Reigate & Banstead Borough Council

Risk management methodology

2026/27 to 2028/29

Contents

Introduction

The risk management methodology gives practical guidance on how to apply the principles and meet the objectives set out in the Council's risk management strategy.

It explains the roles and responsibilities involved in managing risk across the Council, aligned with the three lines of defence, and describes the processes that make up the Council's risk management cycle.

Designed to mirror the structure of the overarching strategy for ease of use, the methodology is intended for managers at all levels and for the Projects and Business Assurance team, who support the delivery 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 management and the Council empowers 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 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 (SMT), 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 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 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 including 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.

Because not all risks can be foreseen and controls may fail unexpectedly, the first line of defence needs support from additional systems and oversight. This support comes from the second line of defence, which monitors compliance with standards, reviews whether policies and procedures are appropriate, and are being followed.

The third line of defence consists of internal and external audit. Internal audit independently evaluates how well risks are identified and managed across the first and second lines, highlighting weaknesses in systems and controls, while management remains responsible for addressing them. External audit focuses on the accuracy of the Council's annual accounts and informs stakeholders of any significant issues, including those relating to governance and risk management.

Recording risks

The Council holds two risk registers:

Strategic Risk Register

- Covers risks affecting **medium to long-term objectives**, such as those in the Corporate Plan and Medium-Term Financial Plan.
- Includes significant external risks or major internal activities (e.g., key projects).
- Managed jointly by the **SMT** and **Executive Members**.

Operational Risk Register

- Captures risks arising from **day-to-day service delivery**.

- A risk is added when it cannot be controlled at service level or exceeds the Council's risk appetite.
- Managed by **Heads of Service and service managers**.

Purpose and Distinction

- Risk registers contain **active, uncontrolled, or insufficiently mitigated risks**, often representing specific manifestations of broader principal risks.
- In contrast, the assurance framework provides a **comprehensive high-level overview** of all theoretical principal risks for awareness and oversight.
- Registers operate on a **"by exception"** basis; risks remain listed until brought within acceptable levels.

Governance Roles

- The Corporate Governance Group (CGG) maintains the assurance framework and oversees the operational risk register, adding or closing risks as required.
- The Executive approves the strategic risk register and any changes to it, informed by CGG and Audit Committee feedback.
- Red-rated operational risks are escalated to the Executive.

Relationship to Other Documents

- Together, the assurance framework and corporate risk registers provide a **comprehensive and well-understood risk profile**, supporting effective governance and control.
- Specific risks may also appear in other documents (committee papers, project logs, health and safety reports).
- The assurance framework captures **high-level principal risks**, while the registers record **live risks** requiring focused action.

Describing a risk

When a risk is identified, it must be described clearly so that its causes, consequences, and required controls or mitigations are fully understood. A good risk description should be concise but provide enough information to explain **what might happen**, **why it might happen**, and **how it could impact objectives**. Specifically, it should:

- **State the cause** – the context, background, or event that gives rise to the risk.
- **State the consequences** – the potential impacts if the risk materialises, with particular focus on effects on the Council's objectives.

Each identified risk must also be assigned a **risk owner**. A risk owner is the officer (usually a Head of Service or a SMT member) and the relevant Executive Member who are ultimately accountable for managing the risk, ensuring controls and mitigations are in place.

Risk owners should be kept to the minimum necessary to ensure clear accountability, although cross-cutting risks may require more than one. While operational responsibility for

actions may be delegated to other teams, the officer risk owner must have the authority and seniority to allocate resources and prioritise actions in line 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

The Council uses a formal risk appetite statement to clearly communicate the level of risk it is willing to accept. This statement provides a foundation for effective risk management and internal control. The Council's appetite varies across different categories of risk, recognising that some areas require a cautious approach while others allow for greater flexibility. These distinctions help form a holistic view of risk and support consistent decision-making.

Risk appetite statements guide the Council in two main ways: assessing appropriate responses to risks that affect corporate objectives and understanding the risk implications of decisions about whether to pursue particular actions. Defining risk appetite also clarifies when risks should be escalated for wider consideration. It is intended as a guide rather than a strict limit, encouraging balanced and well-informed judgement.

The Council's risk appetite can be expressed across a spectrum, from averse to eager, each associated with particular behaviours and attitudes toward risk, as summarised below:

Appetite	Typical behaviours
Averse	A preference for avoiding risks and activities giving rise to risk, could be referred to as 'playing it safe'. Inherent risks will be controlled as far as is feasibly possible. This may mean incurring expense associated with doing so, ceasing certain activities and/or the loss of potential opportunities arising from inaction. Risk aversion is also characterised by a strong desire for full certainty in decision-making related to risk.
Cautious	A preference for options and activities that have a low degree of inherent risk, and a preference for high levels of certainty of achieving successful outcomes in any actions or opportunities involving risk. Risk and uncertainty will generally be avoided. If it can't be, it will be controlled and/or mitigated to a level that significantly reduces the risk of negative outcomes, although these are still possible. Innovation and transformation are generally avoided if marked by high degrees of uncertainty and will only be pursued if a successful outcome is highly likely.

Appetite	Typical behaviours
Open	Prepared to take calculated risks where successful outcomes are reasonably expected, particularly where appropriate controls and mitigations are in place to help secure them and to control the inherent risk. Risk openness seeks to strike a more even balance between risk and reward. Risk does not stop the pursuit of opportunity, innovation and change. Rather it prompts the control and mitigation of risk to a level that is acceptable and which, on balance, minimises negative outcomes (in whole or in part). Failure is therefore possible though not reasonably expected.
Eager	Risk is positively embraced in pursuit of significant reward, and failure is expected and tolerated. Change, innovation and transformation are actively pursued, despite the possibility of the anticipated benefits not materialising or investment proving abortive.

Risk and the Council's tolerance for it must be considered in all decision-making, not only during formal risk reviews. A clear and well-communicated risk appetite ensures proportionate and consistent decisions, supports effective governance, and helps ensure that risks taken are appropriate to the opportunities or benefits being pursued.

A well-defined risk appetite helps the Council to:

- Embed risk considerations into everyday decisions.
- Ensure responses to risks are balanced and proportionate.
- Promote consistency across services.
- Align accepted risks with potential rewards.
- Improve corporate oversight across diverse risk areas.
- Tailor controls and mitigations to the level of risk faced.

Because risks vary in nature, the Council's risk appetite is segmented by risk category. These categories include:

- **Environmental** – impacts of services or investments on the environment.
- **Financial (revenue)** – pressures on income, budgets and external funding changes.
- **Financial (capital)** – risks relating to assets, infrastructure and investment portfolios.
- **People & Communities** – risks affecting residents' needs, social outcomes, or public trust.
- **Corporate objectives** – risks that threaten delivery of the Corporate Plan or strategic priorities.
- **Operational** – risks linked to day-to-day service delivery, organisational resilience, workforce, statutory compliance and health & safety.
- **Legal/reputational** – risks of legal challenge, sanctions, regulatory change or reputational damage.

- **Technological** – risks involving data security, system integrity, digital capability, system change, and cyber awareness.

Risk Appetite Statement

The Council generally adopts a cautious approach to risk but recognises that achieving strategic objectives sometimes requires accepting higher levels of risk in certain areas where necessary and justified.

- The risk appetite is reviewed every three years as part of the broader review of the risk management strategy.
- Appetite statements apply to residual risk, meaning the level of risk remaining after existing controls and mitigations are 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 where we can demonstrate clear benefits of accepting this risk when weighed against other considerations and other risks. Tolerable risks could take the form of direct negative outcomes for the environment or delays to our commitment of reducing emissions and environmental impacts; however, any accepted risks will only be local and generally short term in their nature.
Financial – revenue	**Cautious**	We will only take measured risks and prefer initiatives where we can be confident in positive outcomes or where the risk of financial loss is minimal and/or minimised.
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 will do so in a controlled manner and weighted against other considerations and categories of risk.
People and communities	**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	**Cautious**	We will set realistic and achievable targets given the organisation's capacity and resourcing levels and, as such, we expect them to largely be achieved. However, we accept that there are risks that may delay the delivery of our objectives, though we aim to control and/or mitigate these to a level that is reasonable.

Risk category	Appetite	Risk appetite statement
Operational	**Open**	We accept that change initiatives carry short-term risks of compromising some operational areas and service delivery for a generally limited time. Exceptions are health and safety of staff and residents, and any statutory duties we hold, where there is a very low (averse) appetite for risk of lapses or non-compliance.
Legal/ reputational	**Cautious**	We will act lawfully and in conformance with established standards and codes of regulation as it is the right thing to do. We are also reluctant to incur the risk of reputational damage or external sanction. As such, we will generally err on the side of caution. Where reasonable and ethical, we are prepared to explore areas of opportunity within legislation and codes of regulation, and we are willing to defend our position where challenge could occur.
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 - and will take account 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. To apply the risk appetite effectively and ensure it guides decision making, the overall risk appetite must be underpinned with individual 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 negligible impact on the local environment	Short term minor local impact with no ongoing negative effects **(3)**	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 **(3)**	1-2% of the capital programme **(3)**	>2% of the capital programme **(2)**
People and communities	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 **(3)**	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 **(2)**	40-60% variation. Reconsideration of viability of corporate objectives **(1)**	>60% variation. Unable to deliver objectives. Failure to meet community needs **(1)**
Operational	Little to no impact to service delivery	Failure to meet standard customer expectations and needs	Failure of several non-statutory services **(3)**	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 on how to apply this.

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.

[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 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**

1. **Inherent Risk –** This is the level of risk before any controls or mitigations exist, measuring the raw likelihood and impact of the risk occurring. Controls reduce likelihood; mitigations reduce impact. The assessment must be carried out with the risk owner and relevant service area.

2. **Current Risk –** This reflects the risk after existing controls and mitigations are considered, controls and mitigations work together and are not mutually exclusive. The assessment must be evidence-based and proportionate, acknowledging any limitations, it should involve the risk owner, the relevant service, and – where useful – sources such as internal audit or external assurance. All controls and mitigations must be recorded on the Council's assurance framework. Current risk must be evaluated against the Council's risk appetite using the scoring matrix as a guide, with managerial judgement applied where information is uncertain. The highest-impact category should be used when scoring:

- If the score is within risk appetite → record it for later review.
- If outside risk appetite → consider adding it to the corporate risk register.

Guidance on additional risk treatment options follows in the next section of the document.

1. **Target Risk –** This defines the desired end-state of the risk after management action. It must be documented for all identified risks. It should be set with reference to risk appetite and reflect a realistic level of influence the Council has. Target risk is used to evaluate whether current and proposed controls/mitigations are adequate. Some risks may always remain above target due to limited ability to influence them; these should still be documented to maintain a complete risk profile.

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

Risk owners are responsible for treating risks to ensure they remain within the Council's risk appetite, primarily by designing and implementing SMART actions that reduce either the likelihood or impact of the risk. These actions must be regularly monitored and reported.

Before choosing how to treat a risk, risk owners should conduct an options appraisal to identify the most effective approach. While this appraisal does not always need formal documentation, it should be recorded when costs are high, risks are significant, or wider governance processes require it. Support is available from the Council's Projects and Business Assurance team and other second-line services.

The appraisal should consider four treatment options:

- **Avoid** the activity causing the risk (where feasible and consistent with objectives)
- **Transfer** the risk (e.g., insurance or contractors)
- **Reduce** the likelihood or impact through new or improved controls
- **Accept** the risk, if unavoidable or outside the Council's control

A combination of these approaches may be appropriate. Costs, resources, timing, and both financial and non-financial benefits must be evaluated, ensuring alignment with the Council's risk appetite. Costs alone should not drive decisions; actions must be proportionate, lawful, effective, and ethically sound.

When selecting treatments, risk owners must clearly define implementation plans, including rationale, expected benefits, actions required, responsibilities, resources, performance indicators, timelines, and dependencies. All chosen treatments and controls must be recorded either in the assurance framework (for well-controlled principal risks) or the corporate risk register (for active risks requiring detailed mitigation).

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 primarily the responsibility of first line management, supported by the Council's wider risk management strategy. Service managers must design and run effective monitoring processes as part of day-to-day operations, with specialist support from the second and third lines of defence.

First-line monitoring activities include:

- Tracking trends, KPIs and other indicators that may signal changes in risks or controls.
- Conducting or commissioning deep-dive reviews into specific risk areas.
- Learning from incidents, issues and sector best practice.
- Testing how well current controls and mitigations work.
- Horizon scanning for external changes using tools such as PESTLE.

The **assurance framework** and **corporate risk registers** are the Council's primary tools for monitoring risk and must be reviewed **quarterly** (and more frequently if needed). The **Projects and Business Assurance team** supports these reviews.

Each quarterly review assesses:

- Whether risks are still accurately described.
- The effectiveness and accuracy of current controls.
- The correctness of inherent, current and target risk scores.
- Whether further action or escalation is needed.
- Whether any new risks have emerged.

Because not all risks are foreseeable and environments can change quickly, first line teams rely on additional oversight from the **second and third lines of defence**.

Second line of defence provides policies, frameworks, tools and monitoring, offering assurance on how well risks are being managed. It can escalate concerns directly to senior management via the Corporate Governance Group.

Third line of defence consists of independent assurance, mainly via **internal and external audits**:

- **Internal audit** gives an objective opinion on governance, risk management and internal controls, using the assurance framework and risk registers to direct its work. Findings are reported to the Corporate Governance Group and Audit Committee and may lead to updates to risk registers.

- **External audit** verifies the Council's accounts and reports any significant governance or risk issues, which management and political leaders must then address.

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 three lines of defence.

However, each governance body has varying governance roles and responsibilities.

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 & mitigations, and act in full conformance with them and the member code of conduct.

The Executive will:

- Be responsible for ensuring that the Council adequately addresses the risks 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:
    - 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.
    - 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.
- Independently review 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 SMT.

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

- In acting as the apex of officer governance, hold 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 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.
    - 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.
- Annual (Q3) updates on the assurance framework.

Training and communication

Effective risk management depends on staff and management competence and awareness of their service-level risk controls and the Council's overarching risk management strategy.

Responsibilities:

- All staff and managers must understand the key risk controls relevant to their service and be familiar with the Council's risk management strategy.
- Service management must ensure staff receive the training and support to carry out their duties safely and in line with corporate, service and statutory requirements.
- The Projects and Business Assurance Team is responsible for providing training, guidance and support to managers.

Training and Briefings Provided:

- An annual briefing for Heads of Service and the Senior Management Team.
- Ad-hoc training when requested by Senior Management or the Corporate Governance Group.

The Projects and Business Assurance Team also uses quarterly risk management reviews with Heads of Service as opportunities to reinforce the risk management approach and discuss the operation of the risk cycle.

Access to Key Documents:

- The risk management strategy and methodology will be available on the intranet, the ModGov document library for members, and published on the Council's website.
- Corporate risk registers and the assurance framework will also be accessible to staff via the intranet and to members via ModGov.

Finally, the risk management strategy will be required reading for all new staff as part of the induction process.

Future review

The risk management strategy and methodology will be subject to a 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.