GUILDFORD BOROUGH COUNCIL

RISK MANAGEMENT METHODOLOGY

2025/26 to 2028/29

GUILDFORD BOROUGH

Waverley BOROUGH COUNCIL

Contents

Introduction 4
The risk management cycle 5
Identifying risks 5
Questions to consider 9
Recording risks 11
Describing a risk 15
Assessing and analysing risks 17
Risk appetite 17
Risk appetite statements 23
Risk assessment – analysing and evaluating impact and likelihood 26
Risk assessment and deterministic planning 33
Risk treatment 38
Actions and options 38
Risk monitoring and reporting 41
Risk monitoring 41
Risk reporting 43
Reporting schedule 47
Roles and responsibilities 48
At the first line of defence 48
At the second line of defence 49
At the third line of defence 53
Governance roles and responsibilities 54
Training and communication 57
Future review 58

Version control

Approved by	
Date approved	
Review date	

Introduction

This document describes the underlying processes, procedures and roles and responsibilities necessary for applying the principles and objectives of the council's risk management strategy.

As with the strategy, this methodology has been prepared in accordance with UK Government Orange Book guidance. The Orange Book outlines the principles and concepts of risk management for the public sector and aims to help these organisations develop and implement effective risk management processes.

Risks can relate to:

- The chance or probability of an event occurring and its potential consequences; and,
- Assumptions concerning an independent variable (such as anticipated customer numbers, users, completion dates, inflation etc.) which should be understood and articulated and, where possible, quantified. This has particular relevance in the project and programme management environment, though is also applicable to activities such as service and financial planning.

As the strategy notes, risk management is the set of coordinated activities that are designed and operated to manage risk and exercise internal control within an organisation. In accompanying the strategy, this methodology defines how the council identifies, assesses, manages, monitors and reports on the risks it faces in delivering its objectives. Its aim is to ensure the integrity of the discipline of risk management to all council activities, decision making and governance, as well as fostering and promoting a mature risk culture.

It is primarily a document for the council's management and staff, as well as the Strategy and Performance Team who provide day to day support to the achievement of the council's risk management objectives. As a core component of the council's risk management framework, it should be read alongside the risk management strategy and follows a similar structure for the ease of use and reference.

The risk management cycle

There are four stages in the council's risk management cycle: **identification, assessment, treatment and monitoring and reporting.**

The cycle is a structured approach for managing uncertainty and ensuring that risks are well understood, appraised and considered consistently, as well as being managed and monitored effectively.

The ultimate aim of the cycle is to enable effective corporate governance through supporting the leadership of the council to determine and continually assess the nature and extent of the risks that the organisation is exposed to and is willing to take to achieve its objectives, and to then ensure that planning and decision making reflects this assessment. When implemented and followed well, the cycle ensures that risk is considered and managed in all areas of council business and decision making, leading to better outcomes.

Each stage of the cycle is considered in greater detail in the sections that follow, though at this point it is worth noting that, whilst it may appear to be a sequential and linear process, it is, in fact, a dynamic and iterative one, with each phase overlapping and requiring continual revisiting and review. This is because the environment that the council operates within is continually shifting and highly uncertain, with new risks continually emerging and existing risks often changing in nature. Being adaptive and iterative helps maintain organisational agility and resilience and a high degree of risk awareness, with responses to risks tailored as circumstances and available information change.

Identifying risks

Risk identification is the first key step in the process of building an organisation's risk profile and developing risk awareness, as well as ensuring that risk is managed effectively.

As noted in the accompanying strategy document, the council shares the UK government's Orange Book definition of risk as the effect of uncertainty on objectives.[1] This means that risk encompasses any uncertainty that could impact the achievement of the council's priorities and objectives as set out in the policy framework, with the Corporate Strategy and Medium Term Financial Plan at its apex. Risks should be identified regardless of whether they are under the council's direct control; even ostensibly 'minor' risks could, when combined with particular events and conditions, have the potential to have significant implications on the council.

[1] The Orange Book: Management of Risk – Principles and Concepts. Available from: https://www.gov.uk/government/publications/orange-book

Risks should therefore be considered at all levels of the council and in all aspects of decision making, including in setting priorities, objectives and deploying resources. Under the council's adopted three lines of defence model, the identification and management of risk is the primary responsibility of service management at the first line of defence. This role should be supplemented by teams at the second and third lines as necessary and in accordance with the roles and responsibilities defined later in this document, as well as in conformance with established industry standards of best practice.

Examples of situations where risk should be considered include:

- As part of the **usual course of service and department management** (by the first line of defence), where management is expected to design and manage their services to reduce risk as part of business-as-usual arrangements. This includes undertaking any departmental/operational specific risk identification activities, as well as considering how to best design and deliver services to reduce risk and potential losses to the council.

- During the **annual service and financial planning process** where service objectives are defined and which, in turn, informs the council's annual budget and delivery plan. As part of this process, risks facing services should be considered and documented in service plans, with corresponding controls and mitigations also defined. Risks identified in service plans should then form the basis of service risk registers, maintained by management as part of their role at the first line of defence. Service risks that fall outside the council's appetite should be considered for inclusion on a corporate risk register, by the agreement of the Corporate Leadership Board (CLB).

- On a **quarterly basis** alongside the Joint Leadership Team and Corporate Leadership Board, where service and corporate risk registers are reviewed to establish whether any substantive changes have occurred, thereby requiring a change in management response.

- During the **annual update to 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 in the context of the authority's overall financial health and sustainability.

- When developing and implementing any **policy or strategy**. As part of robust policy and strategy development, consideration must be given to how the council's objectives may be adversely affected by risk, with appropriate action planned to control and/or mitigate as necessary.

- Throughout the **project, programme and portfolio management life cycle.** Considering and identifying risks and designing treatment options is particularly

important when assembling a business case, as any decision to commit resources should encompass a thorough consideration of its attractiveness in the context of uncertainty and achievability. A detailed analysis of the factors potentially giving rise to risk is appropriate in significant and complex projects and programmes, which is considered in greater detail below.

There are a variety of techniques and methodologies available to management that can be used to identify risks. These include:

- Analysis of previous events, losses and incidents, including any lessons learned that give insight into future potential sources of risk. This includes those experienced by this council, as well as other organisations and for which information exists or is shared;
- Analysis of near misses, defined as events and/or circumstances that didn't cause harm or damage but nevertheless have the potential to in the future. Near misses must be recorded for this to be effective, however, and should be subject to regular review;
- The undertaking of analytical activities (such as the analysis of data) and/or deep dive reviews into departments or functional areas of activity to determine whether potential risks are present or forecast, knowingly or otherwise;
- Industry/sector best practice, guidance and/or policy updates, the implications of which may be positive or indeed negative on the council;
- Facilitated workshops with internal and external stakeholders, enabling a rounded discussion to take place on risk and potential responses, though in depth, specific explorations of risk may also be conducted; and,
- Interviews with internal and external stakeholders, allowing, where necessary, an in depth, exploration of risk to take place.

While under the three lines of defence model the first line is responsible for the management of risk, the latter techniques and methodologies are also often carried out by functions at the second line of defence, the role of which is summarised in greater detail below.

Further, when identifying risks it is also useful to consider the areas from which risk may emerge. In this vein, **PESTLE analysis** is a valuable tool for risk identification in providing a scheme for a comprehensive overview of the external environment and how potential threats arising from it may affect the council. By examining **political, economic, social, technological, legal and environmental factors**, we are able to gain an insight into the various forces and sources of threats that may create risk.

Indeed, one of the key benefits of PESTLE is its ability to identify emerging risks. Changes in the political environment, prevailing economic conditions, or technological advancements and changes can introduce new risks that need to be managed or addressed in a different way. By regularly conducting a PESTLE analysis, the council is able to stay informed of these changes,

their interlinking causes and impacts, and adapt their risk management response accordingly. Being proactive enhances resilience and the ability to respond effectively to external threats.

PESTLE analysis also aids in strategic planning by providing a structured approach to understanding the external environment. The insights gained from this analysis enable better decision-making, allowing organisations to anticipate potential challenges.

The factors of PESTLE are:

Political	Factors arising from the political environment, including the national, local and regional. It includes changes in policy and potential instability, as well as how politically led decisions may have potentially negative effects.
Economic	Factors that refer to the economic conditions and background and which effect the council's operations and performance. This includes economic growth, inflation, the fiscal environment, interest rates, exchange rates and the cost of living. It should be noted that prevailing economic conditions also affect resident and business behaviour, and also affect the council's cost base.
Social	These factors encompass societal trends and behaviours, such as demographics, lifestyle changes, and cultural attitudes. Social factors often result in changing needs, expectations and preferences from residents and customers.
Technological	The development and impact of technology both on business operations and on customer/stakeholder expectations. It includes technological innovations and improvements, as well as risks arising from its use, intended or otherwise.
Legal	Changes in the legislative and/or regulatory environment that the councils operates within.
Environmental	Refers to aspects such as climate change, environmental regulations and sustainability practices, and how these may affect, or be affected by, the council's operations.

A PESTLE analysis should be carried out by each service at least annually and as part of the service and financial planning process to support service design and delivery.

However, not all risks are reasonably foreseeable or evident. Likewise, many risks are inherent and ever present, where the environment within which they exist may drastically shift without

warning. Further, previously robust controls and mitigations may fail or degrade, significantly changing the internal control and risk environment.

With the latter in mind, it is crucial that that first line of defence is supported by other systems, processes and best practice to proactively identify risks or the deterioration of controls so that corrective management action may be taken. This support is provided by the second line of defence, whose role is to define standards and ensure compliance through the operation of robust policies and procedures, the totality of which is often referred to as the 'internal control environment'.

The second line of defence will assess service and departmental 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 are set at an appropriate and proportionate level, and whether they are being consistently met.

Roles and responsibilities are set out in the roles and responsibilities section of this methodology document.

The second line of defence is supplemented by the work of the third line of defence, comprised of internal and external audit, as well as any specialist consultancy commissioned by the council to provide assurance.

An independent internal audit function will, through following a risk-based approach to its work, provide an objective evaluation of how effectively the council manages its risks, including the design and operation of the first and second lines of defence. All risks faced by the council are within the scope of internal audit.

In so doing, internal audit's role is to identify weaknesses (potential or otherwise) in systems, controls and procedures that may expose the council to risk. While internal audit identifies these weaknesses, it is the responsibility of management to design and implement actions that address them and, as a result, control and mitigate risk.

External audit is responsible for reviewing and verifying the council's annual statement of accounts. External audit has a duty to inform key stakeholders of any matters of importance that arise from their review, including governance and risk management concerns.

Questions to consider

When identifying risks the following interlinked questions should be considered:

- **What** could happen?

What activities do we carry out that have the potential to cause harm or create risk? What might go wrong? Or what might prevent the achievement of our objectives or outcomes? Both the internal and external environment should be considered, and particularly how they invariably interrelate.

- **How** could it happen?

  What circumstances – or combination thereof – could cause the risk to materialise? Is there a particular cause event or chain of events?

- **Where** could it happen?

  Could the risk occur in any particular location? Or is it location, situation or activity specific?

- **Why** might it happen?

  What factors would need to be present for the risk to materialise? Is there a causal chain that should be understood to help break, influence or mitigate it?

- **What** are the potential consequences?

  If the risk were to materialise, in whole or in part, what are the consequences on our objectives and outcomes? Will the impacts be felt within a particular service area or team, or are wider organisational impacts expected?

- **Who** can influence the risk and outcome?

  To what extent is the risk within the council's control or influence to manage? Do management activities rely on a wider, coordinated cross council response? Is there a need to work with external partners and stakeholders? This is particularly important to understand when considering risk treatment options, considered later in this document.

- **Who** is accountable?

  Who owns the risk and is therefore accountable for its management?

Recording risks

Once a risk has been identified it should be recorded for wider awareness and visibility across the council.

The council has two core mechanisms for maintaining corporate awareness and visibility of risk:

1. Service risk registers
2. Corporate risk registers (strategic and operational)

Service risk registers

Each service should have a risk register that documents the principal risks faced and which are reasonably foreseen as part of service planning and the usual course of management.

Service risk registers cannot be expected to identify every risk faced in specific detail. Rather, it is expected that they should focus and group risks by high level category – or 'principal risk' types – for the ease, clarity and effectiveness of analysis as well as subsequent monitoring and reporting. Doing so will help provide assurance that the council is aware of the risks it faces.

Specific, or 'live', examples of principal risks should also be recorded on service risk registers.

Example principal risk areas include:

- Data protection and information governance (i.e. data breaches and/or misuse of data, personal or otherwise)
- Cyber security
- Governance and decision making
- Management (systems and processes)
- Legislative and regulatory requirements and/or changes
- Organisational/departmental capacity
- Projects and programmes
- Safeguarding
- Health and safety
- Business continuity
- Suppliers and supply chains
- Contracts
- Fraud (internal and external)
- Market factors
- Civil emergencies

Service risk registers should be compiled annually as a key output of the council's service and financial planning process, which culminates in the adoption of the council's annual budget.

Service risk registers should be reviewed at least quarterly by management. They form the basis of regular conversations between the Strategy and Performance Team and service management on risk, with new risk areas identified as necessary.

Corporate risk registers

The council maintains two corporate level risk registers:

1. **Strategic risk register –** risks that could have a negative impact on the council's medium to long-term objectives and priorities as articulated in the Corporate Strategy, medium-term financial plan or other corporate level policies and/or strategies. Strategic risks typically originate from the environment within which the council operates, though may also stem from an internal source – such as a major project – if the potential impact merits its categorisation as a strategic risk.

   Members of the Corporate Leadership Board and Executive members have a shared responsibility for strategic risks.

2. **Operational risk register –** risks that are encountered or faced in the delivery of services and which impact service objectives. Operational risks are ordinarily managed as part of the usual course of management by services. Where a risk cannot be managed within the service and requires a wider degree of corporate awareness/oversight, it should be considered for inclusion in the operational risk register.

   Assistant Directors and service managers have responsibility for operational risks.

Corporate level risk registers should set out risks of concern – that is, operational and strategic risks that fall outside of the council's risk appetite. In this way, risks on the corporate risk registers are best thought of as specific manifestations of principal risks and which present a threat to the council until they are sufficiently controlled and/or mitigated. These risks may 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.

Risks will remain on the appropriate corporate risk register until they are managed to the desired level, in accordance with the council's risk appetite.

Further detail is provided on risk monitoring and reporting in the sections that follow. At this point, however, it is worth noting that:

1. The **Corporate Leadership Board (CLB)** maintains oversight of service risk registers, as well as the corporate (operational and strategic) risk registers. This includes their annual compilation. CLB receives regular updates on risk as part of the leadership and governance role of its members.

2. The **Executive** is ultimately responsible for approving the strategic risk register and key changes made to it during the year – which is mainly closing and opening risks – following recommendations made by CLB and any observations made by the Corporate Governance and Standards Committee.

3. The **Corporate Governance and Standards Committee** receive quarterly updates on corporate risks.

It should also be noted that risks may also be captured in other key corporate and management documentation, including in committee reports, project and programme risk registers and health and safety reports, amongst others. Corporate and service level risk registers are therefore not the sole repository for the documentation of risks, though, if compiled well and kept up to date, they should serve as comprehensive guides to the risks faced by the council and those that are receiving active management attention.

Project, programme and portfolio risks

As previously noted, when confirming investment in change initiatives – delivered via portfolios, programmes and projects (often termed P3M) – consideration should be given to whether doing so is attractive and viable in the context of risk and uncertainty.

In the change environment there is considerable variability in the nature of risks faced and their impact, including how such impacts can accumulate over time and, indeed, impact in different ways across the change portfolio. Understanding this is fundamental to developing and agreeing a business case and, once complete, supports management to undertake a managed and proportionate response to risk given its inherent nature, which is exacerbated in the change environment.

As such, when portfolios, programmes and projects are initiated it is important that the varying nature of risks are considered and captured on portfolio, programme and project risk registers, with an appropriate degree of analysis and aggregation undertaken to ascertain the overall impact on the council, as well as across these three horizons. Each risk register should therefore capture the risks reasonably foreseen as part of planning and delivery, and, as with the process described in this methodology, consider the controls and mitigations that are in place and carry out further such work if, based on the risk assessment, this is required.

It is important that risks are kept under continual review throughout the P3M lifecycle to ensure that consideration of risk underpins decision making and, where necessary, project, programme and portfolio risks are escalated for inclusion on the relevant corporate risk register as described above.

Additional information on the portfolio, programme and project lifecycle – including risk management activities – is contained in the council's programme management framework.

The differing level of risk registers should, in turn, reflect the differing nature of risks, and their impact, across these three domains.

In summary:

1. **Project risk registers –** capture risks that could impact the successful delivery of a particular project. The focus is on ensuring that the project delivers in accordance with the agreed business case and the agreed outputs. While its core reference point for success (or failure) is the project's deliverables and outputs, consideration should also be given to how any risks to these may affect the council more widely.

2. **Programme risk registers –** consider risks that affect programmes, a collection of projects that, taken together, deliver outcomes of benefit. Programmes are designed to achieve strategic objectives by coordinating several projects. Programme level risk registers must therefore consider the risks that could affect the overall benefits and outcomes of the programme. In this way, programme level risk registers may be thought of as residing at a higher level of abstraction than project risks. Consideration should be given to how, with this wider reference point, risks that threaten programme outcomes may require wider attention and inclusion on service and/or corporate risk registers.

3. **Portfolio risk registers –** are more strategic in nature and consider risks that could impact the entire portfolio of programmes and projects. The council's portfolio of change projects and programmes is set with reference to the five corporate strategy priorities.[2] There is a close overlap with portfolio risk registers and the corporate risk register, though a key distinction is that portfolio risk registers should record all risks reasonably foreseen to the successful delivery of the portfolio. Corporate risk registers are for risks that are outside of the council's appetite.

[2] Available here: https://www.guildford.gov.uk/corporatestrategy

Describing a risk

Once a risk has been identified it should be described. In accordance with the UK government's Orange Book methodology, risk descriptions should be expressed in terms of causes, potential events and their consequences or impacts.

A risk description should contain the following core elements:

1. **A cause –** a cause is the origin of the risk and the reason why it exists and presents a threat or danger. Put differently, a cause is an element which alone or when combined with another (known or otherwise) has the potential to give rise to a risk.

   For example – an important system used by a council department is going out of technical support.

2. **An event –** this is the risk itself. An event is an occurrence or a change in a set of circumstances. It can be something that is expected which does not happen or something that is not expected but does happen. Events often have multiple causes and consequences and can affect multiple objectives.

   For example – (i) increased unplanned system downtime and reduced system reliability; (ii) reduced security standards as new threats emerge.

3. **A consequence –** this is the outcome or the effect of the risk and which affects objectives. Consequences can be certain or uncertain, can have positive or negative direct or indirect effects, can be expressed quantitatively or qualitatively and can escalate through a series of cascading and cumulative effects to varying degrees of certainty.

   For example – (i) residents are unable to access an important service, poor standards of customer service and reduced satisfaction levels; (ii) a data breach or compromised network security, risking a fine and wider security issues.

In describing risks, the stating of consequences without their causes should be avoided. One should also avoid defining risks with statements that are simply the converse of objectives. Indeed, stakeholders and decision makers require a clear articulation of the risk, and the factors that can cause and//or contribute to it, to understand its nature and consequences. It is particularly important for identifying controls and mitigations, as well as designing risk treatment options – both of which are considered in greater detail below.

The assessment of consequences and impact is done with reference to a series of categories, namely: political, financial (revenue and capital), social, technological, legal/regulatory, environmental, reputational and corporate objectives. Information on evaluating the likelihood and impact of risks is considered in greater detail in the sections that follow.

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. This means that 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 members of the Joint Leadership Team.

The risk owner(s) may not have primary operational responsibility for implementing controls and/or mitigations related to the risk which, in accordance with the council’s management structure and scheme of delegation, may be delegated to another team or department. However, the officer risk owner is ultimately accountable for the risk and its mitigation and should therefore have sufficient authority to direct and prioritise responses to risk in accordance with the council’s risk appetite.

To support clear lines of ownership and accountability, there should be as few risk owners as necessary. However, some risks that are cross cutting in their nature may necessarily have more than one owner.

Assessing and analysing risks

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

Risk appetite

As we have seen, risk is inherent and ever present – the council therefore cannot be risk averse and be successful. While the risk management strategy and methodology defines the activities that, when operated together, identify and help manage uncertainty, a key underlying consideration guiding risk management activities is the concept of risk appetite.

Simply put, risk appetite is the level of risk that an organisation is prepared to accept or be exposed to in pursuit of its objectives; it supports the striking of the right balance between risk and reward.

Given that risk is inherent and that its management is routine and part of day-to-day activities for staff across the council, defining our risk appetite (and its limits) is chiefly about identifying at what point decisions regarding the management of risk are escalated for wider visibility and awareness.

Risk appetite is therefore a crucial part of the framework within which decisions are made at the council. Its articulation helps establish the accepted boundaries for risk taking and ensures that accepted risks are proportionate to the possible rewards and the achievement of corporate objectives. Our appetite for risk should not be static, inflexible or applied as a rigid target. Rather, it should serve as a guide to the levels of risk that the council is willing to take if supported by a strong consideration of all relevant factors.

To maximise the benefit of the use of risk appetite in decision making, the following core principles must be recognised:

1. While desirable in the abstract, **it is often not possible to manage all risks to the desired level.** Resources are finite and, as a result, difficult decisions on prioritisation must be made. The discipline of risk management and the approach set out in this strategy and methodology provide a mechanism to manage risks to a tolerable level.

2. Outcomes **can never be wholly guaranteed** when decisions are made in conditions of uncertainty.

3. It is usually **impossible to fully remove uncertainty from management decisions** or in the design and application of risk control activities.

4. **Decisions must be made on the best available information and expertise available at the time.** While hindsight may show that a different decision would have achieved a better outcome, conditions of uncertainty mean that the route to good outcomes is not usually known with absolute certainty at the time.

5. With this in mind, when making decisions (and particularly those that are urgent), **uncertainty should be reduced as far as is reasonably practicable** and in line with our agreed appetite for risk. The information on which decisions are made should be retained for later scrutiny and the learning of lessons.

6. The council's risk culture must embrace **openness, transparency, constructive challenge and must promote collaboration, consultation, cooperation and continual improvement.**

In prompting thinking about results and outcomes that the council intends to achieve and what jeopardises their delivery, the articulation of risk appetite statements also prompts management to consider what needs to change if these outcomes are unacceptable.

Whilst an overall risk appetite may be defined, it is important to note that the council's risk appetite varies by the category of risk faced. Indeed, in some risk category areas we have a low appetite for risk, while in others we are more open. Categorising or grouping risks in this way supports the development of an integrated and holistic view of risks, the council's risk profile and its risk exposure, ultimately supporting effective risk management.

Risk appetite statements are therefore used in two core ways:

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

Risk appetite is expressed in terms of differing 'levels' of appetite. These levels reside on a sliding scale, from averse to eager. Particular behaviours, attitudes and approaches are associated with these risk appetite levels, which are summarised below:

Risk appetite levels and behaviours	
Appetite	**Behaviour**
Averse	The avoidance of risk and uncertainty, which could be referred to as 'playing it safe'. Activities undertaken will only be those that are considered to carry virtually no inherent risk. Or, where inherent risk cannot be avoided, efforts and resources will be focused on managing the risk as far as is feasibly possible. This may result in incurring significant expense in management activities and/or losing potential opportunities arising. Risk aversion is typically 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 activities involving risk. Willing, however, tolerate a degree of risk where there is a high level of confidence that positive outcomes/benefits will be achieved. Risk and uncertainty will generally be avoided, however. 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
Open	Prepared to take calculated risks where successful outcomes are reasonably expected, particularly where controls and mitigations can be implemented to help secure them and to control the inherent risk. Risk openness attempts to strike a more even balance between risk and reward. Risk does not stop the pursuit of innovation and change. Instead it prompts the management of risk to a level that is acceptable and which, on balances, minimises negative outcomes. Failure is therefore possible though not reasonably expected.
Eager	Risk is positively embraced in pursuit of reward and failure is expected and accepted. Change, innovation and transformation and actively pursued, despite the likely possibility of the anticipated benefits not materialising or investment proving abortive.

As noted above, the council's risk appetite varies by the category of risk faced. The different categories of risk are defined in the table below. It should be noted that it is unusual for a risk to fall solely within one category, where impacts are usually many and multifaceted. The implications of this are considered in greater detail below.

Risk appetite categories	
Risk category	**Description**
Political	Risks arising from uncertainty in both the influence of the political environment that the council operates within (national, regional and local) and risks that influence or affect the political priorities of the council.
Financial – revenue	Risk related to not achieving income and savings targets, as well as the incurrence of unexpected revenue costs. This category also includes internal budgetary pressures and external macro and fiscal level economic changes, such as changes to funding agreements with central government and the rate of inflation, borrowing costs, etc.
Financial – capital	Risks associated with the council's assets and investment in physical infrastructure, such as property and the council's fleet, plant and equipment, financial assets and investment portfolio.
Social	Risks of failing to meet the needs of residents, local businesses and staff and/or worsening outcomes for these groups. This could be due to failing to respond to changes in service requirements, demographics or wider societal trends. The consequences of risks that fall within this category invariably includes loss of credibility or a degradation in trust.
Technological	Risks that are associated with the use or abuse of technological systems and solutions, including the protection of data and the integrity of internal systems. This category includes the effectiveness of how technology is used to support staff and external stakeholders, including residents and businesses of the borough. It also includes the resilience and security of our adopted technology, as well as the capacity and capability of staff to use it effectively and securely.
Legal/regulatory	Risks that can result in legal or regulatory challenges and being subject to litigation and/or external sanction. This category also includes risks of changing regulatory and legal requirements which could threaten the council's operations and processes.
Environment	Risks that impact the local environment in terms of resilience to extreme weather, the wider context of contributions to climate change, air quality and biodiversity and the and the ability to adapt to future needs of the population as adaptation becomes increasingly necessary.

Risk appetite categories	
Risk category	**Description**
Reputational	Risks that result in negative reputational impacts and the harming of trust in the council and its services.
Corporate objectives	These are risks and possible events that will jeopardise the delivery of the Corporate Strategy and other key corporate policies/strategies. They could arise for several reasons, including the over commitment of available resources and internal and external shocks. If materialised these risks may cause consideration of the hierarchy of the council's objectives and whether some must be prioritised over others.

Applying risk appetite in the public sector

At this point and before considering the next stage of the risk management cycle, it is appropriate to recognise that the use and deployment of risk appetite can be difficult or perhaps counter intuitive in the public sector. Indeed, clear and more readily 'quantifiable' risk appetite statements are easier to develop in organisations that are able to apply consistent, readily comparable units to measure inputs, outcomes and risks that may adversely affect them. In the private sector or enterprises directed by the profit motive, this is usually ultimately expressed as a monetary value.

Difficulty of use and application, however, does not mean that doing so is fruitless or without purpose. Rather, it impels the leadership of the council to follow a considered approach that explicitly recognises that the public sector – and local government in particular – delivers services that provide value across multiple horizons and timeframes and similarly utilises various 'units' to assess value in outcomes, one of which is financial.

The concept of risk appetite in the public sector is further challenged by the need, invariably over a spending period such as a financial year or medium-term financial plan period, to demonstrate that public money is spent well and efficiently, with value for money achieved. Having an appetite for risk may be reasonably perceived as a tacit acceptance of being prepared (however so defined) to experience loss, which includes – though is not limited to – financial loss.

Thus, the taking of calculated risks of the sort described in the risk appetite statements below may, on first glance, be difficult to reconcile with the nature and ethos of local government. However, we find the world as it is rather than as we wish it to be. Local government is not immune to risk and its ever-present nature. In fact, the importance of the services provided by

local government and the wider public sector require the effective management of risk in a highly uncertain environment.

Bearing these conditions in mind, if properly developed, applied and maintained, the use of risk appetite results in improved organisational performance and health, with risk identified and assessed in a robust and consistent way, allowing reasonable and evidence led decisions to be made whist maintaining organisational performance. This, in many ways, is the essence of delivering value for money.

These themes are explored further in the sections that follow.

Risk appetite statements

In pursuit of its objectives and in recognition of the radically uncertain environment within which the council operates, the council recognises that times of uncertainty and challenge require risks to be taken to achieve its ambitious corporate objectives. The council is therefore **open to higher levels of calculated risk taking,** providing that decisions are made on, as far as is possible, a sound evidential basis and are communicated in an open and transparent way. In doing so, the council will ensure that, where necessary, appropriate contingency measures and exit strategies are in place to mitigate risk.

As this is the first risk management strategy adopted by the council that explicitly includes a risk appetite, its use and operation will be subject to regular review in the early years of this strategy's adoption.

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

The statements apply to the residual risk. Residual risk is the level of risk faced after controls and mitigations have been applied.

Risk appetite statements by category		
Risk category	**Appetite**	**Risk appetite statement**
Political	Open	The council will prioritise the long-term resilience of the organisation and will champion the interests of the borough and our residents. We recognise that this may require us to challenge or work creatively within nationally set policy and will do so where we reasonably foresee benefits locally.
Financial – revenue	Open	We are committed to transforming the organisation to be resilient and fit for the future and recognise that this can come with an up-front net cost. We are prepared to do this where in the short term there may be some uncertainties around the ability to generate revenue savings and/or income, though prefer more certainty concerning longer-term benefits. We accept that balancing budgets might involve difficult decisions should anticipated benefits from opportunities not be realised in the short term.
Financial – capital	Cautious	We will invest selectively and will focus on ensuring we have an appropriately balanced portfolio that is managed well. We will consider additional investment where the business case is sound, stress tested under a range of scenarios and well understood. Capital investment must also clearly contribute to

Risk appetite statements by category		
Risk category	**Appetite**	**Risk appetite statement**
		our corporate objectives and we should be confident of realising the anticipated benefits.
Social	Cautious to open	The council is committed to doing the right thing, not the easy thing. While we will be guided by robust evidence and insight, we recognise that transformation, change and improvement could result in short-term impacts to service delivery, as well as not meeting the expectations of some members of our communities. Where possible and reasonable within available resources, we will seek to minimise these impacts. We are keenly aware that vulnerable people often rely on council services and so we are averse to reducing our ability to meet their needs.
Technological	Open	We recognise the importance of investing in technology and keeping pace with changes to ensure the organisation is efficient, resilient and secure. We accept that improving our systems and technological solutions comes with risk, including disruption to service delivery in the short term as new solutions and platforms are deployed. However, given that technology is a fundamental enabler to the council's operation, we are keen to minimise disruption wherever practicably possible. This means ensuring that our systems and practices are robust, fit for purpose, up to date and adhere to all government and industry standards concerning cyber security.
Legal/regulatory	Cautious	We will act lawfully and in conformance with appropriate codes of standards and other regulatory requirements. Where reasonable, legally permissible and ethical, we are prepared to explore areas of opportunity within legislation and codes of regulation and are willing to defend our position should challenge occur. We will be proportionate in our contractual dealings with suppliers, applying greatest internal scrutiny and due diligence to areas of greatest risk.
Environment	Cautious	The council is committed to reducing the impact of its operations on the environment. We will only accept the risk of direct negative impacts on the environment from our activities where we can demonstrate clear benefits of doing so and when weighed against other considerations and other

Risk appetite statements by category		
Risk category	**Appetite**	**Risk appetite statement**
		categories of risk. Environmental concerns are a priority for the council, but we acknowledge that, in some instances, our environmental objectives conflict with other corporate objectives and our ability to deliver and must therefore be balanced accordingly.
Reputational	Open	The council is committed to doing the right thing in achieving our wider corporate objectives, even if this results in short-term reputational damage and/or increased levels of negative external scrutiny. We will seek to communicate openly and effectively to establish public trust and will defend our position where we believe it to be right.
Corporate objectives	Open	We will set ambitious goals and targets in pursuit of change and improvement. We recognise that being ambitious may risk the non-delivery of some objectives and/or disruption to services arising from the need to reallocate resources or reprioritise as new areas of work or challenge emerge, potentially undermining the trust and confidence of internal and external stakeholders.

Risk assessment – analysing and evaluating impact and likelihood

Whilst the council's adopted risk appetite sets out the overall level of risk that the council is prepared to accept in pursuing its objectives, it is necessarily high level and directional. To apply the risk appetite statements effectively and consistently, the overall risk appetite must be underpinned by individual, robust risk assessments.

While each risk may be important on its own, a degree of measurement is required to evaluate the overall level of significance which supports risk informed decision making. Without a standard for measurement and comparison it is not possible to effectively compare and prioritise the myriad possible responses to risks, where effective prioritisation is predicated on robust risk assessment which, in turn, incorporates risk analysis.

Risk analysis must use a common and overarching set of risk scoring criteria to establish 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 ultimate purpose of this process is to use the insight gained to evaluate the extent to which the identified risk aligns 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**.

Before proceeding further, it should be recognised that assessing the likelihood of a risk materialising is inherently complex, particularly for risks that are higher level or 'corporate' in nature, with many dependent variables to consider and understand for a full probabilistic analysis to be complete. Put another way, understanding the likelihood of a risk – or a particular constellation of impact factors – materialising cannot be readily determined in the same way as, for instance, establishing the probability of rolling a certain number on a die or the next card to be pulled from a playing card deck.

Indeed, while it would be possible to undertake this level of analysis, in most instances it would be excessive given the nature of the risks faced by the council, with the likelihood categorisations set out below 'most likely' proving sufficient in most cases of corporate and service risk.

However, there clearly are instances where undertaking more detailed and deterministic risk analysis would be appropriate, such as in the project and programme environment, business case development, service and financial planning and strategic decision making. There are several tools to help quantify risk, uncertainty and to correct the tendency for organisations to be too optimistic in their planning, and therefore underestimating risk. A tool, known as Monte Carlo analysis, is particularly useful in this regard and is summarised below.

Likelihood

The following categories should be used for assessing the likelihood of a risk materialising:

Likelihood level	Description
Highly unlikely (1)	Highly improbable and is therefore not expected to happen (less than a 10% chance).
Unlikely (2)	A low chance of occurrence, but it's not impossible (10-30% chance).
Possible (3)	A moderate chance of occurrence; it's neither unlikely or likely (30-60% chance).
More than likely (4)	The risk event is expected to occur more often than not (60-90% chance).
Almost certain (5)	Highly likely to happen (greater than a 90% chance).

The timeframe for assessing the likelihood of a risk occurring is within the next three financial years, in alignment with the medium-term financial plan.

Risk impact

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 used 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 in this document.

Risk impact scoring matrix ***Note – (#) is the lowest likelihood score that, when multiplied by the impact score, would in most cases cause the risk to be outside of the council's risk appetite***					
Risk category	**Almost none (1)**	**Minor (2)**	**Moderate (3)**	**Significant (4)**	**Grave (5)**
Political	Some short-term local political criticism. No substantial and/or irrecoverable loss of trust or credibility among the political body.	Local political criticism. Short-term compromise of trust and credibility among the political body.	Strong local political criticism, though not significantly affecting political stability. Potential for minor national criticism. Some loss of trust, recoverable in the medium term. (4)	Substantial local political instability, compromising in the short to medium the delivery of policy outcomes and leadership. Criticism and minor action from government ministers. Minor breakdown in officer-member relations, affecting governance and decision making. (3)	Severe local political instability, seriously compromising the delivery of policy outcomes and leadership. Substantial, prolonged criticism or action from government ministers. Breakdown in officer-member relations, severely affecting governance and decision making. (2)
Financial – revenue[3]	<0.1% of the general fund net revenue budget or the HRA net revenue budget.	0.1-0.5% of the general fund net revenue budget or the HRA net revenue budget.	0.5-1% of the general fund net revenue budget or the HRA net revenue budget. (4)	1-3% of the general fund net revenue budget or the HRA net revenue budget. (3)	>3% of the general fund net revenue budget or the HRA net revenue budget. (2)
Financial – capital	<0.1% of the general fund or HRA capital programme.	0.1-0.5% of the general fund or HRA capital programme. (3)	0.5-1% of the general fund or HRA capital programme. (2)	1-1.5% of the general fund or HRA capital programme. (1)	>1.5% of the general fund or HRA capital programme. (1)
Social	Little to no negative impact to community resilience, social cohesion and trust of the council.	Short-term impact on community resilience, social cohesion and/or trust of the council. (3)	A section of the community impacted for the medium term. Loss of credibility and/or trust for the council. (3)	Long term, significant community impacts. Trust and confidence in the council compromised for a prolonged period by the	Community resilience and social cohesion severely compromised. Trust and confidence in the council severely comprised. (1)

[3] In 2024/25 the net revenue budget was approximately £12 million.

Risk impact scoring matrix ***Note – (#) is the lowest likelihood score that, when multiplied by the impact score, would in most cases cause the risk to be outside of the council's risk appetite***					
Risk category	**Almost none (1)**	**Minor (2)**	**Moderate (3)**	**Significant (4)**	**Grave (5)**
				wider community. (2)	
Technological	Negligible service disruption lasting less than 1 day. No requirement to invoke business continuity plans. Critical systems unavailable for less than 1 hour. No data loss or personal data breach.	Disruption to services for 1-2 days, workarounds available as per business continuity plans, though their formal invocation may not be required. Critical systems unavailable for up to 1 day. No data loss or personal data breach.	Disruption to services for up to 1 week, formal invocation of business continuity plans required to manage impacts. Critical systems and functions unavailable for up to 2 working days. Data loss or corruption; no personal data breach. (4)	Disruption of services for 1-3 weeks, invocation of BC plans to manage impacts. Critical systems and functions unavailable for 5 working days. Data loss or corruption and potential for a minor personal data breach. (3)	Disruption of services lasting more than 3 working weeks, BC plans increasingly unfeasible/unworkable. Critical systems and functions unavailable for >5 working days. Data loss or corruption and major personal data breach. (2)
Legal/ regulatory	Scrutiny from a government department, agency or regulator. Some threat of legal action, but no action anticipated.	Potential for minor sanction from a government department, agency or regulator. Minor litigation though with a strongly defensible position. (3)	Breach of law/regulations. Legal prosecution or sanction by an external regulatory body, some defence available. (2)	Significant breach of the law and/or regulations. Enforcement notice issued by a government agency, department or regulator, accompanied by a fine. Litigation probable, with limited defence. (1)	Judicial review, public inquiry or government intervention. Litigation probable with very limited defence. (1)
Environmental	Little or no impact on the local environment.	Short term minor local impacts with no ongoing negative effects. (3)	Short to medium term, reparable impacts on the local environment. (2)	Large scale and long-term damage to the environment, potentially irreparable. (1)	Extensive and irreparable damage to the environment. (1)
Reputational	Negligible local media attention and/or minor	Minor and short-term adverse publicity in the	Sustained local, regional and/or sector media	Adverse publicity in the	Sustained negative

Risk impact scoring matrix ***Note – (#) is the lowest likelihood score that, when multiplied by the impact score, would in most cases cause the risk to be outside of the council's risk appetite***					
Risk category	**Almost none (1)**	**Minor (2)**	**Moderate (3)**	**Significant (4)**	**Grave (5)**
	complaints received.	local media. Sustained level of complaints received.	interest and criticism. (4)	national media. (3)	national media coverage. (2)
Corporate objectives	Up to 5% variation in the achievement of corporate objectives.	5-20% variation. Workarounds required within existing resources, minor delays may be experienced.	20-40% variation. Resources will require reprioritisation. Delays expected. (4)	40-60% variation. Consideration to be given to the viability of corporate objectives, requiring reprioritisation. (3)	>60% variation. Unable to deliver on corporate objectives and failure to meet community needs. (2)

Overall risk score

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**
LIKELIHOOD		**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
		Highly unlikely	**Unlikely**	**Possible**	**More than likely**	**Almost certain**

The colours on the matrix correspond to the colours ascribed to each risk appetite level:

- Red – eager
- Amber – open
- Yellow – cautious
- Green – averse

Identified risks should be scored and assessed in the following three areas:

1. **The inherent risk –** this is the level of risk without any controls and/or mitigations being in place. A risk control is a process, policy or activity that reduces the likelihood of a risk occurring or materialising, whilst a risk mitigation reduces the impact should it do so. The analysis should be undertaken alongside the identified risk owner and the relevant service area.

2. **The current (or residual) risk –** this is the risk score once the current controls and mitigations have been assessed. Assessing the current risk must be done with reference to the council's risk appetite by each category. As with assessing inherent risk, the assessment of the current risk must be done alongside the risk owner and relevant service area to harness their specialist knowledge. It may also be appropriate to draw on other sources of assurance, including internal audit reports as well as other relevant pieces of consultancy or advice.

   The impact scoring matrix above details how the overall risk score (and factoring in the relationship between likelihood and impact) relates to the council's risk appetite. The impact table sets out the minimum likelihood value that, when multiplied by the impact score, would render the risk outside of appetite.

   Further, risks usually have multiple impacts and so the highest scoring category should be used to score the impact of the risk. Due to the individual and often unique 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, then no further action is required. However, if the risk score is outside of the council's risk appetite, then the risk should be considered for inclusion on the relevant corporate risk register for wider corporate awareness and oversight. Risk treatment options are considered below.

3. **The target risk –** this is the target to where management are aiming to treat or manage the risk to. The target risk sets out the desired end point of the risk management cycle. The target risk should be set with reference to the council's risk appetite which defines the level of risk the council is prepared to accept.

Setting a target risk is crucial to evaluating and confirming the adequacy and effectiveness of (a) the current controls and/or mitigations; and (b) the 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 (or likely) that, for certain risks where the council has limited scope to act, the current risk score may remain greater than the target score. Additional information on risk treatment options is set out in the section that follows.

Risk assessment and deterministic planning

As noted in the introduction to this section, assessing the likelihood and impact of risks materialising is particularly complex and difficult, especially with complex risks that require an analysis of the myriad independent – and indeed also dependent – variables for a full understanding to be achieved.

This complexity notwithstanding, the assessment schema set out above (utilising the 5x5 likelihood-impact matrix) is likely to be sufficient for the majority of risks faced by the council in its usual business. However, there will be occasions where undertaking more detailed analysis is necessary, such as in the project and programme environment, business case development, service and financial planning and strategic decision making, where the complexity of decision making impels decision makers to plan as deterministically for outcomes as much as possible.

In this regard, there are several tools and means to help quantify risk, uncertainty and the tendency for organisations to be too optimistic in their planning or decision making. Where appropriate, the use of these tools and approaches will improve decision making and will, in turn, heighten organisational risk maturity. An overview of potential approaches is set out below for illustrative purposes (utilising HM Treasury Green Book guidance), with further guidance available from the Strategy and Performance Team where required.

Risk quantification and optimism bias

In making decisions and appraising a course of action, such as agreeing to a significant investment, uncertainty (and therefore risk) often arises due to a lack of evidence or a robust understanding of the impact of policy or project interventions or actions.

With the inherent nature of risk and uncertainty in mind, coupled with often imperfect evidence, it is common for organisations (with the benefit of hindsight) to be over optimistic in their

planning and subsequent decision making, with risk not quantified appropriately and therefore resulting in unexpected loss.

In strategic planning and decision making, risk should – as much as is reasonable given the scale of investment – therefore be quantified and costed, allowing for initial assessments and determinations to be revised (or optimism bias corrected/adjusted for). As noted, there are various tools and techniques to do this, some of which are summarised below.

Single point probability analysis

Single point probability analysis involves estimating the probability of a specific outcome or event occurring based on a single set of assumptions or data points. Unlike methods that use a range of values or distributions to account for uncertainty (such as Monte Carlo simulations, summarised below), single point probability analysis relies on a deterministic approach. This means it uses fixed values for variables rather than considering variability or uncertainty, and how these variables may interact with one another in ways that are difficult to predict.

An example is set out in the table below:

Example – single point probability	
Project capital cost	£5 million
Cost of a 6-month project overrun	£275,000
Estimated probability of risk occurring	35% (‘possible’)
Estimated value of risk = £275,000 x 35%	£96,250

In such a scenario, it would be appropriate to consider options to reduce the likelihood of delays occurring, or building sufficient contingency into the project’s budget to cover this potential eventuality.

The analysis may be repeated for other risk scenarios within a project or area of work, where the overall aggregation of individual risks may help inform the project contingency budget. Interdependencies should also be considered.

While this approach may be appropriate in many instances, there are some limitations to it, which include:

1. **Fixed variables –** single point probability analysis does not allow for a consideration of a range of potential outcomes. The use of fixed values for variables (as per the example above) in this method ignores inherent uncertainty in real world risk scenarios.

2. **Simplification –** linked to (1), this approach can oversimplify inherently complex situations. One single estimate is provided, which is unlikely to capture the full range of potential outcomes given the inherent uncertainty described.

3. **Optimism bias –** as with the issue it aims to correct, there is a risk of using an overly optimistic estimate, leading to the underestimation of risks. This method therefore works best where there is a high degree of empirically verifiable certainty.

4. **Outcome distribution –** underpinning (1-3), this method does not provide a distribution of potential outcomes, including the likelihood of an extreme (but highly unlikely/rare) value. This is necessary for understanding the potential impact of rare but significant events.

Multi-point probability analysis

In recognition of some of the limitations inherent to the single point model, multi-point probability analysis is founded on the basis that there are a range of possible values for any risk. A probability distribution recognises that some are more likely than others. Indeed, while some risks have a low probability, they may have significant impacts on outcomes and require careful management. An example of multi-point analysis is set out below.

Multi-point probability example

A new leisure centre is expected to cost £15 million to build. The expected costs associated with construction uncertainties are:

Result	Possible cost	Difference from cost estimate	Probability of occurrence (%)	Risk value
1	£15 million	£0	45%	£0
2	£18 million	+£3 million	25%	£750,000
3	£22 million	+£7 million	15%	£1.050 million
4	£24 million	+£9 million	10%	£900,000
5	£28 million	+£13 million	5%	£650,000

With the above example, the most likely result is that of no extra cost (probability of 45%). However, the expected additional cost – the total of each possible result multiplied by its probability – is £3.35 million, which is useful insight in setting a project contingency budget and, indeed, considering its viability in the business case stage.

Monte Carlo analysis

As well as the above, Monte Carlo analysis is a computational technique that uses random sampling to simulate a range of possible outcomes for a given decision or event. By running many simulations, it allows for a detailed assessment and quantification of risks and uncertainties. The outputs are therefore the result of many simulations that model the collective impact of a number of uncertainties.

This technique is particularly useful where there are many variables with significant uncertainties which, despite this, have known or reasonably quantifiable independent probability distributions. This method may be applied in project management to evaluate the impact of different variables on project timelines and budgets, as well as in broader risk management and strategic planning to assess the likelihood and impact of various risk-based scenarios.

Monte Carlo analysis requires:

1. **The problem or issue to be defined –** this involves clearly defining the risk or uncertainty to be analysed.

2. **Identification of key variables –** determine the key variables that influence the outcome of the project or decision, such as costs, time estimates, resources etc.

3. **Assign probability distributions –** for each key variable, assign a probability distribution that best represents the level of uncertainty faced.

   Probability distributions include: uniform, where every possible outcome has an equal probability of occurring; normal, where outcomes typically cluster around the mean value; triangular, capturing three outputs of best, worst and most likely.

4. **Create and run a statistical model –** that relates the key variables to the outcomes and use it to run a large number (thousands) of simulations where each simulation randomly selects values for the key variables based on their probability distributions and then calculates the outcome.

Following the running of the model and an undertaking of statistical analysis, the results can then be used to determine an expected result given a particular probability, such as P50, P80 and P90. Put another way, the data can be used to state that there is an *expected* 50%, 80% or 90% probability that a given outcome will be below or within a particular level.

A Monte Carlo model has been developed for teams at the council to use in making risk-based decisions and is available from the Strategy and Performance Team.

Risk treatment

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

The council's 'three lines of defence' approach to risk management 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 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 therefore 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 risk and taking action to move it to 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 mostly 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.

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

- **Avoidance –** stop doing the activity that creates the risk, or elements of it. This may not be possible or desirable, however, particularly where the risk is unavoidable or arises

from activity that the council is obliged to carry out. 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 stopping 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 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 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 financial. Risks owners must therefore use their professional knowledge and judgement to determine whether costs are justifiable in terms of non-financial benefits to the council. On some occasions it may be reasonably concluded that the costs of action outweigh any perceived benefits.

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

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.

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. It should consider:

- The rationale for the option(s) selected, including the anticipated benefits;
- The proposed actions – i.e. implementing new controls and/or mitigations;

- An identification of those that are accountable and responsible for the implementation of any actions arising;
- Any resources required;
- The key performance indicators that will be used to demonstrate and track progress 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 or dependencies to be aware of.

Where appropriate, contingency, crisis, incident and business continuity management arrangements should be developed and communicated to support resilience and recovery if risks do indeed occur.

Risk monitoring and reporting

The council's risk profile (defined as the risks that the council is actively managing as well as those inherent to the environment that it operates within) should be regularly monitored and reported on. This is because:

1. Risks may change over time and treatment options may subsequently require adaptation;
2. The internal control environment may degrade, with controls and mitigations not adhered to and/or proving ineffectual;
3. New risks may emerge, with current controls and/or mitigations possibly proving inadequate; and,
4. After successful management efforts 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. Whilst each line of defence and team has its own distinct role, they must operate in an integrated way to support the ongoing development of understanding on the council's risk profile and how this changes over time. Roles and responsibilities are summarised in a subsequent section of this document.

When operated well, risk monitoring and reporting activities provide assurance to management and other key stakeholders that controls and mitigations are operating as intended and that, more fundamentally, risks facing the council are understood and, as much as is possible, are being managed in accordance with the risk appetite.

The result of monitoring and review activities should be incorporated into the council's wider performance management, measurement and reporting activities and communicated to stakeholders as necessary via established channels of reporting.

Risk monitoring

In accordance with Orange Book guidance, monitoring should be carried out before, during and after the implementation of risk treatment activities. Ongoing and continuous monitoring should help the leadership of the council, as well as other key stakeholders, understand whether and how the risk profile is changing and the extent to which controls and mitigations are operating as intended.

Under the three lines of defence model, risk monitoring is within the scope and remit of management at the first line of defence.

As part of their primary responsibility and accountability for risk, management are responsible and accountable for designing and implementing processes that monitor risks or changes in the council's risk profile that could create risk.

This may take the form, for instance, of:

- Reviewing **performance and data trends**, as well as other contextual indicators, which may be suggestive of a change in the control and/or external environment;
- **'Deep dive' reviews** into risk areas (specific or otherwise), either carried out by management or commissioned by teams at the second and third lines of defence;
- **Learning from incidents, issues and/or the experience of others.** Learning from experience (direct or otherwise) can help prevent a future recurrence or, if this is not possible, may help with mitigation activities;
- **Testing** of the effectiveness of controls and mitigations. Management may also be supported by the second and third lines of defence, summarised later; and,
- **Horizon scanning** for changes in the risk environment, using tools such as PESTLE as described above.

As described in the risk identification section above, service and corporate risk registers should serve as a comprehensive record of the risks faced by the council and which are reasonably foreseeable (and foreseen) as part of management and service planning. Risk registers must be reviewed at least on a quarterly basis, though more frequent review may be appropriate in some service areas given the varying risk profile therein. Project and programme risk registers will likely require more frequent review, too, given their timeframes of delivery.

The Strategy and Performance team will support service management's role in risk monitoring through the **quarterly risk management review process**. The process – held with Assistant Directors and other members of management as appropriate – should review all identified risks alongside the owner and:

- Consider whether the risk description adequately covers the risk, especially if there have been any recent substantive changes;
- Critically assess the effectiveness of controls and/or mitigations, using available evidence and information and recognising any limitations with it;
- Ensure that controls and mitigations are up to date and reflective of the latest position;
- Review the risk scoring against the council's risk appetite; and,
- Consider whether any further action or escalation may be required.

The quarterly review process must also consider whether any new risks have emerged or, alternatively, whether any degradation in the control environment has itself created risk. This

should be done in accordance with the processes set out in the risk identification and assessment section of this methodology document.

However, as noted above, not all risks may be readily foreseen and therefore recorded on service risk registers. Alternatively, methods for monitoring risks may prove inadequate under certain circumstances, with key risks missed. Management may therefore require support to identify where controls have broken down or where a known risk has changed to such an extent that current controls and mitigations are inadequate. This support is provided by the second and third lines of defence.

The second line of defence provides the policies, frameworks, tools, techniques and support to enable risk and compliance to be managed effectively by the first line, and itself carries out monitoring activity to identify their effectiveness and their adherence and compliance. This can take the form of commissioned work into particular areas of risk, though also includes those 'business as usual' activities for teams at the second line of defence. 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.

Importantly, teams at 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 should any concerns arise.

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.

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 findings made by external audit will be acted upon by management and the political leadership as necessary.

Risk reporting

Risk reporting is crucial to the overall operation of the council's risk management cycle. Indeed, the timely, accurate and useful provision of risk reporting helps drive good decision making and supports bodies with oversight responsibilities to meet their responsibilities under the council's constitution, as well as any other statutory or regulatory requirements.

An effective risk management framework creates a series of processes that anticipates, detects and responds to changes and risk events in an appropriate and timely way. Risk reporting is the crucial mechanism through which key stakeholders are appraised of this, ensuring that the right information is given to the right people and at the right time.

Whilst there are different types of risk reports, all are purposed with:

- Transparently communicating risk management activities and outcomes across the council;
- Helping decision makers and the leadership of the council with the assessment of whether decisions are being made with proper regard to the council's risk appetite;
- Provide information for informed decision-making concerning risk and risk management activities, including prioritisation;
- Reviewing the adequacy and effectiveness of controls and mitigations;
- Improving risk management activities; and,
- Reviewing and amending the risk appetite, keeping it under review and communicating this to stakeholders as necessary.

The types of risk reporting are set out in the accompanying risk management strategy document. Additional information on each report is provided below:

1. **Risk registers –** as noted, risk registers set out the risks that management is aware of and is taking steps to actively manage. Risk registers should be reviewed, updated and reported at a frequency that is appropriate to their content and scope. Risk registers are the most regular form of risk reporting used at the council, with quarterly updates to corporate risks taken to the Executive each quarter via the Corporate Governance and Standards Committee.

   Corporate risk registers are usually reported one quarter in arrears, with, for instance, the Q1 risk register for a financial year reported to the relevant board or committee in Q2. Doing so allows sufficient time for risks to be reviewed at the close of each quarter. A summary of risk register reporting schedule is set out below.

   At a minimum, risk registers should:

   - Describe the risk, in accordance with the guidance in this methodology document;
   - Identify a risk owner, including a senior officer and an Executive member;
   - Identify the controls and mitigations that are in place;
   - Set out the scoring of the risk, including the inherent, residual and target score. Information on how to do this is provided in the risk assessment section of this methodology document;

- Identify the controls and mitigations to be implemented to bring the risk to a level that is either within the council's risk appetite or, if this is not possible, to tolerable level;
- Include an explanatory narrative and background to aid stakeholders and decision makers fully understand the risk. This may be included within an accompanying committee report, for instance.

2. **Principal risk report –** this type of report provides an overview of principal and/or emerging risks, either within a particular area of department, or, indeed across the council more widely. A principal risk report may be contained within another, such as the annual refresh of the council's medium-term financial plan, when developing a corporate policy or strategy, or updates on Corporate Strategy performance. It is also likely to form part of a report where the Executive is asked to make a decision, significant or otherwise. Principal risk reports may have a dual focus – i.e. risks arising from the external or internal environment, or, indeed, how the two may interrelate.

   A principal risk report may follow various formats, including PowerPoint updates, written reports, dashboards or a combination thereof.

   The report may include:

   - **Background –** outlines the scope and purpose of the report, including the risk area covered and why it is a salient topic to consider.
   - **Analysis –** summarises the main issues and information for consideration. This should usually be arranged by risk category (e.g. financial, reputational, etc.), severity or the likelihood of the risk materialising and the impacts should it do so. It should also consider the operating environment and the effects of management activity, as well as any further uncertainties. The use of data and evidence is crucial to this. Where appropriate, different options for management or response should be articulated, with analysis undertaken to establish why a particular course is recommended (or not). Consideration should also be given to how the risk compares against the council's risk appetite.
   - **Assessment/conclusion from the relevant officers –** where necessary, a summative conclusion should be drawn from the officer(s) that hold(s) primary responsibility for the management of the risk.
   - **Recommendations and next steps –** where a decision is sought, clear recommendations should be given, including a summary of the available options. As well as this, a summary of the plan for managing the risk (while initially clarified earlier, should be linked to the proposed next steps.

3. **Deep dive report –** provides a detailed assessment of the nature and extent of an area of or specific risk. Organisations typically commission such reports on a cyclical basis against areas where the greatest principal risk exists, or when aligned to the usual decision-making processes that require it.

   Deep dive reports follow a similar structure to risk registers, though its format should allow for a 'deeper' consideration to be drawn out.

   The report may include:

   - **Purpose and background –** summarise what's included in the report and why.
   - **Risk summary –** provide key details about the risk, such as its description, the date when it emerged or was first escalated for wider corporate awareness. Provide background context and how the risk relates to the council's priorities, outcomes and objectives. Provide an assessment of the risk against the council's risk appetite: i.e. what's the current level of exposure and how does this relate to the council's risk appetite?
   - **Summary of progress –** set out the progress to date in the management of the risk. Use key metrics and/or dates wherever possible, as well as any delays or threats to plans for mitigation, including any internal and external changes to be aware of. Define any subsequent risk management activity required.
   - **Assessment/conclusion from the relevant officers –** building on the previous provide a summary of risk management activity from the relevant officer(s), which is usually the risk owner(s). Provide a summary of key achievements, future concerns and any current issues.
   - **Recommendations and next steps –** where a decision is sought, clear recommendations should be given, including a summary of the available options.

Whichever form it takes, risk reporting should be:

- **Collaborative –** through aligning with the work of teams across the three lines of defence, in drawing on the insight and expertise of risk owners, as well as aligning with the wider processes across the council.
- **Evidence based –** through making best use of evidence and management information to provide assurance on risk as well as utilising data and evidence to guide decision making.
- **Focused on objectives –** to allow for impacts on objectives to be clearly understood and for prioritisation activity to be carried out.

- **Informative –** through providing a clear understanding of risks, as well as confidence in the assessment of the treatment of risks and the taking of timely corrective action.
- **Integrated –** though being integrated with, and complementary to, other governance and leadership processes across the three lines of defence.
- **Tailored –** in being adapted to the target audience and their differing needs.

Reporting schedule

The reporting schedule for corporate risks is summarised in the table below:

Quarter (financial year)	**Report**	**To**
Q1-Q4 **(reported one quarter in arrears)**	**Corporate risk update –** strategic and operational risks, including: • Opening new risks • Closing risks	Corporate Leadership Board
	Corporate risk update – strategic risks and red rated operational risks, including: • Opening new strategic risks • Closing strategic risks	The Corporate Governance and Standards Committee The Executive
Q3	**Service plan risk summary –** a summary and analysis of risks that have been identified in service plans, as part of budget setting.	Corporate Leadership Board. The content will influence the quarterly risk update.

Roles and responsibilities

The effective and efficient operation of the risk management cycle described in this document is founded on well-established and understood roles and responsibilities.

The council operates a three lines of defence model, which is founded on the idea that:

1. Risk should not be left to risk management specialists;

2. Everyone in the council has some responsibility for risk management; and,

3. The varying roles, parts and levels of the council play different but complementary roles in respect of risk management. The interplay between these roles determines how effective the council is in managing risk and exercising effective internal control which, in turn, is essential to robust corporate governance.

The successful operation of the council's risk management strategy is therefore founded on the roles and responsibilities defined in the sections below. Importantly, the roles and responsibilities described are not intended to be exhaustive. Instead, they have been set out to provide a high-level overview and guide that is appropriate for most instances of risk.

Further, the roles and responsibilities set out below have been drafted to be in conformance with the council's Constitution and Scheme of Delegation. For the avoidance of doubt, the latter take precedent in any instances of inadvertent conflict.

At the first line of defence

The Joint Leadership Team and service management (managers/team leaders/supervisors) will:

- Identify, implement and maintain effective internal controls to manage risk on a day to basis within service areas and in accordance with the council's risk appetite.
- Ensure the ongoing adequacy and effectiveness of controls and mitigations and take any remedial action as required.
- Proactively identify potential risks which could affect the council and ensure that these are recorded and managed in accordance with the risk management strategy and methodology.
- Ensure that staff within the service/team understand the potential risks facing the service and the 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, such as in health and safety.
- Seek support from other services as and when required.
- Escalate concerns relating to risk as required.
- Ensure that the appropriate Executive Member(s) is/are briefed on the key risks facing the service.
- Ensure that risks are considered in all aspects of decision making.
- Ensure that risk is considered robustly as part of the annual service and financial planning process.
- Act in collaboration with other services and/or organisations as appropriate to manage risk.

Risk owners will:

- Take accountability for the identified risk and its control and/or mitigation, including on reporting on progress of risk treatment.
- Escalate any concerns in a timely way in accordance with the usual management and leadership structure of the council.
- Act in collaboration with other services and/or organisations as appropriate.

All council employees will:

- Always act lawfully and ethically and in full conformance with 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 and one's role in managing them.
- Following all service and corporate risk controls and/or mitigations.
- Understand how to identify and report any areas of concern, in accordance with established policies procedures.

At the second line of defence

Corporate Health and Safety will:

- Provide effective and competence health and safety advice to support services in maintaining staff and resident welfare and health and safety.

- Ensure that accident and incident investigations are carried out where required, with lessons learned and implemented and any necessary preventative action taken.
- Maintain corporate risk assessments and support services to maintain departmental level risk assessments where required.
- Regularly review the council's health and safety management system, including policies and operational practices, to ensure its effectiveness and compliance with all legislative requirements.
- Share best practice and learning with departments to manage health and safety risks.
- Provide induction training to staff when they join the council on the approach to corporate health and safety.

Corporate Strategy and Performance will:

- Maintain the council's risk management strategy and methodology.
- Support the effective operation of the risk management cycle described within the risk management strategy and methodology, including by undertaking quarterly risk management reviews with the Joint Leadership Team and managers.
- Report on risk to the appropriate governance groups, including the Corporate Leadership Board, the Corporate Governance and Standards Committee and the Executive.
- Support service management in their primary risk management role and help coordinate the activities of other service areas 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 the annual service and financial planning process, performance management, the Code of Corporate Governance and the Annual Governance Statement.
- Monitor and report on corporate and service performance in accordance with the council's performance management framework. Through regular reporting, escalate any performance and/or compliance issues that have a causative effect on risk as appropriate.
- Maintain and communicate a comprehensive knowledge of the local government policy context and potential risks arising from its changing nature. Use this insight to support service areas in the management of risk.
- Provide training to staff on the council's approach to risk management, appropriately tailored to the varying roles within the council.

Data protection will:

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

Democratic Services will:

- Ensure that processes and procedures are designed and implemented and are operating effectively, allowing decisions to be made and authority exercised in accordance with the council's Constitution and Scheme of Delegation as well as prevailing standards of good corporate governance and leadership.
- Maintain the Code of Corporate Governance and Annual Governance Statement.

Emergency Planning and Business Continuity will:

- Mitigate risk to residents and businesses of the borough through the creation of robust emergency plans and operational arrangements that enable the council to respond to a range of civil emergencies and in accordance with its statutory responsibilities under the Civil Contingencies Act (2004).
- Ensure that emergency plans are kept up to date and that the council learns from incidents, alongside multiagency partners at the Local Resilience Forum.
- Support council services to systematically manage the risk of service disruption due to a range of business continuity incidents, ensuring that any weaknesses in resilience are understood and that controls and mitigation measures are in place to overcome disruption, maintaining the delivery of core services as far as is reasonably practicable.
- Support in the recovery from emergency incidents and/or business continuity events.

Finance will:

- Design and apply the council's core financial controls to ensure that public money is spent wisely, effectively and is appropriately accounted for, helping to minimise the risk of fraud and loss.

Human Resources and Organisational Development will:

- Ensure the ongoing effectiveness of the council's employment practices, policies and procedures, as well as monitoring compliance.

ICT will:

- Maintain, as far as is reasonably practicable, a resilient and robust network architecture and infrastructure that reduces the risk of unplanned network and service outage.
- In collaboration with management, help ensure that ICT solutions used by the council departments are fit for purpose and secure, helping maximise service efficiency.
- Maintain the council's disaster recovery plan and procedures to support recovery from an ICT security incident or business continuity event.

Insurance will:

- Maintain the council's insurance arrangements with its insurance provider, ensuring an appropriate level of coverage given the services provided and the risks faced.
- Ensure that learning from insurance claims is acted upon by the relevant service area, or combination thereof.

Legal will:

- Provide appropriate and timely legal advice and services to ensure that the council acts lawfully in its business.
- Defend the council's interests if the council is subject to legal challenge.

Procurement will:

- Maintain the council's procurement and contract management strategies.
- Support services to derive best value from contracts and procurement spend.
- Ensure that in its purchasing decisions, the council acts in conformance with all statutory requirements, public procurement legislation and best practice, as well as the contract procedural rules.

The Programme Management Office (PMO) will:

- Maintain and ensure the effective operation of the council's project and programme management frameworks. The framework help ensure that projects are initiated on sound business cases, that costs and uncertainty are understood as much as is possible and that delivery is done in a controlled way and with regard to the management of all types of risk.

The Risk Management Group will:

- Through bringing together key teams from the second line of defence, oversee the operation and ongoing development of the council's risk management strategy and methodology.
- Provide assurance to the Corporate Leadership Board that the strategy and methodology are operating as intended.
- Serve as a forum within which risk may be discussed, with any concerns escalated to senior officers and the Corporate Leadership Board as required.
- Champion and help embed effective risk management practices and processes across the council.
- Where necessary, receive, for information purposes and the building of risk awareness, key reports and other documents arising from all three lines of defence, including service plans, business continuity plans, emergency plans, risk assessments, internal audit reports and the annual internal audit report and opinion, amongst others.
- Support the coordination of assurance activities operated by services across the three lines of defence.
- Through a regular review of risks and risk registers, enhances corporate risk awareness and helps ensure a common corporate understanding of the councils' risk profile.

At the third line of defence

Internal Audit will:

- In following a risk based approach to their work and adopting a risk based audit plan, identify potential weaknesses in systems, controls and procedures that may expose the council to risk.
- Operate in accordance with the prevailing industry and public sector internal audit standards.
- Report findings arising from reviews to the audit sponsor, usually a senior officer as well as to the Corporate Leadership Board and the Corporate Governance and Standards Committee.
- Produce regular progress reports on the status and overall performance of internal audit activity.
- Based on audit testing for the year, produce an annual report and opinion on the overall effectiveness of risk management and control at the council, highlighting areas of weakness and where improvements should be made.
- Use the corporate risk registers to inform the risk based internal audit plan.

External Audit will:

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

Governance roles and responsibilities

Under the three lines model, constituted governance bodies and senior management are not considered to reside at a particular line. Rather, they are key stakeholders that are served by the collection operation of the three lines of defence.

Each governance body has varying roles and responsibilities, however, which are set out below.

Members of the council will:

- Maintain an awareness of the council's overall risk profile and that of the wider public sector.
- Ensure their awareness and familiarity with key corporate risk controls and mitigations, and act in full conformance with them and the member code of conduct.
- Attend and participate in any training and/or development that is relevant to their role and which supports the council's overall approach to the management of risk.

The Executive will:

- Set the overall policy direction for the council and, in working with officers, ensure that risks threatening corporate objectives are adequately addressed and managed in accordance with the council's risk appetite.
- Receive:
    - Quarterly updates on strategic risks as part of corporate risk reporting.
    - Quarterly updates on red rated operational risks as part of corporate risk reporting.
- Approve:
    - In year new risks for inclusion on the strategic risk register as part of corporate risk reporting.
    - In year closure of strategic risks as part of corporate risk reporting.

- Any subsequent updates to the risk management strategy as required, following review by the Corporate Governance and Standards Committee.

The Corporate Governance and Standards Committee will:

- Act in conformance with its constitutional responsibilities in respect of risk management, which includes 'providing independent assurance to councillors of the adequacy of the risk management framework 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 charter.
  - Internal audit plans.
  - The annual external audit plan.
- Receive:
  - Quarterly updates on strategic risks as part of corporate risk reporting.
  - Quarterly updates on red rated operational risks as part of corporate risk reporting.
  - The council's updated risk management strategy when it is reviewed and updated every three years, or more often if required.
- Make any comments and/or recommendations relating to risk management to the Executive and/or Senior Management Team as appropriate.
- Make any comments and/or recommendations relating to risk management to any other relevant body as required.

The Corporate Leadership Board (comprised of the senior management team and statutory officers) will:

- In serving as the highest point of officer governance and leadership, hold overall responsibility for the management of risks in accordance with the Constitution and Scheme of Delegation, as well as the council's risk appetite.
- Ensure that the council's risk management strategy is robust, fit for purpose and that it is applied effectively and consistently across the council, thereby supporting high standards of leadership and corporate governance.
- Receive:
  - Quarterly updates on strategic and operational risks, or more frequently if required.
  - Updates on service risk registers and any escalations required.

- Approve:
    - Any newly identified operational risks for inclusion on the operational risk register as part of quarterly corporate risk reporting.
- Recommend:
    - That the Executive approves any identified new strategic risks as part of quarterly corporate risk reporting.
    - That the Executive approves the closure of any strategic risks as part of quarterly risk reporting.

Training and communication

The council's risk management strategy must be underpinned by management and staff awareness of the requirements contained within it, as well as a general management competence to manage risks adequately and in accordance with the council's risk appetite.

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

In accordance with the three lines model, service management are responsible for ensuring that staff receive adequate support, training and supervision to complete their duties safely and in accordance with all corporate, service and other statutory risk controls/mitigations.

The Strategy and Performance Team is responsible for providing training and guidance on the risk management strategy to management and other key stakeholders as required. This may take the form, for instance, of:

- Regular briefings to staff on risk management, the risk management strategy and roles and responsibilities;
- Briefings to management on risk management, the risk management strategy and roles and responsibilities; and,
- Other ad-hoc training as required and requested by the Corporate Leadership Board.

The need for training and internal communications will be particularly acute in the first year of the strategy as many of the practices contained within it are new to the council.

The strategy and methodology are made available to all staff and councillors on the council's intranet. A bespoke internal communications portal will be established to support the timely dissemination of risk management news, knowledge and best practice. This will include access to service and corporate risk registers, as well as any other documents required.

The risk management strategy and accompanying guidance will be required reading for new staff as part of the induction process.

Future review

The 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 and impact scoring categories, for instance. Regular review is crucial to ensuring that the strategy remains relevant to the council, its risk profile and wider leadership structures.

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