

RISK MANAGEMENT FRAMEWORK AND POLICY STATEMENT

March 2024



CONTENTS

	Page
Statement of Commitment / Policy	3
Risk Management Framework	4
Introduction	4
Definition of Risk	4
Diagram 1 - Risk Management and Associated Areas.	5
Risk Appetite	6
Hierarchy of Risk within Wirral	7
Table 1 - Levels of Risk Register	7-8
Diagram 2 – Risk relationships and Reporting Lines.	9
Keys Roles and Expectations	9
Table 2 - Key Groups and their Responsibilities	10
Risk Management Process	11
Diagram 3 - Risk Management Process Cycle	11
Establishing the Context	12
Risk Identification	12
Risk Evaluation and Determining if Risk Level is Acceptable	13
Table 3 - Managed Risk Rating and Measures to be Taken.	13
Escalation of Risks	14
Reporting of Risks	15
Monitoring of Risks	16
Programme and Project Management	16
Training	16
Governance	17

STATEMENT OF COMMITMENT / POLICY

We accept that uncertainty and risk are inevitable features of the environment in which the Council operates within.

However, we appreciate that uncertainty also presents opportunities and that we must innovate if the Council is to meet the challenges that it faces. We believe that risk management should not stifle innovation, but rather should support the taking of risks, provided that they are understood, actively managed, and justified.

We also recognise that the pace and complexity of the environment in which the Council operates could create combinations of events that cannot reasonably be envisaged making it important to maintain agility and organisational resilience.

The Council's focus is on being a risk aware organisation, in which risk management is fully embedded in all aspects of the Council's business, and risks are identified, understood, and well managed.

We will achieve this by:

- Maintaining clear roles, responsibilities, and reporting lines, within the Council and the wider partnership environment, for risk management;
- Encouraging maturity and candour in discussions between officers and members about the uncertainties associated with the delivery of our Council Plan objectives;
- Embedding risk management into the Council's decision making and operational management processes;
- Integrating risk management considerations into all elements of strategy, business and financial planning, commissioning and procurement processes, programme and project management, partnership working and reporting;
- Underlining the importance and requirement for the effective management of risk through training and awareness in related fields;
- Monitoring our risk management arrangements, and their effectiveness, on a regular basis.

RISK MANAGEMENT FRAMEWORK

INTRODUCTION

The Council is often faced with difficult decisions, but also opportunities to define an exciting and ambitious future. The Council Plan 2023 – 2027 sets out the vision for the borough in the years ahead and includes the new Enabling Theme: efficient, effective, and accessible council.

Effective governance arrangements are essential to help us achieve that vision and risk management is a key element of those arrangements. The Council's understanding of the risks faced and how well managed and monitored they are will have an impact on its ability to deliver the Council Plan. This framework, and associated appendices, lays out the arrangements, structures, and methodology in support of the Enabling Theme.

The framework is approved by the Strategic Leadership Team (SLT) and considered by the Audit and Risk Management Committee (A&RMC), on behalf of the Council. The framework is subject to a biennial review.

DEFINITION OF RISK

At its simplest **Risk** can be defined as 'the effect of uncertainty on objectives' (ISO 31000:2018, clause 3.1).

Within HM Government's The Orange Book – Management of Risk, Principles and Concepts (2020) this idea is expanded on.

"Risk is usually expressed in terms of causes, potential events, and their consequences:

- A cause is an element which alone or in combination has the potential to give rise to risk;
- An event is an occurrence or change of a set of circumstances and can be something that is expected which does not happen or something that is not expected which does happen. Events can have multiple causes and consequences and can affect multiple objectives;
- the consequences should the event happen - consequences are the outcome of an event affecting objectives, which can be certain or uncertain, can have positive or negative direct or indirect effects on objectives, can be expressed qualitatively or quantitatively, and can escalate through cascading and cumulative effects."

Risk management is an essential part of governance and leadership, and fundamental to how an organisation is directed, managed, and controlled at all levels. The identification, assessment and treatment of risks is subjective and requires all views to be considered. The application of an organisational risk appetite is necessary for a risk management framework to be effective in supporting any organisations priorities.

“Risk should be considered regularly as part of the normal flow of management information about the organisation’s activities and in significant decisions on strategy, major new projects and other prioritisation and resource allocation commitments.”

(The Orange Book – Section A - Paragraph A5)

A glossary of risk management terms can be found at Appendix 8.

Risk management features, or is linked, to many areas across the Council. It is a key tool to support decision making, helping the Council consider whether:

- Intended benefits justify the range of outcomes
- The plausible outcomes are within the current appetite
- Available resources can be reallocated, if necessary, to allow benefits to be realised within the stated appetite

The diagram below highlights the many areas where risk management is an integral part of strategies, policies, and processes.



Diagram 1. Risk Management and Associated Areas.

RISK APPETITE

Risk appetite is defined by Institute of Risk Management (IRM) as “the amount and type of risk that an organisation is willing to take in order to meet their strategic objectives.”

Everyone’s attitude to risk differs depending on knowledge, expertise, and experiences both professional and personal. In addition, risk appetite naturally differs in different areas and levels across the Council. It is important to consider:

- The level of risk the Council **should be willing** to accept in the pursuit of its objectives.
- The level of exposure to different risks the Council is **currently carrying**.

By understanding, articulating, and evidencing the Council’ risk appetite, tolerance of risk and the general environment it operates in helps to:

- Ensure the Council is only taking a level of risk, and the type of risks, it is comfortable with to achieve its goals.
- Ensure the risks are commensurate to the opportunity, benefits, or reward to be gained.
- Provide a framework for decision making; significant decisions can be taken with consideration to how it will affect the level or risk the Council is exposed to, and if this is acceptable or not.
- Enable staff to make judgements about which risks are acceptable in pursuing goals and which are not.
- Ensure the response to specific risks is proportionate.

For more information on the Council’s risk appetite, refer to Appendix 1.

It is recognised that the Council’s plans and objectives have to be delivered within a complex and increasingly dynamic environment. The interplay of social, political, economic, and technological change creates uncertainty which poses threats to the delivery of the Council’s vision, but also presents us with opportunities. Effective risk management will help ensure that we are resilient and able to withstand threats that emerge and exploit opportunities for improvement.

It is not possible to have a single risk appetite spanning the whole Council due to the scale and wide range of services delivered. The vision within the Council Plan and behaviours and values set by the Strategic Leadership Team help to provide a risk embracing and aware culture.

A fundamental part of setting the risk appetite is to provide a scoring matrix with definitions and agreed grading using a Red, Amber, Green (RAG) rating levels. All risks recorded onto the risk register template are assessed against these scoring definitions and mapped against the RAG rating.

More information on the scoring process and scoring definitions can be found in on page 13 and in Appendix 2.

LEVELS OF RISK WITHIN WIRRAL COUNCIL

There are several distinct levels of risk register across the Council with risks flowing between them. To help ensure that risk information is captured in a consistent format, a standard risk register template is to be used for all business planning, strategy, and decision-making risk registers. A separate template is used for hazard risk assessment for health and safety purposes. Use of a standardised template allows for the escalation or demotion of risks more easily, with relevant and consistent information able to be shared between the various levels. It also allows for use of the PowerBI tool for reporting. The template is available at Appendix 3.

Table 1 below details the levels and gives a brief explanation of their contents and management, including the expected frequency of review.

Level of Risk Register (RR)	Owner, contents, and links to other levels
Corporate Risk Register (CRR)	<p>The risks within the CRR are the responsibility of the Strategic Leadership Team. The maintenance of the CRR is supported by the Risk, Continuity & Compliance Manager.</p> <p>It is reviewed on a quarterly basis.</p>
Directorate Risk Register (DRR)	<p>The DRR is owned by each Director and Directorate Management Team. It can be a mixture of strategic and operational risks with the potential to affect the delivery of the objectives and priorities within the Directorate Business Plan. Risks which may be devolved from the CRR or escalated from Service, Programme or Specialist Risk Registers.</p> <p>DRRs are reviewed on a regular by the respective Policy and Service Committee.</p> <p>Must be reviewed on at least a quarterly basis, aligned with performance reporting.</p>
Service or Team Risk Register	<p>The RR is owned by an Assistant Director/Senior Manager and Management Team. Focussed on the operational risks with the potential to affect the delivery of the objectives and priorities within a Service or Team Plan. Risks which may be devolved from the DRR or escalated from Programme/Project or Specialist Risk Registers.</p> <p>Must be reviewed on at least a quarterly basis, aligned with performance reporting.</p>

Level of Risk Register (RR)	Owner, contents, and links to other levels
Specialist Subject Areas / Delivery of Key Strategies	<p>There are a number of specialist subjects which operate on a cross service basis, focussed on the management of risks across the Council. For example Health and Safety, Information Management and Cyber Security, and Fraud. In addition, there are some key strategies which also maintain a risk register focussed on the risks to the delivery of the strategy e.g. Treasury Management, Asset Management.</p> <p>Must be reviewed on at least a quarterly basis, aligned with performance reporting.</p>
Programme Risk Register	<p>The RR is the responsibility of the relevant Programme Board and Senior Responsible Officer (SRO) and are maintained by the Programme Manager. Contain risks that have the potential to impact on the delivery of the Programme objectives, may include risks escalated from the supporting projects.</p> <p>Must be reviewed on at least a monthly basis.</p>
Project Risk Register	<p>These risk registers are the responsibility of the Project Sponsor and will be maintained by the Project Manager.</p> <p>The frequency of review is to be determined by the speed of project delivery and timescales, a minimum of monthly.</p>

Table 1. Level of Risk Register, Owners, and Review Requirements.

Further detail on the escalation of risk is available within the risk management cycle and process later in this framework.

Diagram 2 highlights the movement of risks and key reporting lines. Black arrows denote the movement of risks; up, down, and between the risk registers. Coloured arrows denote reporting routes.

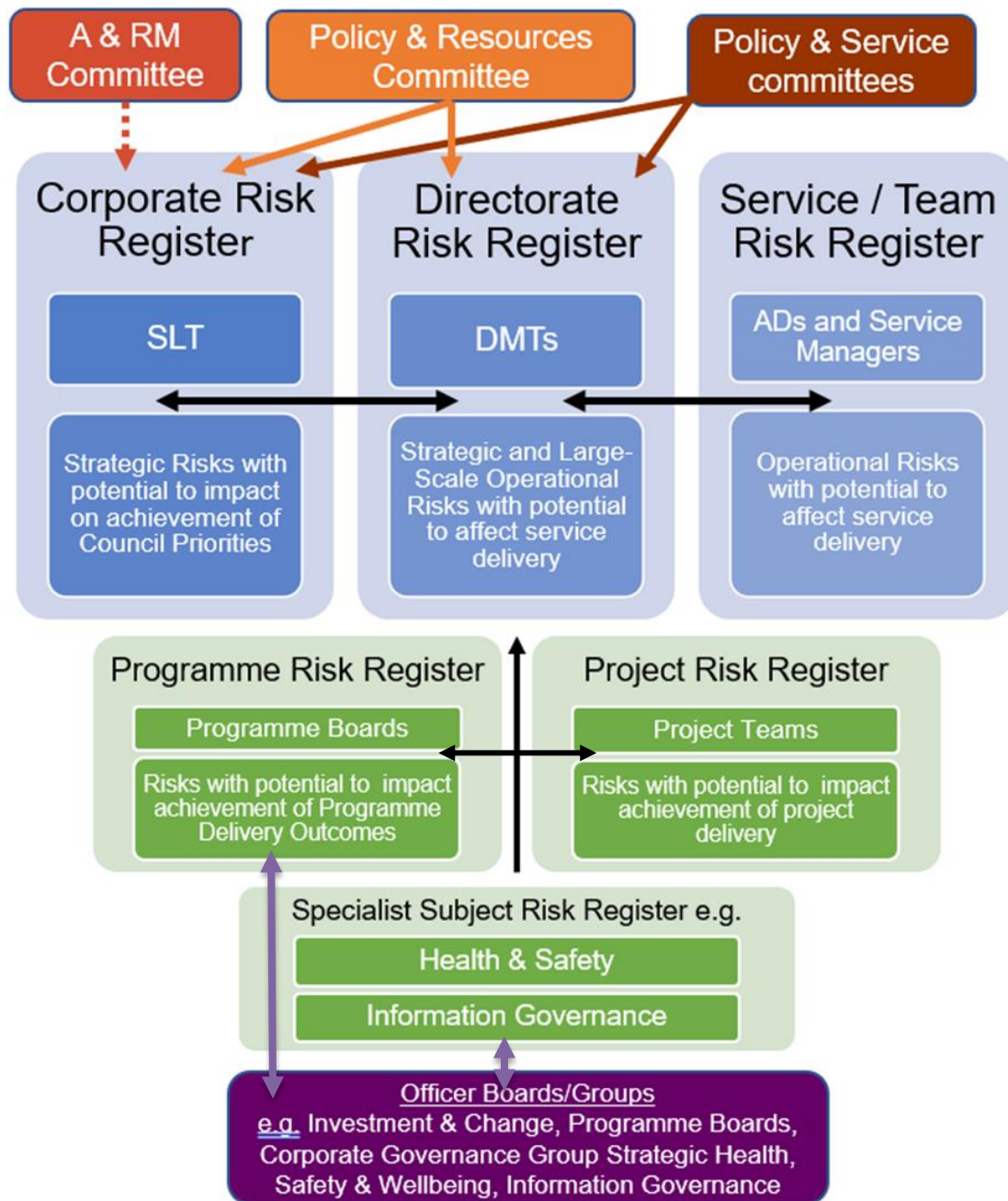


Diagram 2 - Risk relationships and reporting lines.

KEY ROLES AND EXPECTATIONS

A key part of the governance arrangements for risk management is the defining of roles and responsibilities, or the expectation placed on groups for the effective use and delivery of robust risk management.

Table 2 below highlights the key groups and their key responsibilities in relation to the delivery of risk management and this framework.

P&R and Policy & Service Committees	<ul style="list-style-type: none"> • As per the current Terms of Reference in the Constitution • Providing a view of performance, budget monitoring and risk management in relation to the Committee's functions
Strategic Leadership Team (SLT)	<ul style="list-style-type: none"> • Set the tone from the top • Maintains an overview of the Council's risk profile and appetite • Regularly discuss and review the Corporate Risk Register - identify new corporate risks and any for escalation/demotion to DRR level
Audit & RM Committee	<ul style="list-style-type: none"> • As per the current Terms of Reference in the Constitution • Consider the effectiveness of the system of risk management arrangements.
Director / DMTs	<ul style="list-style-type: none"> • Take ownership for the regular monitor and management of their Directorate Risks • Escalating and risks to the CRR as required. • Engage and support the role of the Directorate Risk Co-ordinators • Reporting risk, alongside performance and budget monitoring to Members
Officer Boards / Groups	<ul style="list-style-type: none"> • E.g. Operational Performance Group/Corporate Governance Group / Investment & Change Board • Follow the 3 Pillars approach - monitor and escalate risks • Include the monitoring and reporting of risks within responsibilities
Managers at all Levels	<ul style="list-style-type: none"> • Escalate risks up to the appropriate level, as required. • Take ownership for risks within their area and ensure robust risk management is undertaken for all risk types including operational risks
Programme & Project Managers	<ul style="list-style-type: none"> • Identify and monitor risks with the potential to impact on a project or programme • Escalate risks, as required, to the appropriate level.
Directorate Risk Co-ordinators	<ul style="list-style-type: none"> • Facilitate the regular review of the Directorate Risk Register • Provide support to DMTs
Internal Audit	<ul style="list-style-type: none"> • Undertake a risk based audit plan each year to monitor the effectiveness of the internal controls and operating environment
All Employees	<ul style="list-style-type: none"> • Manage risk as part of their role and report risks to their managers • Develop their understanding of all types of risk, including operational e.g. H&S, and the Council's approach to risk management through training, awareness and peer support

Table 2. Key groups and their responsibilities relating to risk management.

THE RISK MANAGEMENT PROCESS

The risk management process is intended to ensure that the key risks to achieving our objectives are identified and managed. Too little awareness and management of these key risks can adversely affect our performance. But attempting to mitigate all possible risk could divert too many resources away from other key services. Between these two extremes is a balancing point, an area of high performance through the sensible management of risk. This is the position the Council aims to achieve through implementation of its Risk Management Framework and consideration of the risk appetite.

Diagram 3 shows the key stages of the process, more information on the individual stages or supporting information can be found in the appendices. This is a continuous process and which is repeated for the lifetime of the risk register.



Diagram 3: The Risk Management Process Cycle and Key Stages

By following this straightforward process Officers and Members will understand and be able to monitor risks that could affect the achievement of their objectives and the adequacy and effectiveness of existing controls. It also provides the basis for decisions about the most appropriate approach to be used to tackle risks.

The process should be applied to all key business processes, including:

- Setting strategic and service objectives and priorities
- Creating business cases for programmes and projects
- Procuring and/or commissioning services or goods
- Setting of short- and medium-term budgets
- Establishing or refreshing policies and strategies

The risk management process cannot be effective without an appropriate level of communication between all stakeholders. This requires engagement with all those who have an interest in the potential risks to the objectives, at whatever level is being assessed. This may include management teams, partners, programme and project boards, and any specialists, whose assistance may be beneficial when identifying and evaluating risks.

Risk assessment is subjective and requires input from a group with mixed subject knowledge, experience, and risk appetites to ensure a balanced approach to the identification and management of risks.

ESTABLISHING THE CONTEXT

When first considering risks, at any level, it is vital to define the basic parameters for managing risk and sets the scope and criteria for the rest of the process. Without this first stage the process, and risks identified to be managed can quickly become unwieldy and overwhelming. This should be recorded within minutes of meetings, business cases, project documentation or on the risk register itself.

Consideration should be given to:

- The external and internal operating environment;
- What we are looking at, strategic or service objectives, programme/project or partnership objectives, budgets or policies, procurement or commissioning, options for decisions;
- Who will be involved, be they internal or external stakeholders. They should all be considered as they may have an interest in or a valuable contribution to add to the rest of the process;
- Who will be responsible for the process: define responsibilities for review, monitoring and reporting;
- The risk criteria and appetite, whether it is political, economic, legal, environmental, etc. The impact criteria to be included and how they will be measured;
- When looking at partnership risk, agree which partner's processes will be adopted and how and where joint risks will be reported.

RISK IDENTIFICATION

There are several tools available to assist in the identification and capturing of risks. Some may be used for other purposes and the logging of risks may be a byproduct which can be used to develop the risk register. For example SWOT analysis features both threats and opportunities, the two sides of risk. Use of key categories can help to trigger discussion and avoid omitting key areas of risk, PESTLE analysis looks at Political, Economic, Social, Technology, Legal and Environmental. A list of risk categories is available at Appendix 5. In addition past experience, risks identified in reports, third party information or even incidents or near misses all help to inform the risk identification at any stage and help to ensure new and emerging risks are regularly captured.

The crucial question to come back to each time is what are the risks which have the potential to have some effect on the delivery of the agreed priorities or objectives? These risks should be the focus of the risk register. This helps to prevent scope creep and avoid the risk register becoming too large or overwhelming and therefore unmanageable.

Risks must be documented on the risk register in two parts, the possible cause and its potential consequence or impact. This will help with the scoring and ongoing management of the risks. Clarity in the risk description also assists with reporting and escalation of the risks. For more information on the process of risk identification and description refer to Appendix 6.

RISK EVALUATION AND DETERMINING WHETHER THE LEVEL OF RISK IS ACCEPTABLE

Once risks have been clearly articulated, agreed and logged on the template, by the risk register owners, risks are assessed using the scoring definitions and matrix (see Appendix 2).

Risks are scored three times:

- Gross or Inherent Score – where the risk would be with no controls in place, the worst-case scenario;
- Managed, Current or Residual Score – where the risk is today, with controls in place and being effective, working to reduce the chance of the risk occurring or its impact if it did;
- Target Score – the level where the risk will be accepted or tolerated, perhaps if additional actions are taken.

As part of the initial assessment and scoring, by the risk register owners, the risk appetite is considered for each risk and the “Target” score is applied to demonstrate that the risk is either being accepted, the score is the same as the Managed/Current score, or action is to be taken to further reduce the risk score. For more information on the scoring process and scoring definitions refer to Appendix 2.

Table 3 below seeks to demonstrate the key considerations or actions that are required once a risk has undergone a scoring assessment for its Managed or “Current” score.

Risk Rating	Description	Considerations / Actions Required
Red	Critical risks which have the high likelihood and potential impact to significantly affect the achievement of objectives and/or the delivery of key services.	<ul style="list-style-type: none"> • Can additional actions be put in place to reduce the risk further? • Does a lower Target score need to be set to highlight the level of risk is unacceptable? • Keep the risk and existing controls under regular review, are controls still effective? • Should the activity be stopped thereby removing the risk? • Does the risk need to be escalated to a higher level of risk register to ensure greater oversight and awareness.
Amber	Risks that have a medium to high impact but lower likelihood of affecting the delivery of objectives and/or the delivery of key services.	<ul style="list-style-type: none"> • Can the risk be tolerated, if well monitored? • Will the Target score be kept the same as the Managed/Current score? • Will additional actions have enough of an effect on the risk to warrant the resources being committed? • Is the risk worsening, perhaps due to an increase in its likelihood?
Green	Minor risks that are considered to be low or medium in impact and/or with a low likelihood of occurring. This maybe because they are being well controlled.	<ul style="list-style-type: none"> • Maintain existing controls but continue to monitor effectiveness and any external factors which may disrupt them. • Additional control actions are unlikely to be needed. • Will the Target score be kept the same as the Managed/Current score? • Is the risk being over managed and could controls be removed, to release resources, without significant detriment to the risk?

Table 3. Managed Risk Rating and Measures to be Taken.

ESCALATION OF RISKS

Linked to the determination of whether risks are acceptable is the need to escalate risks to a higher level; for awareness, to request for resources or support, and/or to request that the activity is halted.

The need to escalate a risk is not constrained by a certain level of score. This allows risks that are deteriorating or where the context operated in is known to be changing to be escalated before they reach a “red” rating. This will allow for remedial measures to be considered in a timely fashion.

Corporate Risk Register

The escalation of risks to the Corporate Risk Register is considered by the Strategic Leadership Team at each quarterly review. Risks can be put forward by Directors or fed through the Risk, Continuity and Compliance Manager. Risks may be put forward for consideration due to a number of reasons, for example:

- A risk may require cross directorate engagement and support to manage;
- The potential impact of a risk maybe felt across the Council, reputationally or financially;
- Increased monitoring is required and reporting to Members;
- Expansion or refocussing of an existing entry on the Corporate Risk Register, perhaps if external circumstances or pressures change.

In addition, consideration is given to de-escalating or demoting a risk to the next level, where the mitigating activity and management is focussed in one area allowing for ongoing review.

REPORTING OF RISKS

In addition to the escalation mechanisms for highlighting risks to the next level of risk register and responsibility there are clear requirements for the reporting of risks to the appropriate level of management.

The Corporate Risk Register is reviewed and reported to SLT on a quarterly basis. In addition it also goes to the Operational Performance Group, Corporate Governance Group and Audit and Risk Management Committee.

Directorate Risk Registers are also reviewed on a minimum frequency of quarterly, they are loaded into DMT Insights Pack using the Council’s Power BI data visualisation toolkit, supported by the Wirral Intelligence Team. This allows for increased visibility of the risks and for their inclusion and consideration with regular performance reporting arrangements. DRRs are also reviewed on a six-monthly basis, via a workshop discussion session, by the respective Policy and Service Committee as part of the committee’s responsibility for the understanding and oversight of risks.

Individual risks are also reported in committee reports when presenting decisions or updates on specific matters. There is a requirement for all committee reports to consider the risks associated with taking or not taking a decision. Key Decision reports are reviewed at the Committee Coordination and Oversight Group to ensure compliance,

before going to SLT. Other committee reports are reviewed by officers within Democratic Services, Audit and Risk, Legal, and Finance Teams through the ModGov system.

MONITORING AND REVIEWING RISKS

The regular monitoring process should provide assurance that there are appropriate controls in place for the organisation's activities and that the procedures are understood and followed. Any monitoring and review process should also determine whether:

- the measures adopted resulted in what was intended;
- the procedures adopted and information gathered for undertaking the assessment were appropriate;
- improved knowledge would have helped to reach better decisions and identify what lessons could be learnt for future assessments and management of risks.

The Corporate and Directorate Risks are reviewed on a quarterly basis. The risks and associated controls tend to be strategic in nature and therefore the effect of changes is likely to take longer to be felt and be measurable.

The frequency of the review or monitoring of the risks for projects, strategy delivery and specialist areas should be agreed, and recorded, as part of the "establishing the context" discussions by the risk register owners.

For more detailed guidance on the key questions to be asked when reviewing risk registers, refer to detailed guidance Appendix 7.

PROGRAMME AND PROJECT MANAGEMENT

Across the Council there are several areas of programme and project management. The speed of delivery, timescales for projects and complex nature, sometimes involving multiple partners, means that specialist, targeted arrangements are made within the Programme Office to manage the associated risks. This may mean some divergence from the corporate guidance, templates, or lines of reporting. However all arrangements are reviewed and agreed by the Risk, Continuity and Compliance Manager to ensure alignment with the principles of this framework.

TRAINING

Detailed guidance, and supporting information, on the risk management process can be found in the appendices. Targeted training is carried out for key roles either as standalone sessions or as part of a wider training package. This includes Members, project managers, senior officers, and report writers.

Training materials and additional information is available on the risk management pages on the intranet and in Flo, the Council's learning experience platform.

GOVERNANCE

Risk management is a key component of the Council's framework of governance and internal control.

There are several important elements to the governance and monitoring the effectiveness of risk management within the Council that includes the following:

- Annual Governance Statement (AGS)
- Internal Audit.
- External Reviews
- External Audit

Review Frequency and Responsibility		
Responsible officer: Risk, Continuity & Compliance Manager – Helen Turner	Review frequency / Next scheduled by: Every 2 years / March 2026	
Review Version History		
Date	Author/Editor	Comments
February 2024	Helen Turner	Overhaul of document to reflect change to reporting, committee, and management structures and, as well as updated guidance separated into the appendices. Appendices expanded to include framework processes and guidance.