GUILDFORD BOROUGH COUNCIL

RISK MANAGEMENT STRATEGY

2025/26 to 2028/29

GUILDFORD BOROUGH

Waverley BOROUGH COUNCIL

Contents

Version control

Approved by	
Date approved	
Review date	

Strategy on a page

Background

This risk management strategy **explains how the council identifies, assesses, manages and reports on the risks it faces.** It is accompanied by a detailed methodology that defines how its principles and objectives should be applied.

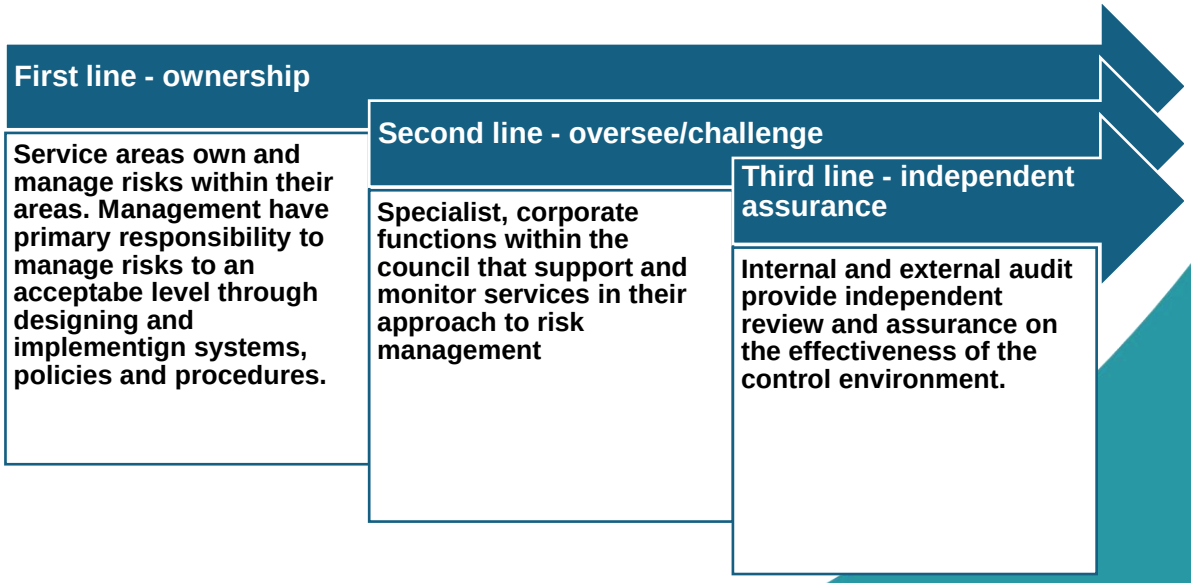
Risk is defined as the effect of **uncertainty on objectives.** Risk is ever present and unavoidable. Put simply, it is not possible for the council to be blanketly risk averse and to be successful. **Risk management** refers to the set of coordinated activities that are designed and operated to reduce risk and exercise internal control within an organisation.

Risk appetite

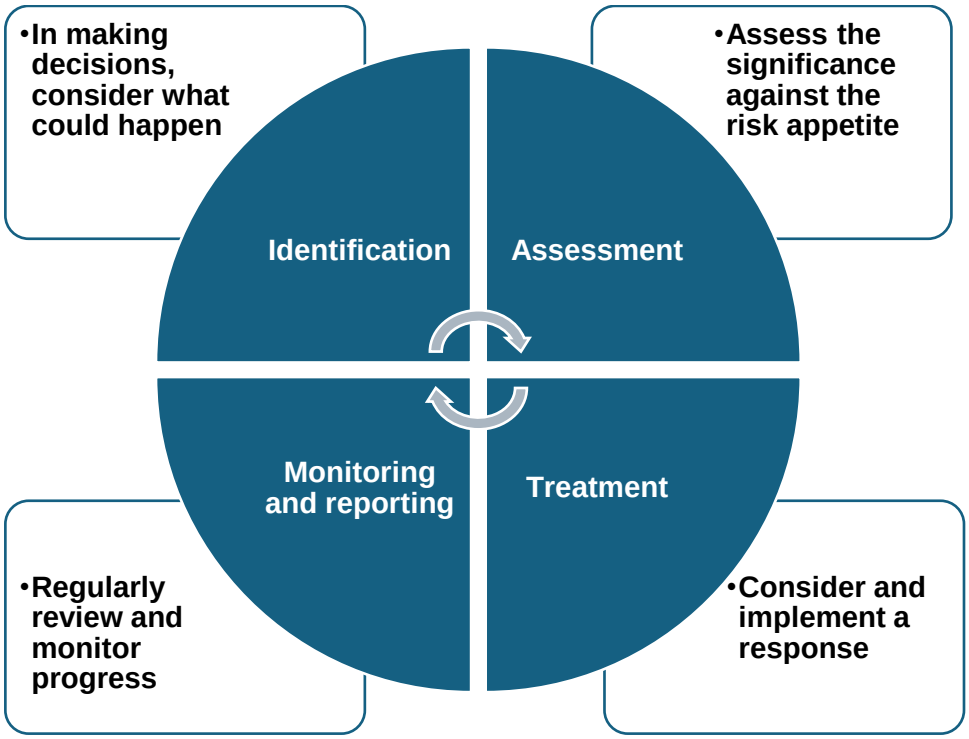
The council recognises that times of uncertainty and challenge require risks to be taken to achieve its ambitious corporate objectives. The council is therefore **open to higher levels of calculated risk taking,** providing that decisions are made on, as far as is possible, a sound evidential basis and are communicated in an open and transparent way.

The three lines of defence model

The council has multiple teams, departments and individual roles that assist in the management of risk. Each has its own unique perspective and skillset that is essential to the overall management of risk, and their efforts must be coordinated for best effect.



The risk management cycle



Roles and responsibilities

The Joint Leadership Team and service management – Identify, implement, and maintain effective internal controls to manage risk in accordance with the council's risk appetite.

The Corporate Leadership Board – holds overall responsibility for the management of risks in accordance with the Constitution and Scheme of Delegation, as well as the council's risk appetite.

The Corporate Governance and Standards Committee – provide independent review of the council's governance, risk management and control frameworks and oversee the financial reporting and annual governance processes.

The Executive – 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.

Introduction

This strategy sets out Guildford Borough Council's commitment to risk management as a core component of good governance and effective leadership.

In broad terms, risk may be defined as the effect of uncertainty on objectives. Risk management is the coordinated set of activities that are designed to manage risk and exercise internal control within an organisation. By following a systematic approach to the management of risk, the council is able to minimise the impact of negative events.

The council's risk management strategy sets out how the council identifies, assesses, manages and monitors the risks that it faces in delivering its objectives. The strategy has been developed to ensure the integrity of risk management to all council activities and decision making, as well as fostering and promoting a positive and mature risk culture amongst councillors, officers and suppliers.

An accompanying risk management methodology sits alongside and complements this strategy. Whilst this strategy sets out the context and overall approach to risk at the council, the methodology defines the systems and processes utilised by the council to deliver the strategy's objectives, including detailed roles and responsibilities.

The strategy and methodology have been designed in recognition of the inescapable fact that risk management is fundamental to effective governance, leadership and strategic planning, and is similarly core to how the council is managed and controlled at all levels.

The two documents therefore form the foundation of robust risk management at the council, contributing to the effectiveness of the wider framework of corporate governance and the achievement of strategic objectives. The documents will be reviewed regularly by officers to ensure the council continuously improves its approach to risk management and corporate governance.

Strategy statement

Guildford Borough Council recognises that risk management is of fundamental importance to effective corporate governance, leadership as well as the direction, control and management of the organisation. Robust risk management systems, practices and culture must be an integral part of all council activities and, in adopting this strategy, the council is committing to ensuring that risk is considered in all aspects of informed decision making.

Risk is ever present and unavoidable, especially as the council is a complex organisation with bold ambitions and objectives – as well as various statutory duties and obligations – operating in an inherently uncertain environment. Put simply, it is not possible for the council to be blanketly risk averse and to be successful.

The council recognises that times of uncertainty and challenge require risks to be taken to achieve our ambitious corporate objectives. The council is **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.

The council is therefore committed to the discipline of risk management to improve organisational planning, performance, governance and decision making. Risk management should not stifle improvement, innovation and the delivery of services. Instead, through being integrated with the council's leadership and management systems, it should harness organisational wide activities to bring risk to a tolerable level.

The effectiveness of risk management activities is fundamentally dependent on the individuals responsible for operating the systems in place. To that end, the council wishes to foster a risk culture that embraces openness and transparency, is supportive of constructive challenge and promotes collaboration and co-operation between councillors and officers.

When delivered well, risk management is as much about analysing the uncertainty of the internal and external environment as it is about managing impacts of risks once choices are made. The risk management strategy and methodology will ensure that:

- Risk management contributes to effective service delivery and the achievement of corporate objectives;
- Accountability and responsibility for risk management is clearly assigned throughout the council;
- Councillors and officers acknowledge and understand the importance of risk management as a core component of effective governance and leadership; and,
- Effective monitoring and reporting mechanisms are in place to review the council's exposure to, and the management of, risks.

Objectives

The objectives of the council's risk management strategy and methodology are to:

1. Integrate effective risk management into the strategic and operational processes, procedures and culture of the council;
2. Ensure that risk is consistently identified, managed and reported on in accordance with established best practice, appropriately tailored to the council's risk profile and appetite for risk;
3. Enable and support effective risk-based decision making;
4. Provide management with early warnings of potential problems so that a response can be made in a planned, preventive way as much as is practicable;
5. Enable management to be clear on the activities over which they require assurance and the extent and adequacy of that assurance based on risk;
6. Foster a culture of risk awareness and ownership;
7. Support the council to anticipate and respond to changing social, environmental and legislative requirements; and,
8. Minimise loss, disruption, damage and injury.

Benefits

A robust approach to risk management will deliver a number of interlinked benefits, including:

- Improved standards of corporate governance and leadership;
- An enhanced ability to deliver against corporate objectives and enhance service delivery;
- Improved risk awareness among staff and management, with risks identified before they materialise, allowing preventive measures to be implemented as required;
- Improved decision-making, planning and prioritisation which can be evidenced;
- Enhanced financial control and reporting;
- Protecting and enhancing our assets, services and reputation;
- The more effective use of resources and the minimisation of waste, including additional expense incurred and resources utilised sub-optimally; and,
- Improved staff, resident and councillor health and safety.

Managing risks

Risk

The council shares the government's Orange Book definition of risk as the effect of uncertainty on objectives.[1]

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

- A **cause** is an element which alone or when combined with another has the potential to give rise to a risk;
- 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 likewise affect multiple objectives; and,
- **Consequences** are the outcomes of an event and which affect objectives. Consequences can be certain or uncertain, can have positive or negative direct or indirect effects, can be expressed qualitatively or quantitatively and can escalate through cascading and cumulative effects.

The council is exposed to many risks. Indeed, there are risks inherent to the operation of the services provided, as well as those arising from the general risk profile of local government and the wider public sector. The external environment is also one that is widely acknowledged as being 'radically uncertain', with the last five years of economic difficulty, geopolitical crises and pandemic merely underscoring this.

The council recognises, therefore, that risk is unavoidable and inherent to everything it does. Given its role in the borough and the various statutory obligations held, it is crucial to acknowledge that the council cannot be blanketly risk averse and deliver for the residents and businesses of the borough.

Risk management

With the ever present and unavoidable nature of risk in mind, risk management is the set of coordinated activities that are designed and operated to manage risk and exercise internal control within an organisation. These activities must be underpinned by – and mutually support – a positive and mature risk culture, where officers and councillors are encouraged and supported to manage and respond to risks in an open and transparent way, heightening

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

ownership and accountability. Indeed, an inappropriate and/or immature risk culture may result in activities being carried out that contradict or undermine organisational objectives.

In accordance with Orange Book guidance, the council recognises that an effective system and culture of risk management is founded on the following core principles:

1) Risk management is an essential component of effective governance and leadership, and is crucial to how the council is directed, managed and controlled at all levels;
2) Risk management is an integral part of all organisational activities to support decision-making in achieving objectives;
3) Risk management activities must be collaborative between teams and informed by evidence and expertise; and,
4) Risk management processes must be structured to include:
    a. Identification and assessment, producing an integrated and holistic view of risk to understand the council's overall risk profile.
    b. The selection, design and implementation of risk treatment options that support the achievement of outcomes and manage risks.
    c. The operation of integrated, insightful and informative risk monitoring, aligned with existing management.
    d. Timely, accurate and useful reporting on risk to enhance decision-making and to support management.
5) The overall approach to risk management should be continually improved through applying learning, experience and expertise.

Further, the council's Code of Corporate Governance (to be developed) sets out the council's wider governance arrangements and, specifically, how the council ensures it is doing the right things in the right way. The code will be developed in accordance with the seven core principles that should underpin the governance framework of a local authority, as outlined in the Chartered Institute of Public Finance and Accountancy (CIPFA) and the Society of Local Authority Chief Executives' (Solace) guidance. Compliance with the code is reported annually through the Annual Governance Statement.

The seven core principles of good governance are:

1) Behaving with integrity, demonstrating strong commitment to ethical values and respecting the rule of law;
2) Ensuring openness and comprehensive stakeholder engagement;
3) Defining outcomes in terms of sustainable economic, social and environmental benefits;
4) Determining the interventions necessary to optimise the achievement of the intended outcomes;
5) Developing the council's capacity, including the capability of its leadership and the individuals within it;

6) Managing risks and performance through robust internal control and strong public financial management; and,
7) Implementing good practices in transparency, reporting and audit, to deliver effective accountability.

It is the responsibility of the Joint Chief Executive and the wider Corporate Leadership Board (CLB) to establish this framework of governance and risk management at the council and to be accountable for its overall operation. Through the operation of this risk management strategy, the CLB determines and continuously assesses the nature and extent of the risks the council is exposed to, as well as those it is prepared to accept. It ensures that organisational planning and decision-making reflects this assessment and that roles and responsibilities are clearly defined and understood, with appropriate escalation and delegation in place.

This strategy sets out the council's approach to risk management and how the latter principles are applied at Guildford Borough Council. Further detail on its application is included in the accompanying methodology document.

Types of risk

Building risk awareness and understanding of an organisation's risk profile is a key first step to the successful management of risks.

As a complex organisation with an ambitious Corporate Strategy, the council faces a diverse range of risks. For the ease of analysis, the risks faced by the council may be initially categorised by their type, largely reflective of their source as well as their potential impact.

It should be noted, however, that the types of risk set out below are not mutually exclusive; it is highly likely that a risk will not wholly reside within a single category and risks impacts may cascade throughout them.[2]

- **Internal –** these are risks that relate to the business-as-usual operation of an organisation and over which it has at least some ability to control and/or mitigate. Internal risks may be regarded as inherent risks insofar as they are fundamental to the organisation's role and purpose and can therefore be reasonably foreseen, though this does not negate the need for their management.

  Examples of internal risks include: fraud (internal and external); health and safety; information governance and data protection; events on our land and assets,

[2] Adapted from Management of risk in government: a framework for boards and examples of what has worked in practice. Available from: https://www.gov.uk/government/publications/management-of-risk-in-government-framework

procurement, safeguarding; and general capacity and capability, including that of delivery partners and other stakeholders. Delivering projects and change will also result in risk.

- **External –** these are risks that arise from the environment within which an organisation operates and usually concerns significant events, perils and external shocks. While external risks originate outside the organisation, they may be best regarded as being inherent to the external environment within which all organisations operate and can therefore be reasonably – though perhaps imperfectly – foreseen. The nature, role and purpose of the organisation will mediate the impacts of external risks. It is in this regard that in some areas internal and external risks overlap. In the local government context, for instance, local authorities have a statutory duty to plan for, and respond to, civil emergencies and, in doing so, use management tools such as reasonable worst case planning assumptions to influence preparations and plans for response.

  Examples of external risks include: civil emergencies included within the scope of the Civil Contingencies Act (2004); business continuity incidents; economic downturns; and geopolitical crises and macroeconomic shocks.

- **Strategic –** strategic risks are closely related to external risks in that their source usually lies outside of the organisation. However, they are distinct in that they concern and impact the organisation's fundamental objectives and reason for existence which, in the context of the council, includes strategic objectives set out in the Corporate Strategy and Medium-Term Financial Plan.

  Strategic risks can be immediate or slower burn in their impact. They usually result from a contextually particular and specific set of events and/or circumstances and, like external risks, are difficult to accurately foresee and/or predict, though a rough order of impact magnitude may be forecast. Their impacts are usually significant. It is in this way that strategic risks underscore the importance of general organisational resilience due to the fact that the modern external environment is characterised by significant levels of uncertainty.

  Examples of strategic risks include: changes in legislation and codes of practice; political instability (local and national); internal leadership capacity and turnover; and general organisational capacity and culture.

- **Major projects and programmes –** the delivery of major projects and programmes forms a crucial part of the council's Corporate Strategy priorities. Projects and programmes are usually described as 'major' based on their size and/or complexity, as

well as their status as being critical to achieving strategic objectives. Their size and associated impacts merit their separate treatment to the other types of risk faced. Indeed, the delivery of major projects and programmes presents significant interlinked risks to an organisation, including revenue and capital budget pressures (such as unforeseen costs or unrealised income); slippage in delivery timescales and a general failure to deliver against client and stakeholder expectations, especially in terms of quality and benefits.

While major project and programme delivery are integral to realising corporate priorities and objectives, it should be noted that not all projects and programmes *must* be delivered. Indeed, the choice to deliver a major project must be a conscious and prioritised one, founded on a sound evidential basis to support the reduction of uncertainty to a tolerable level. There are further choices relating to the means and approach of delivery which have considerable implications on risk.

It is crucial, therefore, that the approach to project and programme governance is integrated with the general approach to risk management, with risks considered and managed throughout the lifecycle, though the need for this is particularly acute in business case development.

Three lines of defence

The council has multiple teams, departments and individual roles that assist in the management of risk to achieve corporate objectives. Each has its own unique perspective and skillset that is essential to the overall management of risk, but as these functions are spread across multiple teams and directorates, it is important that duties are coordinated to best effect. The challenge is to assign specific roles and to coordinate activities so that there are no gaps in management activities or unnecessary duplication of effort. Without a consistent, cohesive and coordinated approach, the council's limited resources may not be deployed effectively and/or significant risks may not be identified or managed appropriately.

In recognition of this, the council operates a three line of defence model for risk management. The model provides a simple and comprehensive way to coordinate risk management activities, enhance organisational communication and clarify roles and responsibilities, underpinning effective internal control. Internal control refers to the dynamic and iterative series of processes, policies and procedures that are purposed with managing risk and exercising effective governance and assurance activities. Internal controls are found throughout the council and are inherent to its successful operation.

The three lines of defence model distinguishes between three groups (or lines) involved in effective risk management:

1) Functions that **own and manage** risks;
2) Functions that **oversee** risks; and,
3) Functions that provide **independent assurance**.

The model is predicated on the interlinked ideas that: (i) risk should not solely be left to risk management specialists; (ii) everyone in the council has some responsibility for risk management; and (iii) that the varying roles, parts and levels of the council play different, though complementary, roles within risk management. Indeed, it is the interplay between the latter that determines how effective the council is in managing risk and is of critical importance to the delivery of effective corporate governance.

The accompanying risk management methodology provides detailed information on how the model is implemented at the council. At this point, however, the model may be summarised as follows:

First line of defence

Management control is the first line of defence in risk management. It refers to management's primary responsibility and accountability for identifying, assessing, monitoring and managing

risks as part of the routine course of management and, ultimately, effective and efficient service delivery.

At Guildford Borough Council, Assistant Directors and service managers (collectively referred to hereafter as ‘management’) fulfil this function.

In this regard, the first line ‘owns’ risks and is responsible for the execution of the council’s response. Through a cascading structure of responsibility that aligns with the council’s management structure and hierarchy, managers design, operate and improve the policies, procedures and practices that manage risk in their service areas.

In so doing, management must be adequately skilled to identify risks and design and deliver their services in a way that brings risk to a tolerable level. This includes an awareness of risk management best practice and principles as articulated in this strategy and the accompanying methodology, as well as service specific policies and/or codes of best practice. It is similarly crucial that managers are aware of the council’s risk appetite to help guide management activities.

Adequate managerial and supervisory procedures must also be in place to ensure compliance and to highlight areas where controls have deteriorated or where the environment has changed. This should be supported by regular monitoring and reporting, as well as training and measures to maintain a shared situational awareness of the risk profile of the service and how this may change over time.

As we have seen, risks may emerge from a variety of sources. A key source for identifying risks is the annual service and financial planning process where service budgets, objectives and deliverables are set. However, not all risks (such as ‘external’ and ‘strategic’ risks) can be reasonably foreseen as part of the annual service and financial planning cycle. The council therefore requires service management to maintain a constant stance of vigilance to risk. Doing this well is reliant on management having the necessary skill and autonomy to foresee and respond to risks affecting their service, which itself is in turn founded on robust and supportive risk management systems, processes and a wider supportive organisational culture.

Second line of defence

The second line of defence is comprised of the specialist, corporate functions within the council that support and monitor services in their approach to risk management and, in so doing, support the establishment and effective functioning of the internal control environment. Put differently, the second line ensures that the first line of defence is properly designed, is in place and is operating as intended.

At the council, second line functions/departments include: Health and Safety; Finance; Human Resources; Legal; Procurement; Emergency Planning and Business Continuity, amongst many others.

The second line supports management by bringing their specialist expertise and knowledge of best practice and wider sector/industry trends to help ensure that risks are effectively managed. They are responsible for designing policies, setting direction, ensuring compliance with controls and other core risk management processes, as well as providing assurance on the effectiveness of the internal control environment.

Examples of activities undertaken at the second line include:

- Supporting management with the development of policies, strategies and plans, with particular consideration of the risk implications therein;
- Developing, implementing and maintaining the organisation's risk management strategy and methodology, often collectively termed the 'risk management framework';
- Identifying risks and issues and escalating these for management attention, including those arising from a deterioration in the internal control environment as well as changes in the external environment;
- Setting and continually reviewing the organisation's risk appetite, and identifying instances of deviation, implicit or otherwise;
- Assisting management in developing processes and controls to manage risks and issues within a service area and across the organisation more broadly; and,
- Provide training, advice and guidance on risk management processes.

As management functions, the second line of defence may directly intervene in modifying and developing the internal control environment. However, given their status as a management function, the second line cannot be regarded as being truly independent of management.

Third line of defence

The third line is often regarded as those functions that are 'external' to, or independent of, an organisation. The latter may take the form of being physically external inasmuch as the service is provided by an external body that is independent of the council, as with external audit or outside regulatory bodies. Alternatively, externality may be defined by functional independence from management, as with internal audit.

In the context of the council, the third line of defence is primarily composed of the council's internal and external audit functions, as well as other ad hoc consultancy work that may be commissioned by management to provide assurance or best practice expertise.

A professional, independent and objective internal audit function is a key element of ensuring good corporate governance and risk management. Through a risk-based approach to its work, internal audit provides an objective evaluation of how well the council assesses and manages its risks, including the design and operation of the first and second lines of defence.[3] Management's response to its observations helps strengthen the effectiveness of risk management, control and, ultimately, corporate governance and leadership.

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

Other sources of assurance include work commissioned by external consultancy services, such as the Local Government Association (LGA), Chartered Institute of Public Finance and Accountancy (CIPFA) and Solace (Society of Local Authority Chief Executives and Senior Managers). External regulatory bodies may also be regarded as residing at the third line, especially where they set requirements purposed with strengthening controls in an organisation. Examples include the Regulator of Social Housing and the Food Standards Agency. In the local government context, government departments – such as the Ministry of Communities, Housing and Local Government (MHCLG), His Majesty's Treasury, etc. – fall within this category, too.

Crucially, when coordinated effectively, external audit, regulators and other bodies can be regarded as being additional lines of defence, providing assurance to senior management and councillors. However, given their specific scope, information concerning risk is usually less extensive than that provided by the 'internal' three lines of defence.

[3] For additional information, see the Public Sector Internal Audit Standards. Available from: https://www.gov.uk/government/publications/public-sector-internal-audit-standards

The risk management cycle

Effective risk management is founded on robust and systematic risk **identification, assessment, treatment and monitoring and reporting.** Collectively these processes are known at the council as the risk management cycle.

Risk identification

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

A mature risk culture is founded on a well-developed understanding and perception of risk, often known as 'risk awareness'. The ultimate aim of risk identification is to build a rich and evolving picture of the council's overall risk profile. This is a continual and ongoing process and encompasses all areas of the council's operations.

There are a range of tools and techniques for identifying the risks that may impact the council. While these are explored in greater detail in the accompanying methodology document, the following factors, and the relationship between them, should be considered in identifying risk:

- Tangible and intangible sources of risk;
- Changes in the external and internal context;
- Uncertainties and assumptions within options, strategies and plans;
- Indicators of emerging risks;
- Limitations of knowledge and reliability of information; and,
- Any potential biases and beliefs of those involved in decision making.

Risks must be identified and considered regardless of whether they are under the council's direct control.

Activities concerned with identifying risks are embedded throughout the council in accordance with the three line of defence model. Under this model, service management have primary responsibility for the management and identification of risks. A key mechanism for identifying risks is the annual service and financial planning process, where management are expected to document the risks they face and consider what the potential impacts may be in their service risk register.

However, risks may emerge and/or be identified at points outside of the service and financial planning cycle. Indeed, the risks set out in service plans are invariably those known as 'known knowns' or 'known unknowns' – that is, risks where the likelihood and/or impact is reasonably available for management to foresee, measure, assess and plan for as part of business as usual. Not all risks are reasonably foreseeable, however, and so management must be

supported by other systems and processes that are established throughout the three lines of defence model to identify risks as they emerge, as well as where the control environment may have broken down. It is similarly crucial to ensuring that the council's risk profile is well informed and robust.

Once a risk has been identified it should be documented and recorded as a key first step of the risk management cycle. While, as noted, there are various mechanisms for identifying risks (explored in greater depth in the accompanying methodology document), for purposes of ownership and accountability, **all risks must have an allocated owner**. Most risk owners will be members of the Joint Leadership Team; a corresponding Lead Councillor (Executive Member) should also be identified.

Risk assessment

Once a risk has been identified it should then be assessed. This is because that while each risk in isolation may be significant, a form of standardised measurement is required to evaluate its relative significance and to inform the allocation of finite resources to managing it. Without a standard for comparison, it is not possible to compare the overall significance of a risk or to aggregate risks across the council. Risk assessment thus facilitates a prioritised response to risks. It is underpinned by risk **analysis** and **evaluation**.

The purpose of risk analysis is to support management to undertake a detailed consideration of the nature and the level of risk that is faced. Indeed, while the potential impacts of risks are initially considered in the risk identification phase, risk analysis adds further insight to this by providing a mechanism for the scoring of risks in terms of their **likelihood** and **impact.**

The analysis should be carried out using the assessment scoring matrix as defined in the methodology document which accompanies this strategy. An analysis of risk can be undertaken with varying degrees of detail and complexity, depending on the scale of the risk, the availability of evidence and the resources available. Further information on how this should be carried out at the council is provided in the accompanying methodology document.

Risks should initially be assessed in terms of their **inherent risk**. Inherent risk refers to the likelihood and impact of a risk occurring in the absence of controls or mitigations being in place. A control is a process, policy or activity that reduces the likelihood of a risk materialising. A mitigation reduces the impact of a risk should it occur. The impact of risk is considered against a number of risk categories, as set out in the accompanying methodology document.

Risk appetite

The next step is to undertake an analysis of the effectiveness of the controls and mitigations in place, otherwise known as the **residual risk** level. Once this analysis is complete, an evaluation should follow in comparing the results to the nature and extent of risk that the council is prepared to accept – otherwise known as **risk appetite** – to determine whether any additional action is required.

Overall, the council recognises that times of uncertainty and challenge require risks to be taken to achieve its ambitious corporate objectives. The council is **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 minimise risk.

The risk appetite has been set in accordance with the council's Corporate Strategy and values and in consultation with the Corporate Governance and Standards Committee, the Joint Leadership Team and the Executive. Its articulation helps establish the accepted boundaries for risk taking and ensures that risks accepted by the council are proportionate to the possible rewards and the achievement of corporate objectives.

Articulating an appetite for risk is thus about identifying the point at which decisions regarding the management of risk are escalated for decision and/or wider corporate awareness. Risk appetite is a crucial part of the framework within which decisions are made at the council. The appetite for risk should not be static and inflexible; instead, it should serve as a guide in the decision-making process.

The assessment of the current risk against the risk appetite allows management to identify whether the controls and mitigations are adequate and applied appropriately to the level of risk faced. If the controls and/or mitigations are found to be inadequate, consideration should be given to whether the risk should be included on the relevant corporate risk register.

In being outside of the council's risk appetite, corporate risks are those that reside outside the usual course of management and require a wider corporate response or awareness, utilising services from across the three lines of defence. The council maintains two corporate level risk registers:

- **Strategic –** risks that could have an impact on the council's medium to long term priorities and objectives as articulated in the Corporate Strategy or other corporate level policies and strategies, including the Medium-Term Financial Plan (MTFP).

  Strategic risks usually originate from the external environment within which the council operates, though the internal environment will mediate the impact of the risk itself, either through mitigating or exacerbating it. Strategic risks may also stem from an internal source, such as a major project, if the impact merits its categorisation as a strategic risk.

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

- **Operational –** risks that are encountered in the delivery of services and which affect service objectives, as defined in service plans. Operational risks are usually managed as part of the usual course of management by services. However, where the operational risk cannot be managed within the service or if it is outside of the council's risk appetite, then it should be considered for inclusion on the operational risk register.

  Members of the Joint Leadership Team (principally Assistant Directors) have responsibility for operational risks.

It is important to note that the creation of corporate level risk registers does not preclude other risk registers being created and maintained as tools to support the successful management of risk.

For instance, projects and programmes introduce change and therefore involve varying degrees of risk in correlation to their scale and/or complexity. The council's approach to project and programme management includes advice and guidance on the management of risk to support effective governance, planning and delivery. At this point it should be noted, however, that project and programme risks are different in nature to corporate level risks. Indeed, projects and programmes are invariably driven by a degree of choice insofar as the council has discretion concerning *whether* – in the context of a fully appraised business case – to deliver a project, or, alternatively, *how* to go about delivery.

Project and programme risks are therefore significantly different in nature to 'business as usual' risks, where, as a result, it is important that they undergo an appropriately tailored approach to risk management and in proportion to the level of risk faced. The detail of this is addressed in the council's project and programme management framework, though further information is also provided in the accompanying risk management methodology.

Risk treatment

Risk treatment refers to the various options that are available to management in managing a risk.

As we have seen, the primary responsibility for risk management lies with service management at the first line of defence. The first line therefore 'owns' the risk and – in collaboration with services throughout the three lines of defence – is responsible for designing processes, procedures and policies to manage risk to an acceptable level.

Risk treatment is concerned with selecting the most appropriate course of action for managing a risk, balancing the potential benefits of action against the costs and disadvantages, as well as against the likelihood and impact of the risk itself. Reference to the council's risk appetite is crucial to completing this proportionately and effectively, though consideration must also be given to the council's ability to influence the risk, especially as many risks are outside the council's ability to influence.

Risk treatment options include:

- **Avoidance –** stop doing the activity that creates the risk, or elements therein.
- **Transfer –** transfer all or part of the risk to another party, such as through taking out insurance or through engaging an agency or contractor.
- **Reduce –** take steps to reduce the likelihood and/or impact of the risk, such as through introducing new or modifying existing controls and mitigations.
- **Accept –** accept the risk exposure and take no measures to reduce the likelihood and/or impact.

Before an option is selected an options appraisal should be carried out to determine the most appropriate course of action. Doing so forms a core component of management's primary risk management role at the first line of defence. Management may decide that it is appropriate to formally document this options appraisal in certain circumstances, particularly 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. All decisions taken must be done so under the authority of the appropriate individual authorised by the Constitution and scheme of delegation.

Risk monitoring and reporting

Once a risk has been identified, assessed and treatment options selected, it should be regularly monitored and reported on. Doing this effectively is predicated on ensuring that the right and appropriately tailored and presented information is given to the right people, at the right level and at the right time. Taken together, robust risk monitoring and reporting is integral to providing assurance of the overall effectiveness of the risk management cycle and is a core component of effective corporate governance.

Risk monitoring and reporting helps ensure:

- That the corporate **risk profile remains relevant** and up to date and that it is well understood across the council;
- That **effective decision-making** is maintained through the timely provision of information on risk, giving management and other key stakeholders confidence and assurance that the right decisions are being made in accordance with the risk appetite;
- That risk, planning, performance and prioritisation discussions are conducted in a **holistic and integrated manner**;
- That stakeholders have assurance over risk management activities, as well as the adequacy of the overall approach to risk management; and,
- The **ongoing adequacy and effectiveness of internal controls**, as well as coordination with other sources of assurance.

The monitoring of risk should be carried out before, during and after the implementation of risk treatment activities. The results should be incorporated into the council's wider approach to governance and leadership, as well as through organisational wide measures concerned with performance management, measurement and reporting. Doing so is purposed with:

- Transparently communicating risk management activities and outcomes;
- Providing timely and actionable information for decision-makers;
- Improving risk management activities; and,
- Assisting with interactions with key stakeholders, ensuring a consistent understanding of risk and efforts to reduce it.

As summarised above, the three lines of defence model defines how each level integrates with the others to manage risks and design a system of internal control that provides assurance through ongoing, regular, periodic and ad-hoc monitoring, review and reporting of the results. Through utilising the three lines model, gaps in coverage should be identified, minimised and, ultimately, eliminated wherever possible.

Risk reporting is the means to communicate the results of risk monitoring and management activities.

The Corporate Leadership Board, as the apex of officer governance, defines the overarching approach to risk reporting at the council in collaboration with the council's Executive. This is supported by the work of the council's Corporate Governance and Standards Committee which has a constitutional role to advise Full Council on the adequacy of the council's risk management framework and the internal control environment.

There are different categories of risk reports utilised at the council, which include:

1. **Risk registers –** as noted above, 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. For

instance, strategic risks should be reviewed at least quarterly, while a project risk register may require more regular review. 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.

Risks that do not meet the threshold for escalation and inclusion on corporate risk registers (i.e. those that are within appetite) should still be recorded, usually on a service risk register. Additional detail on risk registers and how risks are escalated at the council is included within the accompanying methodology document.

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 organisation more widely. Such reports are commonly grouped by area or impact theme, such as economic issues affecting budgets, service delivery and investment position. Indeed, 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.

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 as per the above, or when aligned to the usual decision-making processes that require it. In the context of local government, the latter may include strategic activities such as decisions around treasury management activities, lending on the inter-authority market and/or the development of the capital programme, including specific projects within it.

   A deep dive report may be used to support management intervention when there is concern about the adequacy of the control environment and/or risk management activities, as well as where the external control environment has changed substantially. The report may also be used to consider whether it is appropriate for a risk to be added to a corporate risk register or, indeed, whether it ought to be closed, deescalated or merged into another. In so doing, deep dive reports give management and other key stakeholders assurance on the approach to risk management activities and allows them to provide specific management direction.

The accompanying risk management methodology document sets out the council's approach and expectations concerning risk reporting in greater detail.