Appendix 3

Risk Management Strategy and Framework 2021-2026

CONTENTS

Introduction

Blackburn with Darwen Council has adopted the Institute of Risk Management's definition of a risk, '*A risk is something uncertain - it might happen or it might not. A risk matters because if it happens, it will have an impact on objectives*'.

Risk management is defined as coordinated activities to direct and control the Council with regards to risk. (ISO 31000:2018).

The purpose of this strategy is to explain our approach and outline the principles of risk management, identify the people responsible for it, and promote a culture of risk management throughout the Council. It provides a structured framework and process for embedding risk management across the organisation and defining staff roles and responsibilities. This document is aligned with the Council's Corporate Plan 2019-2023 and is one part of our risk management framework.

The Council recognises that risk management is not simply a compliance issue, but rather it is a way of viewing its operations with a significant impact on long-term viability and that effective risk management helps to demonstrate openness, integrity and accountability in all of the Council's activities.

In defining risk, the Council also recognises that risk can be the failure to take advantage of opportunities to optimise the achievement of its outcomes and priorities. The Council will therefore proactively consider positive risks (opportunities) as well as negative risks (threats).

Corporate governance is the system by which we direct and control our functions and account to and engage with the community and other stakeholders. A key aspect of corporate governance is the requirement to put into place "effective risk management systems, including sound systems of internal control". It is a key strand in the statutory Annual Governance Statement and is fundamental in supporting the Business Planning Process and the Management Accountability Framework (MAF).

This document sets out the structured approach to risk management within the Council designed to support Members and officers in ensuring the Council is able to discharge its risk management responsibilities. It provides a consistent basis for the development and implementation of risk management arrangements.

Risk Management Alignment

Risk management should be an organisation wide embedded process integrated with the strategic planning arrangements. The process provides documented registers of risks the Council faces. These registers will include strategic and operational risks and will be considered from a strategic viewpoint and at a departmental level, including project risks. The risks identified will be aligned to our corporate plan priorities and objectives, and statutory duties. Departmental risks will be aligned to business plan objectives and include links to corporate priorities. These are:

- Supporting young people and raising aspirations;
- Safeguarding and supporting the most vulnerable people;
- Reducing health inequalities and improving outcomes;
- Connected communities;
- Safe and clean environment;
- Strong economy to enable social mobility;
- Supporting our town centres and businesses; and
- Transparent and effective organisation.

Risk Management Levels

		Programme or Project risks can exist at any level and within any service and should be managed using the same risk management process as other risks.

Individual members of the Corporate Leadership Team are responsible for the Council's strategic risks and these are reviewed and updated regularly as part of the MAF process. Departmental level risks are owned by Strategic Directors, Directors or Heads of Service and are discussed and reviewed at Departmental (DMT) or Senior Leadership Team (SLT) meetings.

Most of our risks are service or operational level risks that are owned by an appropriate person, usually a manager, with specialist knowledge of the area. These are managed on a day to day basis as part of business as usual activity.

Risk Management Objectives

The Council's risk management objectives have been set to take into account of the internal and external strategic influences and the requirements detailed in this document.

The detailed objectives are set out in Appendix 1.

Risk Appetite

Risk appetite is defined as '**the amount and type of risk that an organisation is willing to take in order to meet its strategic objectives**' (Institute of Risk Management). Definitions of risk appetite levels for key strategic risk categories are set out in Appendix 1 of the corporate Risk Management Policy Statement.

The Council recognises that it must take risks in the order to achieve its objectives and deliver beneficial outcomes to its stakeholders and will take a 'risk sensible' approach. To achieve this it may accept an increased degree of risk in some cases. However, risks must be taken in a controlled manner, thus reducing the Council's exposure to a level deemed acceptable, from time to time, by the Members and by other stakeholders including auditors, regulators and inspectors.

Our approach is to minimise exposure to compliance and reputational risk, whilst accepting and encouraging an increased degree of risk in other areas in pursuit of the Council's strategic objectives. This approach is reflected in the Council's approach regarding the calculation and assessment of the residual and target risk scores as described in the Risk Analysis/Assessment section.

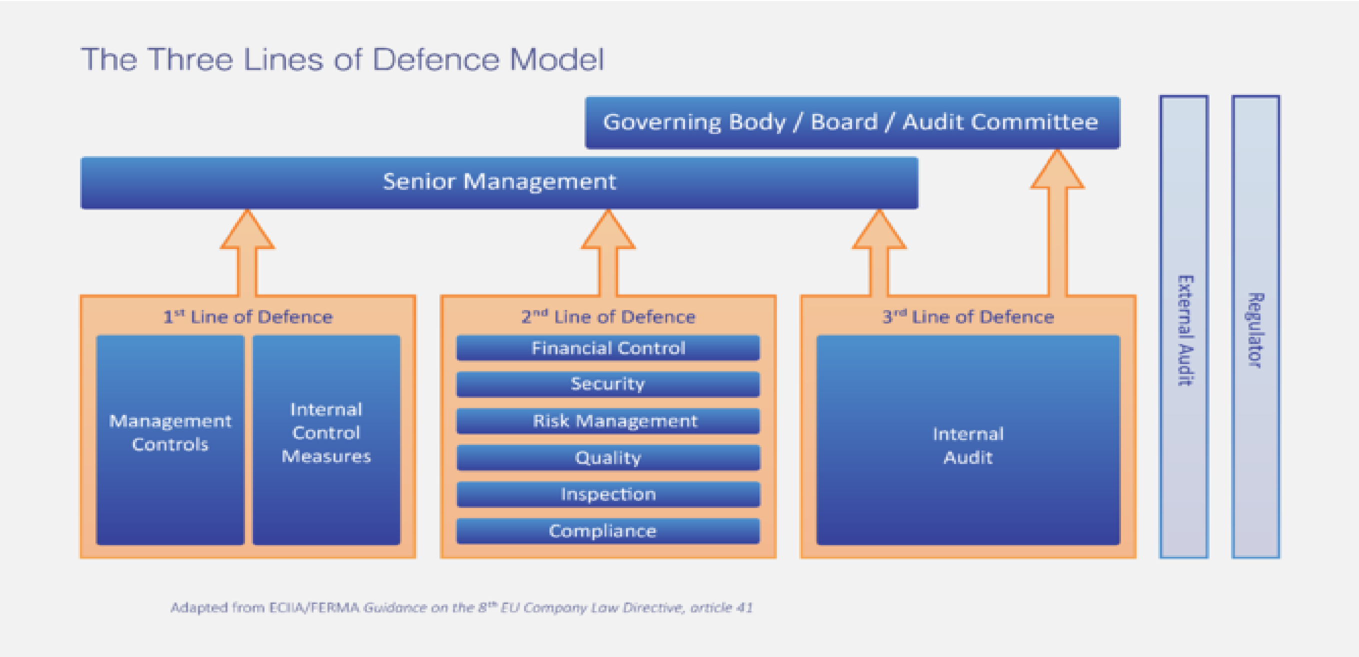
Risk appetite may vary depending on the importance and complexity of each objective that the Council is pursuing and the particular strategies in place to achieve those objectives. As a general principle, the Council will seek to control all highly probable risks that have the potential to:

- threaten the organisation's compliance with law and regulation;

- cause significant harm to service users, staff, visitors and other stakeholders;
- severely compromise the reputation of the organisation;
- have financial consequences that could endanger the organisation's viability; or
- jeopardise significantly the organisation's ability to carry out its core purpose.

Roles and Responsibilities

Everyone in an organisation has some responsibility for risk management. The "three lines of defence" model provides a simple and effective way to help delegate and coordinate risk management roles and responsibilities within and across the Council.



- **First Line of Defence** - management have responsibility and accountability for identifying, assessing and managing risks. The first line 'own' the risks, and are responsible for execution of the Council's response to those risks through executing internal controls on a day-to-day basis and for implementing corrective actions to address deficiencies.
- **Second line of Defence** - consists of functions and activities that monitor and facilitate the implementation of effective risk management practices. They also facilitate the reporting of adequate risk related information up and down the organisation. The second line supports management by bringing expertise and monitoring alongside the first line to help ensure that risk are effectively managed.
- **Third Line of Defence -** the internal audit function will, through a risk-based approach to its work, provide an objective evaluation of how effectively the organisation assesses and manages its risks, including the design and operation of the "first and second lines of defence".
- **External Assurance -** sitting outside of the Council's own risk management framework and the three lines of defence are a range of other sources of assurance that support an organisation's understanding and assessment of its management of risks and its operation of controls such as external audit, Ofsted and the CQC.

Key Risk Management Roles & Responsibilities

Political Leadership	• Ensure consideration of risk in agreeing the Council's direction of travel. • Agree, and oversee the delivery of, a Risk Management Strategy. • Review the Strategic Risk register regularly. • Work with management teams to identify new or emerging risks.
Executive Members	• Oversee risks relating to their portfolio. • Consider risk as an integral part of strategic planning and decision making.
Overview & Scrutiny Committees	• Challenge decisions made by Executive Members where risks have not been considered properly. • Task & finish groups can request risk report information for areas in line with their portfolios.
Audit & Governance Committee	• Consider the arrangements for corporate governance and risk management and advice on any action necessary to ensure compliance. • Understand the role and activities of the Corporate Leadership Team in relation to managing risk. • Approve and monitor a risk based audit programme.
Corporate Leadership Team	• Set the tone from the top and promote the benefits of risk management. • Regularly discuss and review the Strategic Risk Register and associated reports • Work with management teams to identify new or emerging strategic risks • Ensure full compliance with all corporate governance requirements, including the production of the Annual Governance Statement
Director of Finance	• Overall leadership for the effective delivery of the Council's risk management function including the Strategic Risk Register and Strategy in accordance with best practice. • Report progress with risk management to the Audit & Governance Committee.

Strategic Directors and Directors

- Ensure there are effective risk management arrangements in their departments in line with the Risk Management Policy and Strategy.
- Take ownership for risks within their departments and ensure risk registers, risk assessments including project and partnership registers, are regularly discussed, reviewed, updated and escalated as appropriate.
- Identify cross cutting risks which impact on the achievement of directorate objectives.
- Ensure Department risk registers and mitigating actions are regularly reported to the relevant Executive Member.
- Ensure key decision reports contain balanced and considered risk.
- Risk implications of all new business change proposals are satisfactorily taken into account.
- Where key services are to be provided through a partnership arrangement clear lines of risk ownership and accountability are established.

Department Management Teams

- Ensure that risk management within their area of responsibility is implemented in line with the Council's Risk Management Strategy and Framework
- Take ownership for the risks within their department, ensuring the risk register is regularly discussed, reviewed and updated and identifying analysing, prioritising and managing risk within the department as part of the business planning process.
- Ensure that all risks are aligned to corporate objectives.
- Escalate risks up to the strategic level when required.
- Ensure mitigating actions are carried out and controls are in place to

Audit & Assurance

- Periodically assess the robustness of the Council's Risk Management Policy, Strategy and Framework and culture.
- Ensure the design and systematic implementation of policies, procedures and practices for risk identification, assessment, treatment, monitoring and reporting.
- Plan audit work to take into account key risks, and how effectively they are managed providing assurances for the Annual Governance Statement, the Strategic Risk Register and Audit & Governance Committee.
- Co-ordinate the preparation of the Annual Governance Statement on

All staff	• Manage risk as part of their role and report risks to their managers. • Develop understanding and become familiar with the Risk Management Policy and supporting Strategy & Framework. • Maintain awareness of risks, their impact, including costs, and feed these through the adopted risk management process including alerting management to: - Risks which are not effectively managed, or the level of current risk is unacceptably high (amber or above). - Issues that arise or near misses.

<u>Risk Management Cycle</u>

The risk management process is a continuous cycle. It involves identifying the risks, prioritising them, and implementing actions to mitigate the top risks as illustrated by linkages in the diagram below.

The methodology adopted by the Council is a structured, systematic methodology that identifies, evaluates, prioritises and manages risk at a corporate, strategic departmental and operational level.

The Risk management process adopted at the Council is broadly based on the International Standard in Risk Management - ‘ISO 31000’.

The five-step process should take place regularly to identify new risks. The whole process along with the activities of communicating, consulting, embedding and reviewing should take place continuously to encourage the risk management process into the culture at the Council.

An especially relevant time for considering new risks is at the business planning phase, as risks should be identified which could impact on the ability to meet the objectives set out in the plan.

Additional risks may also be formally documented and assessed where appropriate, for example in respect of major projects and partnership arrangements. Guidance regarding the categories and examples of risks to consider is included in the Risk Management Toolkit

A consistent approach will be taken to assessing risks, examining for each risk identified a scenario involving a background, risk (problem) and consequence. Risk scenarios also illustrate the possible consequences of the risk if it occurs so that its full impact can be assessed.

Risk Monitoring

Risk management is an on-going process and requires regular review and monitoring. This process will examine:

- the implementation of agreed actions;
- the effectiveness of the controls that have been put in place;
- how the risk has changed over time.

Where changes have occurred the cycle will be revisited taking into account the changes and their impact on the service. The effectiveness of any control action will be judged on the basis of its success in either reducing the frequency and/or the severity of an incident.

Risk Records

The Council will maintain a strategic risk register, a community risk register (prepared by the Civil Contingencies Team to satisfy the requirements of the Civil Contingencies Act 2004) and a range of other registers for Departments, programmes, projects and partnerships where considered necessary. In addition, departments will maintain a business impact assessment for their services business continuity plans and ensure that the risk impact on critical services and functions is identified, assessed and appropriately recorded in relevant risk registers.

Risk Analysis/Assessment

For every decision or activity there is an associated risk that delivery will not take place.

We determine an inherent and a residual risk score by assessing the likelihood and potential impact of each strategic and departmental risk using the standard scoring matrix set out in the Risk Management Toolkit. The results will be recorded in the relevant risk register.

There are two components to the risk assessment: Likelihood and Impact. Example descriptors for assessing the likelihood and impact scores for risks and opportunities are set out in the Toolkit

The complete risk management assessment calculates inherent (or gross) risk and residual risk. These are calculated as follows:

Total risk score = Likelihood score x Impact score

For each scenario the two risk scores will be calculated and documented:

Gross/Inherent Risk

An assessment of the likelihood and impact of the risk scenario occurring if no controls were in place regarding the activity. This score serves as a baseline measurement of the severity of the specific **risk** facing the Council due to a particular threat.

Current/Residual Risk

To offset the inherent risk identified the Council applies controls to reduce it. Residual risk is the perception of the current situation. It is an assessment of the likelihood and impact of the risk identified today, with the current mitigating controls in place after evaluating the adequacy and effectiveness of the existing controls or measures identified. These controls **must already exist and be operating** to control or mitigate the risk identified. They **must not be planned or in progress.**

The difference between the inherent and residual scores represents the effect of the controls in place and demonstrates their value. It acts as evidence when considering if all the controls identified are required. It may be identified where risks are over controlled and resources can be freed up.

A **Target Score** will then be calculated and recorded for each risk.

This is the level of risk that is aimed for when taking into account the risk actions that have been identified and the Council's risk appetite in respect of the area/activity concerned. This should be realistic and recognise that it is difficult to be able to reduce both the likelihood and impact scores. If this is the same as the residual risk score no further action is required and the risk can be accepted. If the risk is not at an acceptable level further actions should be identified to reduce the risk to the target score.

Risk Matrix

A risk matrix is a key tool used to analyse the probability and impact of a risk. The Council uses a 5X5 risk matrix, with the score determined by multiplying the 'probability' score with the 'impact' score.

Scoring risks allows them to be compared with other risks and enables risk owners to prioritise and allocate more resources to those risks posing the greatest threat to the organisation's objectives. Once completed the risk profile will clearly illustrate the priority of each risk scenario. The categories available are green (low risk, residual score 1-5), amber (medium risk, residual score 8-12) or red (high risk, residual score 15-25).

		IMPACT				
		Marginal/Negligible 1	**Minor 2**	**Moderate 3**	**Major 4**	**Catastrophic 5**
LIKELIHOOD	**Almost Certain 5**	5	10	15	20	25
	Likely 4	4	8	12	16	20
	Possible 3	3	6	9	12	15
	Unlikely 2	2	4	6	8	10
	Very Unlikely 1	1	2	3	4	5

Each risk is then categorised as green (low risk, residual score 1-5), amber (medium risk, residual score 8-12) or red (high risk, residual score 15-25). A target risk score is also identified. This is the level of risk we are aiming for when any actions identified are completed.

Green risks sit within our level of risk tolerance, amber risks sit above our level of risk tolerance but remain within an acceptable level and red risks sit above our acceptable level.

If the residual risk score is considered too high actions are required to change the way we manage the likelihood or impact of the risk. There are four options:

- **Treat** – introduce additional suitable and proportionate controls or actions to reduce the likelihood or impact of the risk to an acceptable level, or establish a contingency to be enacted if the risk materialises;
- **Tolerate** – take an informed decision to accept the consequence and likelihood of the risk accepting the existing level of risk identified, subject to regular monitoring arrangements by management. Actions may not be able to be implemented due to disproportionate cost compared to the benefit obtained, or it is out of the Council's control;
- **Terminate** – an informed decision to not become involved in a risk situation, stop the activity that gives rise to the risk or carry out the activity in a different way to ensure that controls can be implemented; or

- **Transfer** – Pass the risk to a third party who shares or bears the impact if the risk materialises, through contracts, insurance or other means.

The higher the value of residual risk score the higher the priority for action becomes. Risk values can be grouped to determine whether action is required and with what level of priority.

The potential for controlling or modifying the risks identified will be addressed and recorded on the risk register as actions to implement.

These risk registers should not be seen as a separate initiative but be incorporated into the corporate and service planning and decision making framework.

Risk Financing

This is an important element when considering the reduction of the Council's total cost of risk. The financing may take a combination of one or more of the following:

- Payment of premiums to an external insurer.
- Acceptance of deductibles or excesses for individual risks or specific insurance policies.
- Creation of internal Reserves to handle claims rather than the payment of premiums to external insurers.
- Provision of funding for specific projects or issues raised at the Corporate Risk & Resilience Forum.
- Funding from departmental budgets.
- Transfer of risk to a third-party (e.g. by use of the Private Finance Initiative or Public Private Partnerships).

The Director of Finance and the Council's Principal Insurance Officer will provide advice where there are any financial implications affecting existing or additional insurance cover.

The Risk Management Toolkit, available on the Council's intranet, will assist with the various stages of the risk management process.

Further Information

Any comments or feedback in respect of this document or our risk management process are always welcome and can be addressed to:

Colin Ferguson Head of Audit & Assurance Finance Department 4th Floor Old Town Hall Email: colin.ferguson@blackburn.gov.uk Telephone: 01254 585326	**Andrew Tordoff** Principal Internal Auditor Risk/ Governance & IT Finance Department 4th Floor Old Town Hall Email: andrew.tordoff@blackburn.gov.uk Telephone: 01254 58 5526

Appendix 1

Detailed Risk Management Objectives

1. *Embed risk management into the culture of the Council so that it is an integral part of the Council's management systems and processes.*

This will be achieved by:

- Integrating risk management into the Council's business planning and project management processes to monitor the risk to the achievement of objectives, delivery of services or projects, determine which risks have the most significant impact and prioritise resources accordingly.
- Risk management being integral to the decisions made by the Council, its Executive Board, Executive Members and Chief Officers. (Risk management guidance for decision makers and report writers is included at appendices 4 and 5 of the Risk Management Toolkit.)
- Providing specialist advice to the Executive and Corporate Leadership Team on policies, procedures and implications of strategic and operational risk decisions so that the Council can demonstrate control of risk and can protect and manage risks to employees and members of the public, Council reputation and financial values.
- Incorporating the risk management process into the way the Council works with its partners.

How this will be demonstrated/Measures of success:

- The Risk Management Strategy and Framework will be communicational across the Council. Ensuring that risks to the achievement of all business priorities and projects are identified and recorded within business/project plans and associated risk registers.
- The risk management training programme will relevant staff are aware of their roles and responsibilities relating to risk management.
- Key issues and risks associated with all key Council decisions must be clearly identified and recorded on the corporate decision making forms. (See appendices 4 and 5 of the Risk Management Toolkit for further guidance)
- The Director of Finance and Strategic Head of Service (Legal & Governance) being consulted on all policy decisions.
- The corporate Partnership Governance Checklist and Protocols ensure a successful approach to the joint management of risks for significant partnerships.

2. *Maintain systems and processes to manage risk and contribute to good corporate governance through accurate, relevant and timely reporting on risk management.*

This will be achieved by:

- Maintaining guidance to explain to Members, employees and partners the process for managing and reporting risk within the Council.
- Maintaining a hierarchy of risk registers, which are regularly reviewed and monitored.
- Maintaining and testing corporate and departmental business continuity plans.
- The strategic risks and associated control measures being monitored, reported and reviewed by the Audit & Governance Committee (those charged with Corporate Governance).
- Sharing departmental risk registers with relevant Executive Members and the Audit & Governance Committee.

How this will be demonstrated/Measures of success:

- Regular reviewing and communication of the Risk Management Toolkit.
- Quarterly review of the strategic risk by the Corporate Leadership Team and departmental risk registers by Strategic Directors and Directors. Risk registers reviewed at each Partnership and Project Board meeting.
- Progress on the management of risk, particularly strategic risks reported quarterly to the Council's Corporate Leadership Team and Audit & Governance Committee.
- Regular review and challenge of strategic risks by the Audit & Governance Committee.
- Use of the risk management support available from the Council's insurance brokers and insurance provider to provide advice and support on the risk management arrangements in place within the Council, including independent assurance on specific risk areas.

3. *Maintaining clear roles and responsibilities regarding risk management, including business continuity management.*

This will be achieved by:

- Clearly identifying responsibility for overseeing risk management in the Council.
- Clearly identifying officer roles, responsibilities and reporting lines for managing risk, including business continuity management.
- Establishing a risk management structure to act in an advisory and guiding capacity that is accessible to all employees.
- Aligning leadership and monitoring of strategic risks to the responsibility for achieving objectives; assessing threat and opportunity risks;
- Developing and implementing controls/warning mechanisms and reviewing/reporting on progress.

How this will be demonstrated/Measures of success:

- The Council's Constitution outlines the Audit & Governance Committee's oversight of risk management.
- Reviewing and updating the roles and responsibilities section of the Risk Management Strategy & Framework.
- Maintain up to date terms of reference for groups that support the risk management process e.g. Road Risk Management Group, Events, Health & Safety Action Group, Events Safety Advisory Group etc.
- Designating Directors as risk owners for relevant strategic risks and for maintaining risk registers affecting their operational responsibilities including key projects/partnerships.

4. *Develop and disseminate best practice in the management of risk.*

This will be achieved by:

- Independent assurance is provided to the Council on the effectiveness of the risk management framework.
- Risk management is a key contributor to corporate governance with Directors responsible for encouraging good risk management practice and having systems for identifying, monitoring and managing strategic and departmental risks.

- Ensuring that internal audit coverage is driven by a deep understanding of the risks, challenges and opportunities facing the Council.
- Improved co-ordination of risk management activity throughout the Council, reducing duplication and enhancing consistency between departments in managing overlapping risks.

How this will be demonstrated/Measures of success

- Regular review of the Risk Management Framework and supporting processes and procedure to ensure that these reflect current best practice.
- The Audit & Governance Committee approves an annual risk management report providing an independent opinion on the effectiveness of the Council risk management arrangements.
- Directors annually declare that they have effective risk management systems in place, which are summarised in the Council's Annual Governance Statement.
- Audit & Assurance delivers a risk based internal audit programme.
- Audit & Assurance providing support to departments, reviewing the consistency of risk registers and undertaking independent reviews of the risk management process.

5. ***Equip Members and officers with adequate skills and expertise to manage risk effectively as appropriate to their role.***

This will be achieved by:

- Delivery of general and specialist risk training for Members and officers.
- Providing advice, guidance, suitable information and training on risk management.
- Providing opportunities for shared learning on risk management across the Council and with other authorities, partners and stakeholders are taken where appropriate.

How this will be demonstrated/Measures of success

- Utilisation of the risk management support/fund on tailored training for Executive Members, Audit & Governance Committee and Extended Leadership Team.
- eLearning training package for staff
- Provision of up to date guidance in the form of Risk Management Toolkit.
- Risk management updates are shared at appropriate internal and external forums.