Risk Management Framework

Welwyn Hatfield Borough Council

April 2023

WELWYN HATFIELD

1 Introduction

1.1 The purpose of the risk management framework is to define how risks and opportunities will be handled within the Council. The framework provides information on roles and responsibilities, processes and procedures.

1.2 The Council has a clear framework which defines the process for identifying, assessing, managing/ controlling, reviewing and reporting of its risks.

1.3 The Council expects all of its employees and Councillors to have a level of understanding of how risks and opportunities could affect the performance of the Council and to acknowledge the management of those risks as part of their everyday activities. This could be the management of strategic risks (those risks that need to be considered when making judgements about medium and long terms goals), operational risks that managers and staff will encounter in the daily course of their work, of project risks which contribute to successful project delivery.

1.4 The Council has a four-step process for identifying, assessing, managing and controlling and reviewing the risk (See Figure 1, section 3). This is a continuous process and integrates closely with performance management. The Council has an agreed criteria by which to judge the likelihood and impact of risks, effectiveness of control measures and required level of management of residual risks.

1.5 The risk management framework is a continuous cycle designed not only to identify, assess, manage and review risks, but also to support business objectives. The implementation of this framework will support the Council in recognising risk and minimising its impact through all areas of service provision.

2 Roles and responsibilities

2.1 The respective roles and responsibilities within the Council for the Risk Management Framework are set out below:

Council

The Council will:

- Consider risk management implications when making decisions

Cabinet

The Cabinet will:

- Approve the Council's Risk Management Policy, Strategy and Framework
- Consider risk management implications when making decisions
- Maintain oversight of the risk register and risk management issues

Audit Committee

The Audit Committee will:

- Maintain an independent oversight of the risk register and risk management issues
- Undertake reviews of specific areas of risk management activity or initiatives where required
- Oversee the work of Internal Audit. Planning for audits will be on a risk based approach and the programme will include a rolling review of risk management framework (such as the adequacy of the control framework and Health and Safety)
- Review and approve the Council's Annual Governance Statement

Executive Director (Finance and Transformation)

The Executive Director (Finance and Transformation) will:

- Be responsible for the oversight of risk management activities of the Council
- Provide the Cabinet and Audit Committee with assurance that the Councils corporate business risks are being actively and appropriately managed
- Make arrangements for the review maintenance the strategic, operational and project risk registers
- Ensure appropriate training is provided to all of those involved with risk management.

Senior Management Team (SMT)

The Senior Management Team will:

- Maintain oversight of the risk register and risk management issues
- Identify and maintain Strategic risks
- Oversee the corporate approach to risk management
- Identify, assess, and manage and oversee risks through the risk management framework
- Demonstrate commitment to the embedding or risk management across the organization
- Identify the risk managers in their services

Corporate Groups

There are a number of corporate working groups, who as part of their responsibilities will:

- Maintain oversight of the risk register and risk management issues within their remit
- Ensure risk management issues are escalated to the appropriate group or Management Team
- Monitor and influence processes and controls for risks within their remit
- Put plans in place and monitor these plans to improve risk management issues

These groups include (but are not limited to) the Corporate Governance Group, the Operational Health and Safety Board and the Safeguarding and Equalities Group.

Risk Managers

Risk Managers are employees involved in the management of risks. This would include (but is not limited to) members of SMT, Service Managers, Team Leaders, Lead Officers, project managers, will:

- Identify and assess new risks
- Maintain the Council's operational risk registers in relation to their areas of responsibility, identifying and reporting any significant risk management issues affecting their service area.
- Ensure that an effective processes and controls are in place to manage risks faced by the service.
- Updating risks on a regular basis for impact, likelihood, control measures and appropriate commentary.
- Identify initiatives that could reduce the impact and/or likelihood of risks occurring.
- Ensure that risk register entries and controls are accurate and up to date.
- Monitor the progress of planned actions on regular basis to ensure that aims are achieved.

PMO, Performance and Data Team

The PMO, Performance and Data Team will:

- Ensure that risk management records and procedures are properly maintained and that clear audit trails exist in order to ensure openness and accountability.
- Provide the Executive Director (Finance and Transformation) with progress of delivery of risk register timescales and any other risk issues as appropriate.
- Produce regular reports against the risk register for reporting to Senior Management and Members.

Insurance, Treasury and Controls Team

- Ensure the timely purchase of adequate insurance for the transfer of risk, where appropriate.
- Ensure risks identified as part of claims management are reported to management for inclusion in the risk register.

All employees

All employees, within their given areas of responsibility and work, will:

- Understand risks and regard their management as part of their everyday activities, including the identification and reporting of risks and opportunities which could affect the Council.
- Assist with risk assessments for their areas of work
- Support and participate in risk management activities.

Internal Audit

The Internal Audit team will:

- Independently assess the Council's risk management arrangements
- Review the adequacy of procedures by departments to assess, review and respond to risks
- Review the effectiveness of the Councils system of internal control
- Take a risk based approach to audit planning and consider the content of the risk registers when preparing the Annual Audit Plan

3 Risk Management Process

3.1 The Council has a four-step process for its risk management process, and all four stages are fundamental to good risk management.

3.2 Figure 1 below shows the four steps and the link to business objectives.

Figure 1: The Four Steps of the Risk Management Cycle

4 Risk Identification

What is a Risk

4.1 Risk is something that may have an impact on the achievement of our objectives.

4.2 The Council faces risks from both internal and external factors. Understanding this helps us to assess the level of influence and control we may have over the risk.

4.3 There are three main parts to a risk – an **event** that has a **consequence** that leads to an **impact** on the Council objectives – and it can be measured by estimating the likelihood of the event happening and impact it may have on the objectives if it does.

Risk Categories

4.4 It also helps to think of risk being driven by three basic categories: **Strategic**; **Operational**; and, **Project**.

4.5 At Strategic levels, the focus is on identifying the key risks to successful achievements of the Councils overall objectives as set out in its Corporate Plan and its annual Action Plan.

4.6 Operational risks are the risks that are most likely to affect the performance and delivery of business services.

4.7 Project risks are the risks that are most likely to affect the successful delivery of a project.

4.8 Risk categories are not mutually exclusive, and a risk may escalate from one to another. For example a risk which escalates to severe at project level which suggests there is a risk to project failure, may then create a risk at operational or strategic level.

4.9 When identifying the risk, both positive and negative effects need to be considered. This will help with risk taking and exploiting opportunities.

4.10 Insignificant risks can be ignored, significant risks can be planned for and the costs of taking action can be compared with the price to be paid if adverse events occur.

Risk Influencers

4.11 It can sometimes help to consider the different influencers of risk when considering the factors that may lead to a risk event occurring.

4.12 A good way to think about this is by considering the common drivers of risk. Figure 2 shows the common influences of risk.

4.13 Using these, it is important to consider the things that could prevent or hinder the council from achieving its objectives. There does not need be too much focus on the categories, or what risk fits under which category, they are just a general guide to assist risk managers in considering what may impact the council.

Figure 2: Risk Influencers – PESTLE Model

Economic These factors are linked the economy, both nationally and locally and impact directly on the costs, income generation or funding for the Council. Examples include changes in inflation, base rates and cost of living.

Political These factors are linked to the extent to which government policy may impact the organisation. For Local Authorities these apply nationally and locally. Examples include changes in political control following elections, policy decisions and council reputation.

Legal These factors are linked to the current and future regulatory requirements the council works within. Examples include statutory service requirements, new ombudsman standards, changes to legislation and compliance with the councils constitution.

Environmental These factors are linked to the influence of the surrounding environment, or the impacts on the surrounding environment. Examples include climate change, weather, pollution, trees, and natural disasters.

Technological These factors are linked to the rate of technological innovation and advancement that may affect the Council. Examples include system upgrade requirements, data management and cyber security.

Social These factors are linked to the social environment including emerging trends and customer interactions. Examples include customer demand and expectations, public health and wellbeing and public opinion/reputation.

Determining Risk

4.14 Once the influencers on the objectives are understood, risks can be determined. The thoughts and ideas then need to be grouped into common themes and developed into the actual risk.

4.15 There should be three parts to a risks **Event –> Consequence –> Impact**. This will ensure that focus and action is placed on the event.

4.16 When recording risks on the risk register, these three factors will be recorded, so risk managers must identify all three elements

4.17 For example, Waste Services may identify the failure of the waste collection service due to environmental factors as a risk;

Failure of the waste collection service due to inclement weather (**the event**) could lead to unacceptable delays in collecting refuse (**the consequence**) resulting in public health issue and loss of reputation (**the impact**).

5 Risk Assessment

Types of Assessment

5.1 There are two risk assessments undertaken on each risk:

Table 1 – Risk Assessment Types

Assessment Type	Description
Inherent Risk	This is an assessment of the likelihood of the risk event happening, and of the impact to the councils objectives, if no controls or management measures are put in place. It helps understand the level of risk, and the level of management required. It also provides a baseline to compare against to understand the effectiveness of control measures.
Residual Risk	This is an assessment of the likelihood of the risk event happening, after management and control measures have been put into place. It helps risk managers, senior officers and members understand how the management and control measures impact on the likelihood and the impact of risk events.

Assessing Inherent Risk

5.2 Once a list of risks has been established, the next step is to assess those risks in terms of the likelihood that they will occur and the impact if they do.

5.3 This provides an inherent risk score that will help identify the most serious risks before any controls have been applied. Decisions can then be made about the significance of those risks and how or whether they should be addressed.

5.4 Consideration should be given to each of the identified risks and using the criteria in the likelihood table (section 5.14), assess the risk in terms of likelihood that it will occur.

5.5 The risk manager should then assess the impact using the criteria in the impact table (section 5.16) if it the risk event were to happen.

5.6 When both the risk likelihood and impact have been assessed, the likelihood score should be multiplied by the impact score – this will give the inherent risk score. This is the score used to identify which risks are the most serious, allowing decisions to be made about the significance of those risks to the Council and how, or whether they should be addressed.

5.7 The scoring methodology and risk appetite is set out in section 5.18.

5.8 The Council has determined that inherent risks which score as “Acceptable”, no further work is required. However, it is important to reconsider these risks on a rolling basis, as inherent risk can change based upon impacts from risk influencers.

Assessing Residual Risk

5.9 For any risks with an inherent scoring of “Manageable” or above, risk managers will need to consider the control and management measures that can be put in place to reduce the

likelihood and/or impact of the risk event (see section 6).

5.10 Once these control and management measures have been identified, the risk must be reassessed to determine the risk score after these controls and management actions are in place. This should demonstrate a reduction to the inherent risk level.

5.11 Using the criteria in the likelihood table (section 5.14), the risk manager should assess the risk in terms of likelihood that it will occur, with the control and management measures in place.

5.12 The risk manager should then assess the impact using the criteria in the impact table (section 5.16) if it the risk event were to happen with the control and management measures in place.

5.13 When both the risk likelihood and impact have been assessed, the likelihood score should be multiplied by the impact score – this will give the residual risk score.

Likelihood

5.14 Table 2 in this section sets out the definition, rating and descriptions used when assessing the likelihood of a risk event occurrence.

5.15 There should be a focus on the description when assessing the level of likelihood and the number rating should be used to summaries the descriptive information in a numerical format.

Table 2 – Likelihood Rating – Description and definitions

Definition	Rating	Description / Likelihood Guidance
Very Likely	5	• Regular occurrence • Circumstances frequently encountered • Possibility of occurrence more than 80%
Likely	4	• Occasional occurrence • Circumstances have been encountered before • Possibility of occurrence between 50% and 80%
Possible	3	• Likely to happen at some point in the next 3 years • Circumstance occasionally encountered • Possibility of occurrence between 10% and 50%
Unlikely	2	• Only likely to happen once every 10 or more years • Circumstances rarely encountered • Low change of occurrence (under 10%)
Remote	1	• Has never happened before • Circumstance never encountered • Negligible change of occurrence (under 2%)

Impact

5.16 Table 3 in this section sets out the definition, rating and descriptions used when assessing the impact of a risk event occurrence.

5.17 There should be a focus on the description when assessing the level of impact and the number rating should be used to summaries the descriptive information in a numerical format.

Table 3 – Impact – Description and definitions

Definition	Rating	Indicative Guideline
		Threat
Catastrophic	5	• Major loss of service for more than 5 days • Severe disruption to the Council and its residents affecting the whole council • Major financial loss > £1,000,000 • Loss of life, intervention by HSE • National news coverage • Likely successful judicial review or legal challenge of key Council decision • Major environmental damage • Loss of Assets or ICT incidents preventing continuation of service for more than 5 days
Major	4	• Major loss of service for 2 to 5 days • Severe disruption to the Council and its residents affecting several parts of the council • Major financial loss > £100,000 • Extensive/multiple injuries, intervention by HSE • National news coverage • Possible successful judicial review or legal challenge of Council decision • Major environmental damage • Loss of Assets or ICT incidents preventing continuation of service for 2 to 5 days
Significant	3	• Loss of service for up to 2 days • Serious disruption to the ability to service residents affected across one or two service areas areas of the council • Serious financial loss £50,000 to £100,000 • Major injury, possible intervention by HSE • Local adverse news item/ professional press item • Likely judicial review or legal challenge of service specific decision • Serious damage to local environment • Loss of Assets or ICT incidents preventing continuation of service for under 2 days
Serious	2	• Noticeable disruption to a service area • High financial loss £10,000 - £50,000 • Injury to an individual • Local news/minor professional press item • Moderate damage to local environment
Minor	1	• Brief disruption to service less than 1 day – minor or no loss of resident service • Low financial loss, less than £10,000 • Minor / no injuries • Minimal news/press impact • Affects single team only • Minor/ no damage to local environment

Scoring and Appetite

5.18 Table 4 in this section sets out the scoring methodology and risk rating (linked directly to the councils appetite to risk.

Table 4 Risk Scoring Matrix

Likelihood	Very Likely (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
	Remote (1)	1	2	3	4	5
		Minor (1)	Serious (2)	Significant (3)	Major (4)	Catastrophic (5)

5.19 Risks need to be managed within the Council's risk appetite. Whatever the risk score, mitigating controls and actions need to be applied to manage the risk down. The Councils Risk Appetite is demonstrated as follows:

Acceptable	Manageable	Serious	Severe

5.20 Section 8 of this framework sets out which level of risks will be reported, and to which groups.

6 Risk Management and Controls

6.1 When all the risk and opportunities have been identified and assed for likelihood and impact, there needs to be agreement on who will own the risk and who the risk will be managed, controlled or exploited.

6.2 There are three questions that will help:

- Can the likelihood of occurrence be reduced?
- Can the impact be reduced?
- Can the consequences of the risk be changed?

6.3 **Tolerating the risk** An organisation that recognises the value of risk management may accept that it might be appropriate to continue with an “at risk” activity because it will open up greater opportunities for the future, or perhaps limited things can be done to mitigate a risk.

These risks must be monitored, and contingency plans should be put in place in case the risks occur.

6.4 **Treating the risk** This is the most widely used approach. The purpose of treating a risk is to continue with the activity which gives rise to the risk, but to bring the risk to an acceptable level by taking action to control it in some way through either:

- Containment actions, these lessen the likelihood of consequences of a risk and are applied before the risk materialises
- Contingency actions, these are put in action after the risk has happened, thus reducing the impact.

6.5 **Terminating the risk** Doing things differently and therefore removing the risk. This is particularly important in terms of project risk.

6.6 **Transferring the risk** Sometimes a risk can be transferred to a third party, for example via insurance or by arranging for a third party to take the risk in another way.

6.7 The cost of risk management and control of the risk should be proportionate to the risk that is being addressed. There is a need to;

- Identify existing controls and actions plans that are in place. Develop new controls and action plans where none exist.
- Identify and agree who will own and manage the. The risk manager should have authority to implement and manage the controls.

6.8 When the existing controls and action plans have been identified, the risk can be re-assessed for likelihood and impact, to determine the residual risk score.

6.9 All key controls and management measures should be recorded on the Councils Risk Register.

7 Risk Registers

7.1 Risks should be recorded on the Councils Risk Register.

7.2 The Risk Register is maintained on a single sharepoint list for operational and strategic risks, available to risk managers. A separate risk register is maintained as a single list for project risks.

7.3 Risks should be updated on a monthly basis. This should include:

- A review of the inherent risk where appropriate. Inherent risks may be influenced by the risk influencers, leading to an increase or decrease in the risk score.
- A review of the residual risk where appropriate. Residual risks may be influenced by a failure in the control or management measures, or the risk influencers, leading to an increase or decrease in the risk score.
- New narrative each reporting period.

7.4 For each reporting period, the risk narrative should include:

- A description to explain any changes to the inherent or residual risk scores.
- A description to explain any additional control measures put in place, or any issues with the control measures that are in place
- Any key activity undertaken in the previous reporting period, or upcoming reporting period.
- A description to explain any new risks that have been added during the period, or for any risks that have been closed.

8 Risk Reporting

Regular reporting for risk oversight and the management of risk will be as follows:

Strategic Leadership Team	Monthly
Performance Clinic	Quarterly
Cabinet	Quarterly
Audit Committee	Quarterly

8.1 Reporting will include all strategic risks. Operational risks will be reported where the residual risk is “Serious” or “Severe”. The management of “Manageable” risks will be the responsibility of Directors and risk managers.

8.2 Project Risks will be the responsibility of Project Sponsors and Managers. These should be transferred to Operational and Strategic risk registers where there is a likely impact on the Council’s ability to deliver its objectives.

8.3 Audit Committee is responsible for monitoring the Councils risk management arrangements.

8.4 Directors should ensure that Executive Members are briefed where appropriate at monthly briefings to ensure they are aware of significant risks affecting their portfolios and any improvements in controls which are proposed.

8.5 The production of the Annual Governance Statement signed by the Chief Executive and Leader of the Council at the end of each financial year, will report on the effectiveness of Risk Management and report on any governance issues.

8.6 Other Corporate Groups will also oversee specific themed risks, such as Health and Safety Risks being overseen by the Operational Health and Safety Board, who will report significant matters to the Corporate Governance Group.