Reigate & Banstead Borough Council

Risk management methodology

2023/24 to 2025/26

Contents

Introduction

This risk management methodology provides the information and additional detail that is required to apply the principles and achieve the objectives that are set out in the Council's risk management strategy.

The methodology sets out the roles and responsibilities relating to risk management across the Council and across the three lines of defence, as well as detailing the processes and procedures that collectively (and sequentially) comprise the Council's risk management cycle.

The methodology should therefore be read alongside the risk management strategy, where it follows a similar structure for the ease of use and reference.

The methodology is targeted at all levels of management at the Council, as well as the Council's Projects and Business Assurance team who provide support to the achievement of the Council's risk management objectives.

Identifying risks

Risk identification is the first step in the process of building an organisation's risk profile and developing risk awareness.

Processes for identifying risks

Risk identification is about identifying what could happen and what the impacts could be on the Council.

Risks should be considered at all levels of the Council and in all aspects of decision-making, including in setting priorities, objectives and in deploying resources. The identification and management of risk is the primary responsibility of service management at the first line of defence. Managing risk is a core component of effective, competent management and the Council is keen to empower first line service management to deal with risk effectively as part of business-as-usual.

It is important that all risks threatening the Council's objectives are identified and documented as a key first step in managing the risk to an acceptable level, as defined by the risk appetite. All risks, even those outside the direct control of the Council should be considered.

Examples of situations where risk should be considered include:

- As part of the **routine course of service and department management** (the first line of defence), where managers and Heads of Service are expected to design and manage their services to reduce risk (both service and corporate) as part of business-as-usual arrangements.

- During the **annual service and financial planning process**, which informs the Council's annual budget. Risks facing services should be considered and documented in each respective service business plan.

- On a **quarterly basis** alongside Heads of Service and the Senior Management Team, where existing risk registers and the Council's assurance framework is reviewed to identify if there have been any substantive changes to its contents and, by extension, the Council's risk profile, with appropriate action taken.

- During the annual update of the Council's **Medium-Term Financial Plan (MTFP)**. The MTFP highlights the key financial risks facing the Council and the action being taken to mitigate them.

- As part of developing and implementing any **policy or strategy.** Consideration must be given to how the Council's ambitions detailed therein may be adversely affected by risk, with appropriate action planned to control and/or mitigate the risk through various treatment options.

- When any **delegated or constituted decision-making body makes a decision**, the risks associated with the decision (or non-decision) must be considered.

- Throughout the **project and programme management life cycle**, including in developing the initial business case as well as ongoing implementation and reporting against it.

PESTLE analysis is a widely used business tool that involves identifying and evaluating political, economic, social, technological, legal and environmental factors that affect a business. It is particularly useful in risk management in identifying risks arising from the **external environment** and should be used as part of the annual service and financial planning process to support service design and risk management.

Political	Factors arising from the political environment, including the national, local and regional. Closely related to legal.
Economic	Factors which include economic growth, the fiscal environment, interest rates, exchange rates, inflation, wage rates, working hours and the cost of living.
Social	Factors that include cultural, health and wellbeing and wider demographic issues.
Technological	The development and impact of technology both on business operations and on customer/stakeholder expectations.
Legal	Changes in the legislative environment affecting the organisation.
Environmental	Impacts of climate change or how the environment affects business operations.

Not all risks are reasonably foreseeable or evident, however. Likewise, many risks are inherent and ever present, where the environment within which they exist may drastically shift

with little warning. Similarly, previously robust controls and mitigations may fail, drastically changing the wider control and risk environment. As such, it is crucial that the first line of defence is supported by other systems, processes and best practice to proactively identify risks or failures of controls so that appropriate management action may be taken. This support is provided by the second line of defence.

The role of the second line of defence typically includes assessing service compliance with agreed corporate and operationally defined standards. It also includes review activity to determine, in the context of risk, the extent to which standards, expectations and policies and procedures are set at the correct level and whether these are being met.

Full roles and responsibilities are set out in the roles and responsibilities section below.

The third line of defence is comprised of internal and external audit.

An independent 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. All risks faced by the Council should be in the internal auditor's scope.

Internal audit's role is to identify potential weaknesses in systems, controls and procedures that may expose the authority to risk. Whilst internal audit highlights these weaknesses, it is the responsibility of management to design and implement actions that address them and, in so doing, control and mitigate risk.

External audit is responsible for reviewing and verifying the Council's annual statement of accounts. External auditors also have a duty to inform key stakeholders of matters of importance arising from their reviews, including governance and risk management concerns.

Recording risks

The Council has two core mechanisms for maintaining corporate visibility of risk:

- The assurance framework
- Corporate risk registers (strategic and operational)

Assurance framework

The assurance framework should record all principal risks faced by the Council and which are reasonably foreseen as part of service planning and the usual course of management. It should also include those risks that are regarded as being sufficiently controlled in accordance with the Council's risk appetite.

The assurance framework cannot reasonably or usefully be expected to identify every risk the Council faces in specific detail, or all specific permutations or situations within which risk may be manifested. Instead it should focus and group risks by high-level category – referred to as principal risks – for the ease, clarity and effectiveness of analysis. Doing so will also provide clarity of assurance to key stakeholders. The identification of sub-categories of principal risks may also be appropriate to aid its use.

Example principal risk areas include:

- Health and safety (staff and resident)
- Safeguarding
- Cyber security
- Business continuity
- Governance and decision-making
- Political and officer leadership (capacity and culture)
- Recruitment and retention
- Management (systems and processes)
- Legislation and regulations
- Financial
- Contracts
- Suppliers and supply chains
- Projects
- Civil emergencies
- Market factors
- Fraud (internal and external)

The assurance framework should be compiled annually as an output of service and financial planning. It should be reviewed quarterly as a basis for regular conversations with service management on risk, with any new risk areas added as appropriate.

The Projects and Business Assurance Team maintains the Council's assurance framework alongside service management and the Council's wider Senior Management Team.

Corporate risk registers

The Council maintains two corporate level risk registers: strategic and operational.

- **Strategic risk register:** risks that could have a negative impact on the Council's medium to long term objectives and priorities as set out in the Corporate Plan or other corporate level policies and strategies, including the Medium-Term Financial Plan (MTFP). Strategic risks typically originate from the environment within which the Council operates, though may also stem from an internal source – such as major project – if the impact merits its categorisation as a strategic risk.

  Members of the Council's Senior Management Team and Executive members have shared responsibility for strategic risks.

- **Operational risk register:** risks that are encountered in the delivery of services and which affect service objectives. These risks are ordinarily managed as part of the usual course of management by services, including their business-as-usual activities and projects that are being delivered. However, where the operational risk cannot be managed within the service or if its score is outside of the Council's risk appetite, then it should be considered for inclusion in the operational risk register.

  Heads of Service and service managers have responsibility for operational risks.

Risk registers deal with risks of current concern; that is, risks that are not sufficiently controlled and/or mitigated in accordance with the Council's risk appetite.

Risks on the risk register are likely to be specific manifestations of principal risks and/or those that are situationally specific and the outcome of a particular constellation of circumstances, including previously 'unknown unknowns' and which present a threat to the Council until they are sufficiently controlled and/or mitigated. They may also arise from a breakdown of current controls and/or mitigations, either due to a change in the risk environment or from a degradation in the Council's internal control environment.

To be clear, risk registers are distinct from the assurance framework in that they are separate documents. The assurance framework, in order to heighten risk awareness and support

effective governance, should list all theoretical, principal risks facing the authority. Risk registers deal with risks by exception, and which are of current concern given their assessment and scoring in terms of the Council's risk appetite.

Risks will remain on the appropriate corporate risk register until they are treated to the desired level.

Additional detail on risk monitoring and reporting is provided below. At this point, however, it is important to note the following:

- Corporate Governance Group is responsible for maintaining and approving the Council's assurance framework as part of its governance role. It does so in close collaboration with the Executive and, in so doing, benefits from comments and/or observations made on its contents by the Audit Committee.

- The Executive is ultimately responsible for approving the strategic risk register and changes made therein – including closing risks and raising new risks – following recommendations made by Corporate Governance Group and any observations made by the Audit Committee.

- Corporate Governance Group maintains oversight of the operational risk register, including its annual compilation and in adding in new risks or closing existing risks. Operational risks are reported to the Executive when they are at a level of concern (red rated).

The assurance framework and risk registers support one another and represent the successful and mature operation of the Council's risk management cycle. They are fundamental, supporting components of effective risk management, governance and control through giving management and key stakeholders confidence that the Council's risk management profile is comprehensive and well understood, is supported by an effective control environment and that management attention is being focused in the right areas.

It is important to note that risks may also be captured in other key corporate and management documentation, including in committee reports, project level risk registers and health and safety reports, amongst many others. The corporate assurance framework and risk registers do not hold the monopoly on documenting risks. Instead, the assurance framework should document high-level, principal risks and avoid unnecessary granularity, whilst the corporate risk registers should document risks that are of current concern and are receiving concerted management attention.

Describing a risk

Once a risk has been identified it should be described. It is important that a risk should be described clearly so that it is fully understood and to assist with the identification of controls and mitigations, both current and potential. A clear risk description also helps with assessing the likelihood and impact of risks.

The risk description should avoid being lengthy and detailed, though should give sufficient information to clearly understand the cause and potential consequences or impacts of the risk.

The risk description should:

- Set out the **cause** of the risk. This refers to the relevant context and background. A cause may be a discrete element or an event or occurrence which either happens or does not happen in giving rise to the risk.

- Set out the **consequences** of the risk should it occur and which will need to be managed, with particular reference to the impact on objectives.

Once a risk has been identified it should also be allocated a risk owner.

A risk owner is the officer(s) and relevant Executive Member that owns the impact of the risk should it materialise. They are ultimately accountable for controlling and mitigating the risk to the desired level and minimising its potential impact on the Council's objectives. Risk owners are usually Heads of Service, though, depending on the risk, may also include members of the Senior Management Team.

To aid ownership and accountability there should be as few risk owners as necessary, though risks that are cross cutting in their nature may necessarily have more than one owner.

The risk owner may not have primary operational responsibility for implementing controls and/or mitigations related to the risk, which may be delegated to another team or department within the Council. The officer risk owner is ultimately accountable for the risk and its mitigation, however, and should therefore have sufficient authority and seniority to identify, prioritise and deploy resources to manage risks in accordance with the Council's risk appetite.

Assessing and analysing risks

Once a risk has been identified it must be assessed to ascertain the potential impact and for treatment options to be designed.

Risk appetite

It is good practice for an organisation to articulate and communicate its appetite for risk with a formal risk appetite statement. The risk appetite statement provides a sound management foundation for risk management and exercising effective internal control across the organisation.

Whilst an overall risk appetite may be articulated, it is important to note that the Council's risk appetite varies by the category of risk, the detail of which is set out below.

Risk appetite statements can be used in two core ways:

1. When considering and evaluating the best response to risks threatening corporate objectives; and,
2. When making decisions and considering the risk implications of accepting or rejecting a course of action.

Defining the limits of a risk appetite is about identifying at what point decisions regarding the management of a risk are escalated for decision and/or wider corporate awareness. Risk appetite forms part of the overall framework around which decisions are made at the Council. Risk appetite should not be applied as a rigid target, but instead serves as a guide to the levels of risk that we are willing to take if supported by a strong consideration of all relevant factors.

Risk, and the Council's appetite for it, should be considered in all aspects of decision-making and not just when management considers formal risk management reports, such as its quarterly receipt of risk registers.

A clear, well understood risk appetite statement helps ensure:

- Risks are appropriately considered in decision making and that acceptable outcomes are achieved;
- Responses to risks are proportionate;
- Consistency in decision-making with respect to risk from across the Council's functional business areas;
- That the accepted risks are commensurate to the opportunity or reward to be gained;

- Corporate oversight and understanding of the Council's diverse range of risks, underscoring effective management and corporate governance; and,
- Risk controls and mitigations (either those for inherent risks and those of concern) are appropriately tailored to the level of risk faced.

The risk appetite of the Council varies on the nature of the risk and the impact therein. As such, the risk appetite is segmented on the basis of categorising the impacts of risk.

The risk categories are as follows:

- **Environmental –** risks that concern the environmental impact of Council services and investment priorities.

- **Financial (revenue) –** risks related to not achieving income and savings targets, as well as the incurrence of unexpected costs. It covers both internal budgetary pressures and external macro level economic changes, such as changes to funding agreements with central government and other agencies.

- **Financial (capital) –** risks associated with the council's assets and investment in physical infrastructure, such as property or the council's fleet vehicles, financial assets, and investment portfolio.

- **Sociocultural –** risks of not meeting – or jeopardising – the needs of residents or worsening social outcomes. This could arise from not responding to changes in demographic or socio-economic trends that impact on the Council's ability to meet its objectives. The consequence of these risks could be credibility loss or a diminution in trust.

- **Corporate objectives –** these are risks that will put corporate plan delivery and other strategic policies at jeopardy. These risks, if likely to materialise, may cause consideration of the hierarchy of the Council's objectives and whether some must be prioritised over others.

- **Operational –** risks associated with the delivery of day-to-day services. This includes maintaining the resilience of the organisation, such as capacity and workforce risks; the failure to meet service plans that impact the achievement of objectives set out in the corporate plan; health and safety of employees; and adequate delivery of statutory duties.

- **Legal/reputational –** risks that can result in legal challenges and being subjected to litigation and external sanction. These risks include non-compliance with legal frameworks and statutory requirements, employment, health and safety processes etc. It also includes risks of the changing national regulations that could threaten the Council's operations and processes. Included in this category are risks that would result in negative reputational impacts.

- **Technological –** risks that are connected with technology, including the protection of data and the integrity of internal systems as well as how technology processes work for both internal (officers) and external (residents) stakeholders. This also includes the adoption of new systems and the maintenance of legacy systems as well as the security awareness of officers to keep information secure as well as the capacity of the Council to deal with technological advancements and changing demands.

Risk appetite statement

In pursuit of its wider strategic objectives, the Council recognises that it will be required to take calculated risks.

Overall, the Council **prefers a cautious approach to risk** but acknowledges that it in some areas it is necessary to accept higher levels of risk to ensure the achievement of objectives.

The Council's risk appetite will be subject to review on a three yearly basis as part of the regular, cyclical review of the Council's risk management strategy – or more frequently if necessary.

The Council's risk appetite statements on the above categories are set out in the table below.

It should be noted that the risk appetite statements apply to the level of residual risk. Residual risk is the level of risk after controls and mitigations have been applied.

Risk appetite statements by category

Risk category	Appetite	Risk appetite statement
Environmental	**Averse**	We will only accept the risk of negative impacts to the environment from our activities (which could take the form of direct negative outcomes for the environment or delays to our commitment of reducing emissions and environmental impacts) where we can demonstrate clear benefits of accepting this risk when weighed against other considerations and other risks.
	Cautious	
Financial – revenue	**Cautious**	We will only take measured risks and prefer initiatives where we can be confident in positive outcomes in order to preserve our ability to pursue significant returns when the opportunity arises and conditions are right.
Financial – capital	**Open**	We acknowledge that investment comes with risk, and we are willing to be open in our approach. This means that we are prepared to accept higher levels of risk but aim to do so in a controlled manner.
Sociocultural	**Open**	We are willing to make decisions that could prove to be unpopular in the short term, where clear benefits can be demonstrated in the medium and longer term.
Corporate objectives	**Open**	We will set ambitious, and sometimes aspirational, targets with the understanding that we might risk delays, non-delivery or later adjustment of some corporate objectives.

Risk category	Appetite	Risk appetite statement
Operational	**Open**	We accept that change initiatives carry short-term risks of compromising some operational areas for a limited time. Exceptions are health and safety of staff and residents, and statutory duties, where there is a very low appetite for risk of lapses or non-compliance.
Legal/ reputational	**Cautious**	We will explore areas of opportunity within legislation, and we are willing to defend our position where challenge could occur. However, we are reluctant to incur the risk of significant reputational damage or external sanction.
	Open	
Technological	**Cautious**	We will be cautious with technology related risks. When we look to upgrade and deploy new technology, we prefer investing in proven solutions although we are conscious of the risks associated with not acting in time or applying continuous upgrades and maintenance.

Note – the colours in the appetite column correspond to the risk scoring matrix below.

Risk assessment: analysing and evaluating impact and likelihood

Whilst the risk appetite sets out the overall level of risk that the Council is prepared to accept in pursuit of its objectives, it is necessarily high level. In order to apply the risk appetite effectively and ensure it guides decision making, the overall risk appetite must be underpinned with individual, robust risk assessments following the risk identification process.

Whilst each risk may be important on its own, a degree of measurement is required to evaluate its overall significance, thereby supporting effective and risk informed decision-making. Without a standard for measurement and comparison it is not possible to effectively compare and prioritise the various possible responses to risks.

Prioritisation is predicated on the undertaking of robust risk assessment which, in turn, incorporates effective risk analysis.

Risk analysis must use a common and overarching set of risk scoring criteria to foster a consistent interpretation and definition of risk, based on an assessment of the **likelihood** of the risk occurring and the type and level of **impacts** that are expected should it do so.

The upshot and ultimate purpose of this process is to use the insight gained to evaluate the extent to which the identified risks align with the Council's risk appetite. Doing so helps determine what, if any, action is required or whether the current controls and/or mitigations are excessive and out of proportion to the risk faced.

Identified risks must therefore be analysed and scored on a **likelihood and impact matrix**.

In terms of **likelihood**, the following levels are used:

- **Almost certain (5)** Very likely to happen (>80% chance)
- **More than likely (4)** Likely to happen (60-80% chance)
- **Possible (3)** Might happen (30-60% chance)
- **Unlikely (2)** Unlikely to happen (10-30% chance)
- **Rare (1)** Highly unlikely to happen (<10% chance)

The timeframe for assessing the likelihood of a risk occurring is within the next two to three years.

Once the likelihood has been assessed, the **impact of the risk** should then be considered. The risk impact scoring matrix below sets out the impact categories and thresholds to be considered when scoring the impact of a risk. It also defines the relationship to the Council's risk appetite, with additional information on this set out in greater detail later.

Risk impact scoring matrix

	1 Almost none	2 Minor	3 Moderate	4 Significant	5 Grave
Environmental	Little or no impact on the local environment	Short term minor local impact with no ongoing negative effects	Medium term, moderate and reparable local impacts **(2)**	Large scale and long-term damage to the environment **(1)**	Extensive and potentially irreparable damage to the environment **(1)**
Financial – revenue[1]	<0.1% of net revenue budget	0.1-0.5% of net revenue budget	>0.5% of net revenue budget **(2)**	0.6-1% of the net revenue budget **(1)**	>1% of the net revenue budget **(1)**
Financial – capital[2]	<0.1% of the capital programme	0.1-0.5% of the capital programme	0.5-1% of the capital programme **(4)**	1-2% of the capital programme **(3)**	>2% of the capital programme **(2)**
Sociocultural	Little to no negative impact to community resilience and social cohesion	Short term impact on community resilience and social cohesion	A section of the community impacted for the medium term. Some loss of credibility for the Council **(4)**	Long term, significant community impacts. Trust in the Council compromised **(3)**	Community resilience and social cohesion is severely compromised **(2)**
Corporate objectives	Up to 5% variation in achievement of corporate targets	5-20% variation. Workaround required within RBBC resources to deliver objective	20-40% variation. Resources must reassigned and prioritised **(4)**	40-60% variation. Reconsideration of viability of corporate objectives **(3)**	>60% variation. Unable to deliver objectives. Failure to meet community needs **(2)**
Operational	Little to no impact to service delivery	Failure to meet standard customer expectations and needs	Failure of several non-statutory services **(4)**	Temporary loss or disruption to critical services **(3)**	Sustained loss of disruption to critical services **(2)**
Legal/ Reputational	Minor adverse publicity in the local media	Sustained local media and online criticism. Potential for minor financial penalties	Adverse publicity in the national media. Potential for legal sanction and/or moderate fine **(2)**	Negative national media attention or criticism from an external agency. Litigation likely with some defence **(1)**	Sustained negative national media coverage. Penalties likely with little defence from litigation **(1)**
Technological	Negligible service disruption of less than 0.5 days. Critical systems unavailable for less than 1 hour	Disruption of service for 1-2 days. Critical systems unavailable for up to 0.5 days	Disruption of service for 3-7 days. Critical systems unavailable for up to 1 working day **(2)**	Disruption of service for 7 to 21 days. Critical systems unavailable for 2 working days **(1)**	Disruption of service >21 days. Critical systems unavailable for more than 2 working days **(1)**
(#) is the lowest LIKELIHOOD score that, when multiplied by the IMPACT score, would most likely render the risk outside of appetite. The colour corresponds to the risk scoring matrix should this threshold be breached (see below). See the guidance notes below for additional information.					

[1] The net revenue budget in 2022/23 was £19.8 million.
[2] In 2022/23 the total capital programme value was £52 million.

The likelihood and impact scores are then combined to give an **overall risk score**. This is done by multiplying the likelihood score by the impact score.

The total risk score is then plotted on a scoring matrix to illustrate the risk scoring visually:

IMPACT						
Grave	**(5)**	**5**	**10**	**15**	**20**	**25**
Significant	**(4)**	**4**	**8**	**12**	**16**	**20**
Moderate	**(3)**	**3**	**6**	**9**	**12**	**15**
Minor	**(2)**	**2**	**4**	**6**	**8**	**10**
Almost none	**(1)**	**1**	**2**	**3**	**4**	**5**
		(1)	**(2)**	**(3)**	**(4)**	**(5)**
LIKELIHOOD		**Rare**	**Unlikely**	**Possible**	**More than likely**	**Almost certain**

It is important that identified risks should be **scored and assessed** on the following three points:

1. **The inherent risk –** refers to an analysis focused on identifying the likelihood and impact of a risk occurring without any controls or mitigations in place.

   A risk control is a process, policy or activity that reduces the likelihood of a risk materialising, whilst a risk mitigation reduces the impact should it do so.

   The analysis should be done alongside the identified risk owner and relevant service area.

2. **The current risk –** refers to analysing and assessing the current controls and mitigations that are in place to reduce the likelihood and impact of a risk materialising. Risk control and mitigation are not exclusive, binary concepts. They should be designed by management to work together to reduce the overall impact of risk on the Council in a balanced and proportionate way.

   The analysis should be substantive though proportionate and based on evidence. Any limitations of the evidence should be recognised.

   As with assessing inherent risk, the assessment of the current risk must be done alongside the risk owner and the relevant service to harness their specialist knowledge. However, it may also be appropriate to draw on other sources of assurance, including internal audit reports as well as any other relevant pieces of consultancy or advice.

   As part of this process, it is important that the risk controls and mitigations are clearly documented, at a minimum, on the Council's assurance framework. The assurance framework considers *principal risks* and so the content relating to controls and mitigation should be tailored appropriately.

   Assessing the current risk must be done with reference to the Council's **risk appetite** by category. The impact table set out above details how the overall risk score (arrived at by multiplying the impact by likelihood) relates tx`o the Council's risk appetite. The impact table sets out the *minimum* likelihood value that, when multiplied by the impact score, would likely render the risk outside of appetite.

   Risks invariably have multiple impacts and so the highest scoring category should be used to score the impact of the risk. Moreover, due to the individual nature of risks, the table and the relationship to the Council's risk appetite should be used as a guide, with appropriate discretion exercised in application, particularly where gaps in information exist or where its quality or certainty is in doubt.

   If, following assessment, the risk score is **within the Council's risk appetite** as set out above, then no further action is required. The risk (in its high level, principal form) and the corresponding controls and mitigation should be recorded on the assurance framework for review at a later date (likely at the end of the next quarter).

   However, if the risk score is **outside of the Council's risk appetite** as set out above, then the risk should be considered for inclusion on the relevant corporate risk register for wider corporate awareness and oversight.

   Risk treatment options – i.e. new controls and mitigations – are considered below.

3. **The target risk –** is concerned with where management are aiming to treat or manage the risk to. The target risk sets out the desired and acceptable end point of the risk management cycle.

   For purposes of governance and the exercising of effective internal control, the target risk should be documented for all risks that have been identified.

   The target risk must be set with reference to the Council's risk appetite which defines the levels of risk the Council is prepared to accept.

   Setting the target risk is crucial to evaluating and confirming the adequacy and effectiveness of (a) the current controls and/or mitigations; and (b) the new controls and/or mitigations proposed in response.

   The target risk score should be set at a realistic level and recognise the Council's ability to influence the risk. It is certainly possible – and likely – that, for certain risks where the Council has limited scope to act, the current risk score may remain in excess of the target score. These risks should still be documented as appropriate, however, to maintain the effectiveness of the Council's risk profile.

   Additional detail on risk treatment options is set out in the section that follows.

Treating risks

Risk treatment is ultimately concerned with selecting the most appropriate course of action for managing a risk and returning it to within the accepted corporate risk appetite, balancing the potential benefits of action against the costs and disadvantages, as well as against the Council's ability to influence or act against a risk.

The Council's approach to risk management (as set out in the three lines of defence model) delegates primary responsibility for managing risks to service management. The effective, collective functioning of the three lines of defence model should therefore largely deal with risk management as business as usual, with risks identified and management processes designed to minimise and treat risk in accordance with the Council's risk appetite.

It is important for purposes of governance and the exercising of effective internal control that risk treatment is carried out in a standardised way, with adequate ownership and oversight maintained. The process articulated below should apply as part of effective, routine service management and not just for risks deemed to be of concern and captured on the corporate risk register.

Actions and options

The risk owner is responsible for treating the identified risk and taking action to move it to being within the risk appetite or, if this is not possible, to take action to return it to a level that is as close to being acceptable as possible. This will in most instances take the form of designing and implementing a range of actions or measures which will reduce the likelihood of the risk materialising (a control), and/or the impact should it do so (a mitigation).

These actions should be specific, measurable, achievable, relevant and time-bound (SMART) and should be regularly reviewed and reported on. The process for risk monitoring and reporting is set out below.

Before designing treatment options, risk owners should carry out an options appraisal to gauge the most effective and advantageous course of action. There is no expectation that this should be formally documented and reported on, though risk owners may decide that doing so is appropriate in certain instances, such as where considerable costs are involved, where the overall impact of the risk is significant or where other Council governance and decision-making processes require it. Such an appraisal would likely form a key part of any business case where additional or unbudgeted costs are to be incurred as part of a management response.

Risk owners will be supported in carrying this out by the Council's Projects and Business Assurance team who provide advice as part of their second line of defence function, as well as any other services at the second line of defence.

The options appraisal should consider how to treat the risk on the following basis:

- **Avoidance –** simply stop doing the activity that creates the risk, or elements therein. This may not be possible or desirable, however, particularly where the risk is unavoidable or arises from activity that the Council is obliged to undertake. Risk avoidance must also be balanced against the effect of doing so on the Council's objectives and how this reconciles with the wider risk appetite. Indeed, there are invariably risks associated with ceasing an activity and which must be likewise considered to give a rich, fulsome picture of the Council's wider risk profile.

- **Transfer –** transfer all or part of the risk to another party, such as to insurance or to an agency or contractor. The risk owner still maintains ultimate ownership of the risk, however. There will likely be costs associated with this course of action and these must be considered appropriately.

- **Reduce –** take steps to reduce the likelihood and/or impact of the risk, such as introducing new or modifying existing controls and mitigations.

- **Accept –** accept the risk and take no measures to reduce the likelihood and/or impact. This is not ordinarily a recommended course of action, though if the risk is outside of the Council's control it then it may be the only option available.

Depending on the risk, the pursuit of a combination of these options may be appropriate.

The appraisal should consider the associated costs, resources, time pressures and potential financial and non-financial benefits of any course of action. Advice from specialist staff – including those at the second and third line of defence – should be taken where appropriate.

It is worth noting that the benefits of action will not always be solely financial. Risk owners must therefore use their professional knowledge and judgement to ascertain whether costs are justifiable in terms of non-financial benefits to the Council. On occasion, it may thus be reasonably concluded that the costs of action outweigh the perceived benefits.

However, it is imperative that any chosen option should be well reasoned, proportionate, effective, lawful and in full conformance with standards of good and ethical governance.

Costs should not be the overriding determining factor in implementing risk treatment options, however. At a minimum, all categories set out it the risk appetite should also be considered to ensure that risk treatment aligns with the Council's risk appetite.

As part of selecting and developing risk treatments, the risk owner is responsible for defining how the chosen option(s) will be implemented in a way that is well understood by key parties and stakeholders. This should include:

- The rationale for the option(s) chosen, including the expected benefits;
- The proposed actions (e.g., implementing new controls and/or mitigations);
- Identifying those that are accountable and responsible for the implementation of any actions arising;
- The resources required;
- Any key performance indicators that may be used to demonstrate progress of implementation or any other indicators which may demonstrate a change in the nature of the risk or control environment;
- When actions are expected to be undertaken and completed by; and,
- Any constraints and dependencies to be aware of.

Ultimately, the category of treatment option chosen, as well as all controls and mitigations, should, as required, either be recorded on the Council's assurance framework or the relevant corporate risk register.

Whilst the former sets out principal risks which are regarded as being sufficiently controlled, the latter sets out current risks of current concern. As such, corporate risk registers will necessarily include greater specific detail on the control and/or mitigation of risk.

Risk monitoring and reporting

The Council's risk profile should be regularly monitored and reported on. This is because:

- Previously identified risks may change over time and treatment options may require adaptation;
- The internal control environment may degrade and action is required as a result;
- Previously unknown or new risks may emerge, with current controls and/or mitigations possibly proving inadequate; and,
- Following management attention or a change in circumstances, known risks may merit closure.

Monitoring and reporting are two distinct though mutually reinforcing processes that underpin the effective operation of each stage of the risk management cycle.

Risk monitoring involves teams and functions from across the three lines of defence model.

Whilst each line of defence and team therein has its own distinct functional role, they should operate in an integrated way to support the ongoing development of understanding on the Council's risk profile and how this may change over time. It provides assurance that risk controls and mitigations are operating as intended to provide reasonable assurance over the management of risks to an acceptable level, as defined by the Council's risk appetite.

Risk monitoring should thus be carried out before, during and after the implementation of risk treatment options for those risks that are being given active management attention (and therefore set out on the relevant corporate risk register), as well as those that have been identified as being sufficiently controlled and/or monitored (and therefore set out on the assurance framework).

The results of risk monitoring are incorporated into the Council's wider performance management and governance activities and must be reported and communicated to stakeholders as appropriate.

Monitoring

Risk monitoring is fundamentally within the scope and remit of service management, given that the Council's risk management strategy empowers them to manage risk as part of business-as-usual arrangements.

As experts in their field first line management are responsible and accountable for designing and implementing adequate risk monitoring processes as part of effective service

management and in accordance with the Council's constitution and scheme of delegation. They are supported by specialist services found at the second and third lines of defence (internal and external).

There are many ways in which risk existing risks may be monitored by the first line of defence, including:

- Monitoring of trends, key performance indicators or other contextual indicators which may suggest a change in the control and/or external environment;
- Deep dive reviews into particular risk areas, either carried out by management or commissioned by teams at the second and third lines of defence;
- Learning from incidents, issues and/or the experiences of others or wider sector best practice;
- Testing of the effectiveness of identified controls and mitigations; and,
- Horizon scanning for changes in the external risk environment, using tools such as PESTLE as set out above.

Taken together, the Council's assurance framework and corporate risk registers serve as a comprehensive record of the risks faced by the Council and are key corporate control documents for risk monitoring.

The assurance framework and corporate risk registers must be reviewed at least on a quarterly basis, though management are encouraged to do so more regularly if necessary as part of the usual course of service management.

The Council's Projects and Business Assurance team will support service management in undertaking risk monitoring via the quarterly risk management review process.

The quarterly risk management review process will review all identified risks alongside the risk owner – namely, those principal risks set out in the assurance framework and the risks of concern set out in the corporate risk registers.

The quarterly risk management review will:

- Consider whether the risk description continues to adequately cover the risk (particularly important for the risk registers, given their specificity);
- Critically assess the prevailing effectiveness of controls and/or mitigations that are in place;
- Ensure the recorded controls and/or mitigations are up to date and reflect the latest position;
- Review and confirm the inherent, current and target risk scores to ensure they are accurate and reflect the current situation; and,

- Consider whether any further action or escalation may be required.

The quarterly risk management review process will also consider whether any new risks have emerged in accordance with the process as set out in the risk identification and assessment section of this methodology.

Not all risks are reasonably foreseeable or evident, however, and may not be recorded on the Council's assurance framework and/or corporate risk register. Likewise, many risks are inherent and exist perennially, where the environment within which they exist may drastically shift with little warning. Previously robust controls and mitigations may also fail, changing the internal control and wider risk environment.

It is therefore crucial that the first line of defence is supported by other systems, processes and best practice to monitor and review the Council's risk profile so that appropriate, corrective management action may be taken. This support is provided by the second and third lines of defence.

The second line of defence provides the overarching policies, frameworks, tools, techniques, and support to enable risk and compliance to be managed effectively by the first line, and conducts monitoring activity to judge how effectively this is being done. It may take the form of bespoke, commissioned pieces work, or may be undertaken as part of the second line's 'business-as-usual'. In any case, the second line of defence is a key source of assurance in the context of risk and must be drawn upon as part of the quarterly risk review process.

The second line of defence should not solely rely on the corporate risk monitoring and review process to escalate concerns and should have a direct reporting route into senior management via Corporate Governance Group should any concerns arise.

The teams in the second line of defence as set out in the risk identification section of this methodology will exercise a similar function in risk monitoring; full roles and responsibilities are set out in a later section of the methodology.

The third line of defence relates to independent, external assurance in risk monitoring and is largely focused on the roles of internal and external audit.

Internal audit, through its annual risk-based audit plan, will provide an objective opinion on governance, risk management and internal control. It sits outside of the first and second lines of defence, where its main role is to ensure that the first two lines are operating effectively and to also advise how they may be improved. The Council's assurance framework and corporate risk registers are key sources of information in helping to direct internal audit activity.

Internal audit reports to Corporate Governance Group and the Audit Committee. Matters of concern arising from internal audit reviews should be included within the assurance framework and/or corporate risk registers as appropriate.

External audit reviews and verifies the Council's annual statement of accounts. External auditor has a duty to inform key stakeholders of matters of importance arising from their reviews, including governance and risk management concerns. Any such findings made by external audit will be acted upon by management and the political leadership as necessary.

Reporting

Risk reporting is the ultimate output of risk monitoring. High quality and timely reporting provides assurance to key stakeholders that the risk management cycle is working effectively and as intended. It has the added benefit of helping ensure that the organisation's risk profile is well understood, supporting key stakeholders to focus their attention on areas of where they may add greatest value.

Risk reporting aims to:

- Transparently and effectively communicate risk management activities and outcomes across the Council and to key stakeholders;
- Provide information for robust and informed decision-making;
- Improve risk management activities; and,
- Assist stakeholders exercise their roles and responsibilities with respect to risk management.

Risk reporting should be:

- **Collaborative –** in aligning with other processes and mechanisms across the Council, and also drawing on the insight and expertise of the relevant risk owners and contributors.

- **Evidence based –** in making use of appropriate management information to provide assurance on risk as well as in containing the information necessary for the reader to make decisions or fulfil their role.

- **Focused on the delivery of objectives –** through providing the information required for risk informed decision-making as required.

- **Informative –** through providing a clear understanding of risks, confidence in the assessment of the treatment of risks and the taking of prompt corrective action.

- **Integrated –** through being integrated with other governance processes across the three lines of defence.

- **Tailored –** in being appropriately adapted to the intended target audience.

The **assurance framework** is set and reported annually to Corporate Governance Group, the Audit Committee and the Executive. Its annual reporting gives these groups assurance in their respective governance roles that there is a rich and comprehensive picture of the Council's risk profile. It provides assurance that controls and/or mitigations have been identified or implemented by management, rendering these risks adequately controlled in accordance with the Council's risk appetite.

The assurance framework should be reviewed on a quarterly basis, with amendments and additions made as appropriate.

The **corporate risk registers** – given that they report on current risks of concern and where management attention is being focused – are reported to Corporate Governance Group, the Audit Committee and the Executive on a quarterly basis.

Operational risks are reported to the Audit Committee and Executive where their rating is 'red', as per the risk scoring matrix.

A summary of the Council's risk reporting arrangements is provided in the table below. the table should be read alongside the list of roles and responsibilities relating to risk which is provided in the section that follows.

Output	Reported to	When
The assurance framework (for the next financial year)	Corporate Governance Group The Audit Committee The Executive	As part of Q3 reporting each year, ahead of the next financial year
Strategic risks (for the next financial year)	Corporate Governance Group The Audit Committee The Executive	As part of Q3 reporting each year, ahead of the next financial year
Operational risks (for the next financial year)	Corporate Governance Group	As part of Q3 reporting each year, ahead of the next financial year
The assurance framework (for the current financial year)	Corporate Governance Group	As part of Q2 and Q4 reporting
Strategic risk register – updates	Corporate Governance Group The Audit Committee The Executive	Quarterly
New strategic risks	Corporate Governance Group The Audit Committee The Executive	Quarterly
Operational risk register – updates	Corporate Governance Group To the Audit Committee and the Executive if ‘red’ rated.	Quarterly
New operational risks	Corporate Governance Group	Quarterly

The assurance framework and corporate risk registers are made available to all staff and members of the Council via the Council’s intranet and document portal.

Roles and responsibilities

Effective risk management is founded on well-established and understood roles and responsibilities.

The Council operates a three line of defence model in respect of risk management. The model is predicated on the threefold notion that:

(i) Risk should not be left to risk management specialists;

(ii) Everyone in the Council has some responsibility for risk management; and,

(iii) The varying roles, parts and levels of the Council play different, but complementary, roles within effective risk management. It is the interplay between these roles that determines how effective the organisation is in managing risk and is of fundamental importance to the delivery of effective corporate governance.

The successful operation of the Council's risk management strategy is founded on the roles and responsibilities set out in the sections below. It is organised around the three lines of defence to help illustrate where each function and team resides within it.

It is not intended to be exhaustive, though nevertheless serves as a useful guide to the various roles and responsibilities that are found at the three lines of defence and beyond.

At the first line of defence

Heads of Service and service management (managers/team leaders) will:

- Identify, implement and maintain effective internal controls to manage risk on a day-to-day basis and in accordance with the Council's risk appetite.
- Ensure the ongoing adequacy and effectiveness of identified controls and take any remedial action as required.
- Proactively identify potential risks which could affect the delivery of services and ensure that these are recorded and managed appropriately, in full accordance with the risk management strategy.
- Ensure staff within the service/team understand the potential risks facing the service and wider organisation and that they are aware of how to escalate concerns.
- Ensure that staff are adequately trained in accordance with key service and corporate controls.
- Seek the support from other services as and when required.
- Escalate concerns relating to risk as appropriate.

- Ensure that the appropriate Executive Member(s) is briefed on all key risks facing the service.
- Ensure that risks are considered in all aspects of decision making.
- Ensure that risk is considered as part of the annual service and financial planning process and ultimately that their section within the Council's assurance framework is comprehensive and robust.
- Act in collaboration with other services and/or organisations as appropriate.

Risk owners will:

- Take accountability for the identified risk and its control and/or mitigation, including reporting on progress of risk treatment.
- Act in collaboration with other services and/or organisations as appropriate.

All Council employees will:

- Act lawfully and ethically at all times and within the Council's constitution, scheme of delegation and employee code of conduct.
- Maintain a good awareness of the types of risk that the Council faces.
- Follow all service and corporate risk controls and/or mitigations adequately and faithfully.
- Understand how to identify, report and control and/or mitigate risk in accordance with the risk management strategy.

At the second line of defence

Emergency planning and business continuity will:

- Mitigate risk through the creation of robust emergency plans and operational arrangements that enable the Council to respond to a range of civil emergencies in accordance with its statutory responsibilities.
- Support services to systematically manage the risk of service disruption due to a range of business continuity events, ensuring any weaknesses are understood and that controls and mitigation measures are in place to overcome any disruption and to maintain the delivery of core services as far as is reasonably practicable.
- Support in the recovery from emergency incidents and/or business continuity events.

Democratic Services will:

- Ensure that processes and procedures are designed and implemented allowing decisions to be made and authority exercised in accordance with the constitution and

scheme of delegation, in full conformance with prevailing standards of good corporate governance in local government.
- Maintain the code of corporate governance and annual governance statement.
- Manage the corporate complaints process. Identify where complaints have risk management implications and escalate as appropriately.

Data protection will:

- Ensure that the Council maintains high standards of data protection and information governance and acts in conformance with the Data Protection Act (2018), as well as all other appropriate statutory guidance.

Corporate Policy, Projects and Performance will:

- Maintain the Council's risk management strategy which sets out the Council's overarching approach to the management of risk.
- Support the effective operation of the Council's risk management cycle, including by undertaking quarterly risk management reviews with Heads of Service and Senior Management and reporting on risk to appropriate governance groups, including the Audit Committee and Executive.
- Support service management in their primary risk management role and help coordinate the activities of other services at the second and third lines of defence.
- Support the establishment of effective operational and strategic relationships between risk management and all other corporate governance processes, including annual budgeting and service and financial planning, as well as performance management.
- Monitor and report on corporate and service performance in accordance with the Council's performance management framework. Escalate performance and compliance issues that have a relation to risk management as appropriate.
- Maintaining a comprehensive knowledge of the wider local government policy context and potential risks residing therein. Use this insight to support services in the management of risk.
- Provide training to staff on the Council's approach to risk management.

The Programme Management Office (PMO) will:

- Maintain and ensure the effective operation of the Council's project and programme management frameworks, which helps ensure that projects and programmes are initiated on a sound business case and are delivered efficiently and with due regard to the management of risk.

Finance will:

- Design and apply the Council's core financial controls to ensure that the public money administered by the Council is spent effectively and is appropriately accounted for.
- Maintain the Council's insurance arrangements and ensure that the Council has adequate and proper insurance cover against risks that are faced.

Fraud will:

- Provide a proactive and reactive counter fraud service to support all departments within the Council in cases of suspected internal or external fraud.
- Maintain the Council's anti-fraud and anti-corruption policies, as well as the whistleblowing policy.
- Provide fraud awareness training for staff to help them recognise and report the signs of fraud.

Human Resources will:

- Ensure the ongoing effectiveness of the Council's employment practices and policies and likewise monitor staff and service compliance.

Legal will:

- Provide appropriate legal advice to ensure that the Council acts lawfully in its business.
- Defend the Council's interests if the Council is subjected to legal challenge.

Procurement will:

- Maintain the Council's procurement and contract management strategies.
- Support services to derive best value from contracts and spend.
- Monitor the Council's compliance with the contract procedural rules and all public procurement legislation and requirements.

Corporate health and safety will:

- Provide competent health and safety advice to support services to maintain staff and resident welfare.
- Ensure that accident and incident investigations are carried out, with lessons learned implemented and any required preventive action taken.
- Maintain corporate risk assessments and support services to maintain departmental level risk assessments.
- Regularly review the Council's health and safety management system to ensure its effectiveness and compliance with all legislative requirements.

Information Technology (IT) will:

- Implement and maintain the Council's IT strategy. The strategy sets out the specific measures and controls to protect and defend the Council's systems and data from attack, malicious or otherwise.
- Maintain the Council's disaster recovery plan and procedures to support recovery from an IT security incident or business continuity event.

At the third line of defence

Internal audit will:

- In adopting and following a risk based internal audit plan and charter, identify potential weaknesses in systems, controls and procedures that may expose the authority to risk.
- Operate in accordance with the prevailing public sector internal audit standards.
- Report findings to the Audit Sponsor, Corporate Governance Group and the Audit Committee.
- Produce an annual report and opinion on the overall effectiveness of risk management and control at the Council.
- Use the assurance framework and corporate risk registers to inform the annual risk based internal audit plan.

External audit will:

- Report any concerns relating to risk management arising from the audit of the statement of accounts to the appropriate body.

Governance roles and responsibilities

As noted above, constituted governance bodies and senior management are not considered to reside within a line of defence in the model. Instead, they are key stakeholders that themselves are served by the collective operation of the three lines of defence.

However, each governance body has varying governance roles and responsibilities, the detail of which is set out below.

All Members of the Council will:

- Maintain an awareness of the Council's risk profile and that of the wider sector to aid the fulfilment of their role as local representatives.

- Ensure their awareness and familiarity with key corporate risk controls and/or mitigations, and act in full conformance with them and the member code of conduct.

The Executive will:

- Be ultimately responsible for ensuring that the Council adequately addresses the risks that it faces.
- Delegate the effective, day to day management of risk to officers.
- Ensure that risk is adequately considered in all aspects of decisions taken by the Executive in accordance with the constitution and scheme of delegation.
- Approve:
    - The Council's strategic risks for the forthcoming financial year in Q3 of the current year.
    - In year new risks for inclusion on the strategic risk register.
    - In year closure of strategic risks.
- Receive:
    - The Council's assurance framework for the forthcoming financial year in Q3 of the current year.
    - Quarterly updates on strategic risks.
    - Quarterly updates on red rated operational risks.
- Recommend:
    - That Full Council adopts the Council's risk management strategy following its update and review every three years, or more often if required.

The Audit Committee will:

- Act in conformance with its constitutional responsibilities in respect of risk management.
- Provide independent assurance on the adequacy of the Council's risk management strategy and the internal control environment.
- Provide independent review of the Council's governance, risk management and control frameworks and oversee the financial reporting and annual governance processes.
- Oversee internal and external audit, helping to ensure effective independent assurance arrangements are in place.
- Approve:
    - The annual internal audit plan and charter.
    - The annual external audit plan.
- Receive:
    - The Council's assurance framework on an annual basis.

    - Quarterly updates on strategic risks.
    - Quarterly updates on red rated operational risks.
    - The Council's updated risk management strategy when it is reviewed and updated every three years, or more often if required.
- Make any recommendations relating to risk management to the Executive or Senior Management Team as appropriate.

Corporate Governance Group (comprised of the Senior Management Team and statutory officers) will:

- In acting as the apex of officer governance, hold overall responsibility for the day-to-day management of risks in accordance with the constitution and scheme of delegation.
- Ensure that the Council's risk management strategy is robust, fit for purpose and that it is applied effectively.
- Recommend that:
    - The Executive approves the Council's strategic risks for the forthcoming financial year in Q3 of the current year.
    - The Executive approves any new in year risks for inclusion on the strategic risk register.
    - The Executive approves in year closures of strategic risks.
- Approve:
    - The assurance framework for the forthcoming year in Q3 of the current year.
    - The operational risks for the forthcoming year in Q3 of the current year.
    - Any new operational risks identified in year.
    - The in year closure of any operational risks.
- Receive:
    - Quarterly updates on strategic risks.
    - Quarterly updates on operational risks.
    - Biannual (Q2 and Q4) updates on the assurance framework.

Training and communication

It is imperative that the risk management strategy is underpinned by management and staff competence and awareness; doing so will help ensure the achievement of the strategy's objectives.

All staff and management have a responsibility for being familiar with the core risk management controls within their service and to similarly be aware of the Council's overarching risk management strategy.

Service management are responsible for ensuring that staff receive adequate support and training to complete their duties safely and in accordance with all corporate, service and other statutory risk controls.

The Council's Projects and Business Assurance Team is responsible for providing appropriate training and guidance on the risk management strategy to managers as required.

The following will be provided by the Projects and Business Assurance Team:

- An annual briefing to all staff on risk management and the risk management strategy;
- An annual briefing to Heads of Service and the Senior Management Team on risk management and the risk management strategy; and,
- Any additional ad-hoc training as required and requested by Senior Management/Corporate Governance Group.

The Projects and Business Assurance Team undertake quarterly risk management reviews with Heads of Service which are to be used as an opportunity to discuss the overarching approach to risk management, as well as the specific operation of the risk management cycle.

The risk management strategy and methodology is made available to all staff via the intranet. It will be made available to members via the ModGov document library. It will also be published on the Council's website.

Corporate risk registers and the assurance framework will be made available to all staff via the intranet. They will also be made available to members via the ModGov document library.

The risk management strategy will form part of the essential reading for new staff as part of the induction process.

Future review

The risk management strategy and methodology will be subject to a substantive review every three years at a minimum.

The review will include all aspects of the Council's approach to risk management, including the risk appetite statements and the thresholds set out therein. Regular review is crucial to ensuring that the strategy remains relevant to the Council, its risk profile and wider corporate and management structures/processes.

An administrative review will be carried out on an annual basis.