some vulnerable residents	Minimal negative impact on the County's economy, including hard infrastructure	Minimal regional and/or local environmental damage and/or failure to meet some internal climate change targets	Minimal external or internal disruption and/or loss of service (less than 24 hours)	Minimal under-performance from skills gaps and/or shortages	Minimal legal action, claims and/or penalties against or by the Council	Minimal impact on service delivery from a contract and/or partnership failure	Minor external or internal breach with no loss of sensitive data
0	**None**	No impact	No impact	No impact	No impact	No impact	No impact	No impact	No impact	No impact

All risks have the potential to impact on the Council’s reputation. Each risk is given a separate reputation impact assessment, as shown in Table A4.

Table A4 – Reputation impact assessment

Extremely High	Lasting or permanent national/local brand damage resulting from adverse comments in national press and media. Members/Officers almost certainly forced to resign.
High	Temporary national/local brand damage lasting up to two years from coverage in national and/or regional press/media. Members/Officers potentially forced to resign.
Moderate	Temporary local brand damage lasting up to one year from extensive coverage in regional press/ media.
Low	Temporary local brand damage lasting up to a few weeks from minor adverse comments in regional press/social media.
Extremely Low	Negligible local brand damage from limited adverse comments with minimal press/social media.

Each risk is assessed for the potential range of capital and/or revenue loss to the Council if the risk materialised, as shown in Table A5.

Table A5 – Financial impact assessment

Band 8	Loss over £20 million
Band 7	Loss between £10 million and £20 million
Band 6	Loss between £5 million and £10 million
Band 5	Loss between £3 million and £5 million
Band 4	Loss between £1 million and £3 million
Band 3	Loss between £100,000 and £1 million
Band 2	Loss between £50,000 and £100,000
Band 1	Loss under £50,000
Band 0	No financial loss

The information from these assessments is recorded in APEX. An additional classification of risks is also included in APEX to enable analysis and reporting as required.

Appendix B – Glossary

4T's	The four management options to tolerate, treat, transfer or terminate a risk
APEX	The Council's performance management information system
BS	British Standard
Category 1 responder	Designation of corporate statutory obligations for business continuity and contingency planning under the Civil Contingencies Act 2004
CIPFA	Chartered Institute of Public Finance and Accountancy
CMT	Corporate Management Team
CRMG	Corporate Risk Management Group
DMT	Department Management Team
ERM	Enterprise risk management
Impact	The potential consequence of a risk if it occurred
ISO	International Organisation for Standardisation
Likelihood	The probability of a risk materialising
Major risk	A risk which has been assessed as 'red' or 'amber'
Operational risk	A process or resource risk
One Council	Collective and unified action by the whole Council focussed on delivering successful public service outcomes from the objectives stated in the Council and service delivery plans
Process risk	A risk which concerns the policies, procedures, practices and related vulnerabilities in delivering the Council's operational objectives
Resource risk	A risk which concerns the human, financial, physical, information and intellectual resources of the Council required to successfully deliver its strategic and operational aims and objectives
Risk	An internal or external event, issue, relationship, process or resource which presents a degree of uncertainty in delivering a desired outcome
Risk appetite	The acceptability or tolerance of a risk
Risk management	The proactive identification, assessment, acceptance and management of risks to successfully deliver the Council's vision, aims, objectives and statutory obligations
Strategic risk	An external or internal risk which could have a fundamental impact on the Council's purpose, constitution, strategic aims and objectives and ability to carry out its statutory and other major obligations
Terminate	Rejection of a risk if it is judged too high, even after management action is applied

Tolerance	The acceptability of a risk after necessary management actions are applied
Tolerate	Accept a risk with no further management action
Transfer	Passing a risk to third party, usually through a contract or insurance
Treat	Active management action to control or reduce the risk exposure to an acceptable level

Appendix 3

Outline implementation plan

Timescale	Action	Owner
Ongoing	Strategic Risk Register quarterly reviews by CMT and Audit Committee	Risk and Insurance
Ongoing	Departmental Risk Register monthly reviews by department management teams (prioritising major risks)	All Departments
Ongoing	Executive/Service Directors attend Audit Committee to discuss service delivery risk management (at least annually)	All Departments
May 2021 – ongoing	Council and committee reports requirements strengthened to include risk assessments as appropriate	
May 2021 – ongoing	Communicate with all Directors, managers and other staff	Risk and Insurance
June - July 2021	Risk management maturity baseline assessment (CIPFA/ALARM framework) – with quarterly progress updates and an independent annual review thereafter	All Departments/Risk and Insurance
July 2021	Agree Corporate Risk Management Strategy 2021-2025	Audit Committee
July 2021	Install APEX risk management module	Strategy and Policy/ICT/ InPhase
July – September 2021	DCC and ‘Our Derbyshire’ websites – update risk management information	Risk and Insurance
July – September 2021	Financial Regulations – update risk management sections as required	Risk and Insurance
July – September 2021	Procurement risk management framework developed and published for all significant procurement/commissioning	Risk and Insurance

Timescale	Action	Owner
July – October 2021	Departments identify and assess risk portfolios for all service delivery plan deliverables	All Departments
July 2021 – ongoing	Training sessions delivered to teams and Members as required	Risk and Insurance
July – November 2021	Online risk management induction and annual refresher training modules developed and published for all staff and Members	Risk and Insurance
December 2021	Q3 performance and risk reports – first reports using APEX data	Risk and Insurance
September 2021 – March 2022	Corporate Risk Register developed and published alongside Council Plan	Risk and Insurance
September 2021 – March 2022	Service delivery planning 2022-2023 – risk-based decision making about deliverables	Strategy and Policy/ All Departments
October 2021 – March 2022	All Council business continuity plans reviewed, gaps identified, and action plan produced (business continuity management specialist to be recruited to coordinate and support this work)	Emergency Planning/ All Departments
April-May 2022	Managing Executive Director’s annual report on risk management	Risk and Insurance

Appendix 4

CIPFA/ALARM risk management maturity framework

	Leadership & Management	Strategy & Policy	People	Partnership, Shared Risk & Resources Processes	Processes	Risk Handling & Assurance	Outcomes & Delivery
Level 5: Driving	Senior management uses consideration of risk to drive excellence through the business, with strong support and reward for well- managed risk-taking.	Risk management capability in policy and strategy making helps to drive organisational excellence.	All staff are empowered to be responsible for risk management. The organisation has a good record of innovation and well-managed risk-taking. Absence of a blame culture.	Clear evidence of improved partnership delivery through risk management and that key risks to the community are being effectively managed.	Management of risk and uncertainty is well-integrated with all key business processes and shown to be a key driver in business success.	Clear evidence that risks are being effectively managed throughout the organisation. Considered risk-taking part of the organisational culture.	Risk management arrangements clearly acting as a driver for change and linked to plans and planning cycles.
Level 4: Embedded & working	Risk management is championed by the CEO. The Board and senior managers challenge the	Risk handling is an inherent feature of policy and strategy making processes. Risk management	People are encouraged and supported to take managed risks through innovation.	Sound governance arrangements are established. Partners support one another's risk management	A framework of risk management processes in place and used to support service delivery.	Evidence that risk management is being effective and useful for the organisation and producing clear benefits.	Very clear evidence of very significantly improved delivery of all relevant outcomes and showing positive

	risks to the organisation and understand their risk appetite. Management leads risk management by example.	system is benchmarked and best practices identified and shared across the organisation.	Regular training and clear communication of risk is in place.	capability and capacity.	Robust business continuity management system in place.	Evidence of innovative risk-taking.	and sustained improvement.
Level 3: Working	Senior managers take the lead to apply risk management thoroughly across the organisation. They own and manage a register of key strategic risks and set the risk appetite.	Risk management principles are reflected in the organisation's strategies and policies. Risk framework is reviewed, developed, refined and communicated.	A core group of people have the skills and knowledge to manage risk effectively and implement the risk management framework. Staff are aware of key risks and responsibilities.	Risk with partners and suppliers is well managed across organisational boundaries. Appropriate resources in place to manage risk.	Risk management processes used to support key business processes. Early warning indicators and lessons learned are reported. Critical services supported through continuity plans.	Clear evidence that risk management is being effective in all key areas. Capability assessed within a formal assurance framework and against best practice standards.	Clear evidence that risk management is supporting delivery of key outcomes in all relevant areas.
Level 2: Happening	Board/ Councillors and senior managers take the lead to ensure that approaches for addressing risk are being	Risk management strategy and policies drawn up, communicated	Suitable guidance is available and a training programme has been implemented to	Approaches for addressing risk with partners are being developed and implemented.	Risk management processes are being implemented and reported upon in key areas.	Some evidence that risk management is being effective. Performance monitoring and assurance	Limited evidence that risk management is being effective in, at least, the most relevant areas.

	developed and implemented.	and being acted upon. Roles and responsibilities established; key stakeholders engaged.	develop risk capability.	Appropriate tools are developed and resources for risk identified.	Service continuity arrangements are being developed in key service areas.	reporting being developed.	
Level 1: Engaging	Senior management are aware of the need to manage uncertainty and risk and have made resources available to improve.	The need for a risk strategy and risk-related policies has been identified and accepted. The risk management system may be undocumented with few formal processes present.	Key people are aware of the need to understand risk principles and increase capacity and competency in risk management techniques through appropriate training.	Key people are aware of areas of potential risk in partnerships and the need to allocate resources to manage risk.	Some stand-alone risk processes have been identified and are being developed. The need for service continuity arrangements has been identified.	No clear evidence that risk management is being effective.	No clear evidence of improved outcomes.