Reigate & Banstead Borough Council

Risk management strategy

2023/24 to 2025/26

Contents

Strategy Summary 3
Introduction 5
Strategy statement 6
Objectives 7
Benefits 7
Managing risks 8
Risk 8
Risk management 8
Types of risk 10
Three lines of defence 12
The risk management cycle – a framework for assurance 15
Summary 15
Risk identification 17
Risk assessment 19
Risk treatment 24
Risk monitoring and reporting 26

Strategy Summary

Setting the scene

The purpose of our Risk Management Strategy is to explain how the Council identifies, assesses, manages and reports on the risks that it faces in delivering its objectives.

Risk management refers to the set of coordinated activities designed to manage risk and exercise internal control within an organisation. The Council's approach to risk management considers **internal** risk, **external** risk, **strategic** risk and **major project** risks.

The way we **define risk** is consistent with Government guidance: we identify the **cause**, the potential **event**(s) that might be experienced and the **consequences** of the event(s).

Defining the Council's appetite for risk

The Council is committed to being **risk aware rather than risk averse**. Unfortunately, risk is ever present and unavoidable.

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

The three line of defence model

Key roles and responsibilities

Heads of Service: Identify, implement and maintain effective internal controls to manage risk on a day-to-day basis and escalate risks as appropriate.

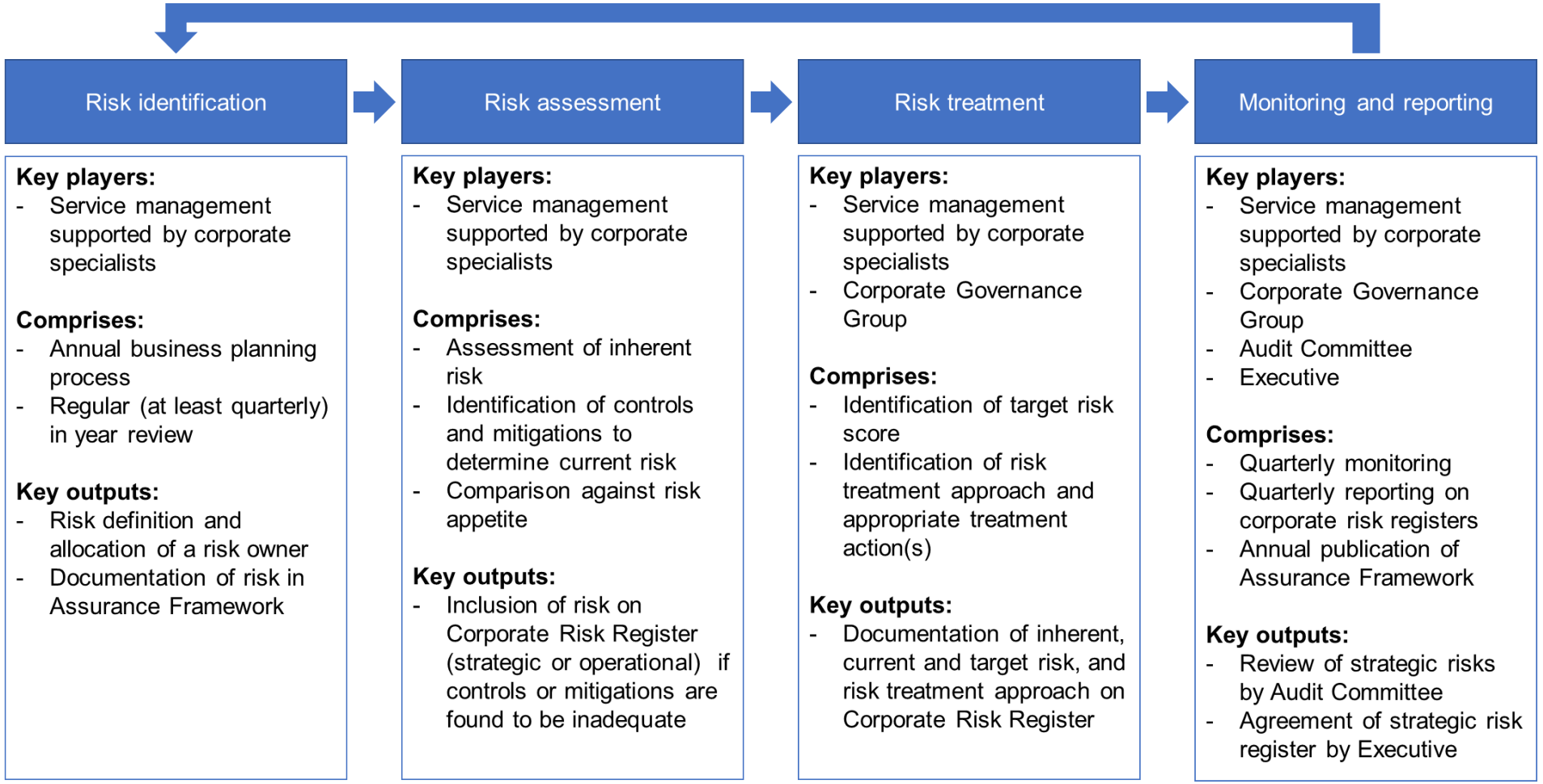
Corporate Governance Group: Overall responsibility for day-to-day management of risks

Audit Committee: Provides independent review of and assurance on the Council's risk management approach and internal control frameworks

The Executive: Holds overall responsibility for ensuring that risk is adequately considered and addressed across the full range of Council activities.

How we manage risk

Risk is managed using a structured approach, defined as the **risk management cycle**.



Introduction

This strategy sets out Reigate & Banstead Borough Council's commitment to effective risk management.

In broad terms, risk may be defined as the effect of uncertainty on objectives. Risk management refers to the set of coordinated activities designed to manage risk and exercise internal control within an organisation.

The purpose of the Council's risk management strategy and framework is to articulate how the Council identifies, assesses, manages and reports on the risks that it faces in delivering its objectives. The strategy will help ensure the integrity of risk management to all organisational activities and decision-making, as well as the fostering of a positive and mature risk culture.

Whilst the strategy sets out the overarching approach to risk management at the Council, an accompanying risk management methodology sits alongside it. The methodology defines the method and processes that are followed in pursuit of the strategy, including detailed roles and responsibilities.

The strategy and methodology have been designed in recognition of the fact that risk management is fundamental to effective governance and leadership and is similarly core to how the Council is managed and controlled. The two documents therefore form the foundation of robust risk management activity at the Council, thereby helping to contribute to the effectiveness of the wider corporate governance framework and the achievement of corporate objectives.

Strategy statement

Reigate & Banstead 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. Effective risk management is an integral part of all Council activities and, in adopting this strategy, the Council is setting out its commitment to ensuring that risk is appropriately considered in all aspects of informed decision making.

The Council is committed to being risk aware rather than risk averse. Unfortunately, risk is ever present and unavoidable. As a complex organisation with bold ambitions that operates in an inherently uncertain environment, it is not possible for the Council to be risk averse and to be successful.

The Council **prefers a cautious approach to risk** but acknowledges that in some areas it is necessary to accept higher levels of risk to ensure the achievement of objectives. The Council is therefore committed to embracing the discipline of risk management to improve planning, performance, decision-making and to help identify and respond to challenges and to keep risks within the risk appetite.

This strategy recognises that the core practices and principles of risk management should be embedded throughout the organisation and underpinned by a mature and supportive risk culture that encourages innovation, awareness, transparency and ownership.

The Council is keen that risk management does not stifle innovation and the delivery of services for residents and businesses. Instead, risk management should underpin all activities in fostering an environment within which informed risks can be taken, providing they are actively managed in accordance with the Council's risk appetite.

The strategy will therefore ensure that:

- Risk management contributes to ensuring effective service delivery and the achievement of the Council's objectives;
- The ownership and accountability of risks are clearly assigned throughout the Council;
- Members and officers acknowledge and understand the importance of risk management as a good governance process, by which risks are identified, evaluated and managed effectively; and,
- Effective monitoring and reporting mechanisms are in place to review the Council's exposure to, and management of, risks.

Objectives

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

- Integrate risk management into the strategic and operational processes, procedures and culture of the Council, thereby maintaining good governance;
- Enable effective, risk-based decision making;
- Provide management with early warnings of any potential problems so that a response can be made in a planned, preventive way;
- Enable management to be clear on the activities over which they require assurance and the extent and adequacy of that assurance based on risk;
- Ensure that risk is identified, managed and reported on in accordance with established best practice, appropriately tailored to the Council's risk profile;
- Foster a culture of effective risk awareness and ownership;
- Anticipate and respond to changing social, environmental and legislative requirements; and,
- Minimise loss, disruption, damage and injury.

Benefits

An effective approach to risk management will deliver a number of benefits, including:

- Improved standards of corporate governance;
- An enhanced ability to deliver against corporate objectives, with risks clearly understood, documented and controlled;
- Improved strategic and operational decision-making;
- Improved risk awareness amongst staff and management;
- Enhanced financial control and reporting;
- The appropriate and effective use of resources;
- The minimisation of waste, including additional expense incurred and resources otherwise wasted;
- Cost avoidance; and,
- Improved staff, resident and member health and safety.

Managing risks

Risk

The government's Orange Book defines 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 in combination with another has the potential to give rise to a risk;
- An **event** is an occurrence or change of a set of circumstances. It can be something that is expected and which does not happen or something that is not expected but does happen. Events can have multiple causes and consequences and can affect multiple objectives; and,
- **Consequences** are the outcome of an event affecting objectives, which can be certain or uncertain, can have positive or negative direct or indirect effects on objectives, can be expressed qualitatively or quantitatively, and can escalate through cascading and cumulative effects.

The Council is a complex organisation that provides a diverse range of important services – many of which are statutory – to residents and businesses. There are risks inherent to delivering these services. There are similarly risks inherent to the risk profile of local government. The Council also operates in an external environment that is widely acknowledged as being 'radically uncertain'. The recent Covid-19 pandemic, economic and geopolitical crises merely underscore this.

Due to its role and the uncertain context within which it operates, risk is thus unavoidable and inherent in everything that the Council does. The Council cannot be blanketly risk averse and deliver for our residents and businesses.

Risk management

The Orange Book defines risk management as a coordinated set of activities that are designed and operated to manage risk and exercise internal control within an organisation.

Taking the unavoidable nature of risk into account, risk management allows an organisation to systematically identify risks, evaluate their potential consequences and determine the most appropriate way of controlling and monitoring them, with the ultimate objective being to

---

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

achieve corporate objectives. Successful organisations therefore embrace risk and use risk management to enhance their strategic and operational planning and prioritisation.

As the Orange Book notes, risk management should be regarded as a core component of corporate governance and leadership. Put simply, it is fundamental to how the Council is directed, managed and controlled at all levels.

The Council's Code of Corporate Governance sets out the Council's wider governance arrangements and, specifically, how the Council ensures it is doing the right things in the right way.[2] The code has been 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.

The seven core principles of good governance are:

1. Behaving with integrity, demonstrating strong commitment to ethical values and respecting the rules 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.

In achieving these principles, risk management should be integral to all strategic and operational activities and considered in all aspects of decision making. As an integrated part of the wider management system of internal control, risk management harnesses and coordinates the various activities across the Council that identify and manage risks to a common effect.

[2] Reigate & Banstead Borough Council, Code of Corporate Governance. Available here: https://www.reigate-banstead.gov.uk/info/20400/your_council_documents/1285/code_of_corporate_governance

This strategy sets out the Council's approach to risk management and how the aforementioned principles are applied at Reigate & Banstead. The detail of its application is included in the accompanying methodology document.

Types of risk

The Council faces a diverse range of risks. They may initially be categorised by their type, which largely reflects the source of the risk as well as the potential impact. Understanding the type of risks faced by an organisation is a key first step to identifying the best action to take in managing the risk.

Whilst the range of risks faced by the Council are diverse, they may be grouped into four key categories, as set out below.[3] The types of risk are not mutually exclusive, and a given risk may not wholly reside within a single category.

- **Internal –** These are risks that are inherent to an organisation by virtue of its existence and/or the operational activities that it undertakes. The organisation will have some influence over internal risks, either to control and/or mitigate them.

  Examples include health and safety; information governance and data protection; safeguarding; fraud and general capability and capacity. The delivery of projects will also result in risks.

- **External –** External risks are those that arise from the external environment and could negatively impact the organisation. Some external risks may overlap with internal risks. For instance, local government has a statutory responsibility to plan for and respond to civil emergencies.

  External risks, whilst originating outside the organisation, may be regarded as being inherent to the external environment within which all organisations operate, though the nature of the organisation will affect and mediate the impact of the risk itself.

  Examples include civil emergencies, business continuity incidents and economic crises.

- **Strategic –** Strategic risks are closely related to external risks, though are subtly distinct. Strategic risks relate to external risks inasmuch as their source usually lies

[3] Adapted from Management of Risk in government: framework. Available from: https://www.gov.uk/government/publications/management-of-risk-in-government-framework

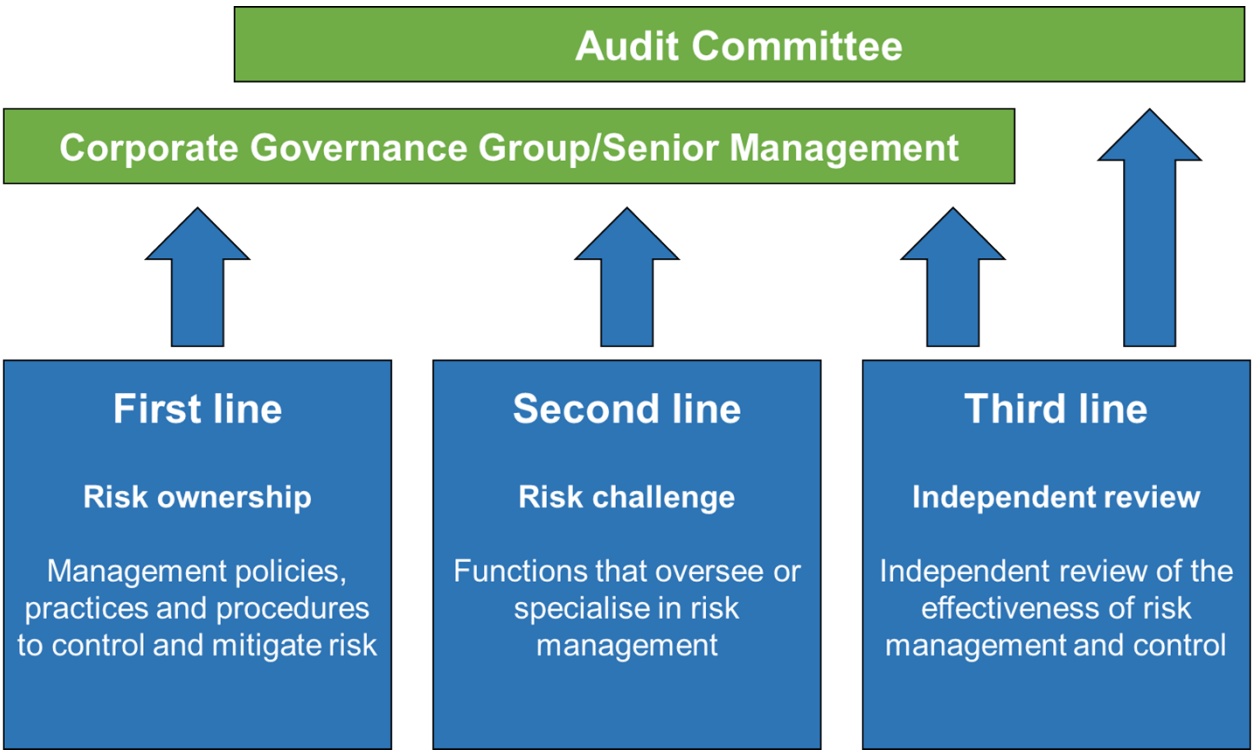
outside the organisation, though they are distinct in that they concern – and impact – the organisation's fundamental reason for existence. In the local government context, the latter refers to key corporate objectives set out in policy documents such as the corporate plan and medium-term financial plan.

Strategic risks usually result from a particular constellation of forces and dynamics which are inherently situationally specific and are not inherent in the same way as internal and external risks are. They may be immediate or slower burn in their impact. Their impacts are usually significant.

Examples include changes in legislation; political instability (local and national); internal leadership capacity; and general organisational capacity and culture.

- **Major projects –** Major projects are typically defined as such by their size and/or complexity. Major projects present significant risks to organisations in their delivery and indeed their non-delivery. Their size and associated impacts merit their separate treatment to other risks faced by an organisation. There are several reasons for this, including ensuring sufficient corporate visibility and governance standards as well as the fact that risks – of action and indeed inaction – should be considered within the development of the project's business case.

Three lines of defence



The Council operates a three line of defence model for risk management.

The model provides a comprehensive framework for considering, mapping and structuring the arrangements for exercising internal control to achieve effective governance and assurance. Internal control refers to the dynamic and iterative series of processes, policies and procedures that are purposed with managing risk and exercising effective governance. Internal controls are found throughout the Council and are inherent to its successful operation.

The three line of defence model is predicated on the tripartite concept that (i) risk should not 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, but complementary, roles within risk management. Indeed, it is the interplay between the latter that determines how effective the organisation is in managing risk and is of fundamental importance to the delivery of effective corporate governance.

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

The accompanying methodology provides more information on how the model is implemented at Reigate & Banstead. At this point, however, the model may be summarised as follows:

First line of defence

The first line of defence refers to service management's primary responsibility and accountability for identifying, assessing, monitoring and managing risks as part of effective service delivery.

As the first line of defence, Heads of Service and service managers (collectively 'service management') own and manage risks encountered within, or faced by, their service area.

Service management is therefore ultimately responsible for implementing and maintaining effective internal controls and managing risks on a day-to-day basis and in accordance with the Council's risk appetite, thereby helping to prevent risks from negatively affecting the achievement of service and corporate objectives.

Through the Council's management structure, managers design, operate and improve the policies, procedures and practices that manage risk in their area. Management should therefore be adequately skilled to identify, assess and manage risks. Moreover, adequate and appropriately tailored supervisory arrangements should be in place to ensure compliance with controls, supported by regular monitoring and reporting, training and measures to secure a shared situational awareness of the risk profile faced by the service and how this may change over time.

Risks may emerge from a variety of sources. The Council therefore expects and requires service management to consider all risks that may affect their service. A key source for identifying risks is the annual service and financial planning process where service budgets and objectives are set. It is recognised, however, that not all risks (e.g. 'external' and 'strategic' risks) can be reasonably foreseen as part of the annual budgeting cycle. As such, management require the skill and autonomy to respond to risks as they emerge and as required, though with appropriate escalation routes clearly identified in advance.

Second line of defence

The second line of defence is comprised of the specialist, corporate functions within the Council that support services in their approach to risk management. They may be regarded collectively – and through their interactions with one another – as being key components of effective internal governance.

Second line functions include teams such as Finance, Human Resources, Legal, Procurement, Health and Safety, Projects and Business Assurance and Emergency Planning, amongst several others.

The second line supports management by bringing expertise and best practice alongside the first line to help ensure that risks are effectively managed. They are responsible for designing policies, setting direction, ensuring compliance with controls and providing assurance on the effectiveness of controls put in place to mitigate risks. The second line also monitors and facilitates the implementation of effective risk management practices by management and supports risk owners in reporting on their risks, including progress on control and mitigation to Corporate Governance Group, the Audit Committee and the Executive.

Third line of defence

The third line is primarily made up of the Council's internal and external audit functions, as well as other ad hoc consultancy 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. Internal audit helps an organisation maximise performance and accomplish its objectives through bringing a systematic approach to the evaluation and improvement of the effectiveness of risk management, control and governance.

The Council is responsible for establishing and maintaining appropriate risk management processes, control systems, and governance arrangements. Internal audit plays a vital role in advising the Council that these arrangements – which are invariably found at the first and second lines of defence – are in place and are operating effectively.

External audit is charged 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.

The risk management cycle – a framework for assurance

Summary

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.

The risk management cycle is key to the creation of the Council's **assurance framework.**

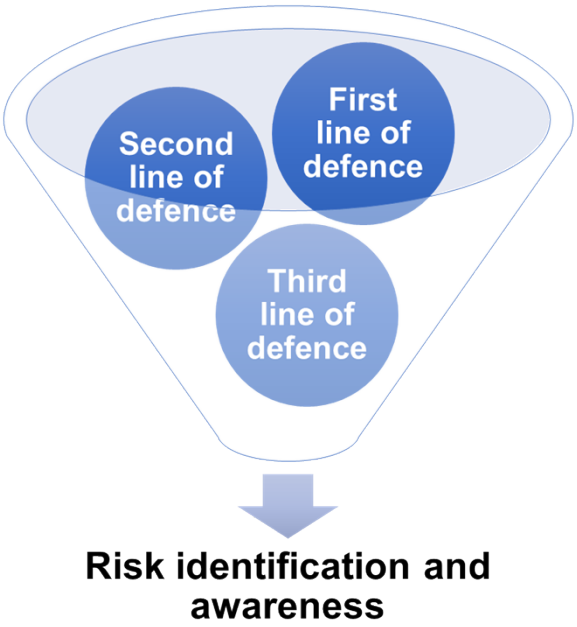
An assurance framework is a systematic means through which an organisation gathers, documents and demonstrates a comprehensive awareness of the risks it faces and the effectiveness of the controls that are in place. It provides a structured means of identifying and mapping the main sources of assurance relating to risks and helps coordinate management response to best effect. The framework also helps highlight where gaps in assurance exist. It cannot reasonably be expected to identify all specific permutations or situations within which risk may be manifested, but instead should focus and group risks by category for the ease and effectiveness of analysis.

The Council's assurance framework is distinct from risk registers which deal with risks of current concern and are being actively managed. The assurance framework sets out all risks, including those that are otherwise sufficiently controlled and do not therefore merit the same level of management attention. It is a product of, but likewise underpins, the Council's risk management cycle and a mature, risk aware culture.

The assurance framework should be regarded, alongside risk registers, as a central outcome of the successful operation of the risk management cycle. It is an outcome inasmuch as it takes the form of a written document. It is more than this, however, where its robust completion is indicative of mature and effective risk management systems, processes and culture. It is a fundamental supporting component of effective risk management, governance and control through giving management and key stakeholders confidence that the risk management strategy is working effectively.

The Council follows the aforementioned four key stages in its overarching approach to risk management, which are summarised in the sections that follow.

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. Risks should be identified and considered regardless of whether they are under the Council's direct control; we are fundamentally concerned with the impact that risks may have on our objectives to allow for an informed management response.

Activities concerned with identifying risks are embedded throughout the Council in accordance with the three line of defence model.

Service management have primary responsibly for the management and identification of risks. As such, a key mechanism for identifying risks is the annual service and financial planning process. As part of this process, service managers and Heads of Service are expected to document the risks that they face and consider what the potential impacts are.

However, risks may emerge and be identified at points outside service or other formal planning cycles. Indeed, the risks set out in service plans are often those known as 'known knowns' or 'known unknowns'. That is, risks where the likelihood and/or the impact is

reasonably available for management to measure, assess and plan for as part of business planning.

Not all risks are reasonably foreseeable or evident, and so the first line of defence must be supported by management systems and processes that are established throughout the three lines of defence model to identify risks as they emerge and to provide assurance that the Council's risk profile is robust and well informed.

Once a risk has been identified it should be documented and recorded as a key first step of the risk management cycle.

All identified risks must be allocated a **risk owner.** The risk owner is the appropriate individual and/or body that takes accountability for the risk, including efforts made to manage it. Most risk owners will be Heads of Service, though strategic risks may be owned by Senior Management. A corresponding owning Executive Member should also be identified.

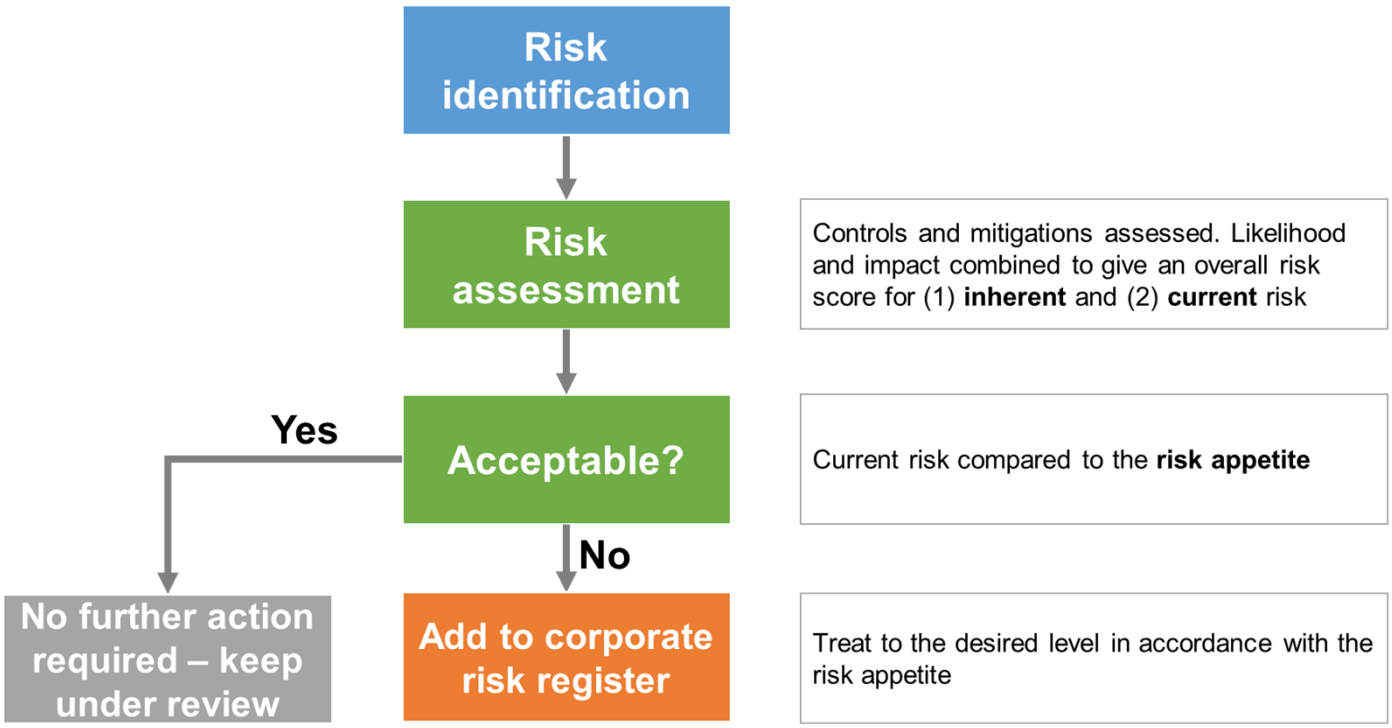
Risk assessment

Once a risk has been identified it should be assessed.

The potential impacts of a risk are initially considered in the identification phase. Risk assessment adds further detail and insight to this by scoring risks in terms of **likelihood** and **impact.** The assessment is carried out using the scoring matrix as set out in the methodology document which accompanies this strategy.

Risks should initially be assessed in terms of their **inherent risk**. Inherent risk refers to the likelihood and impact of a risk occurring without any controls or mitigations in place. A risk control is a process, policy or activity that reduces the likelihood of a risk materialising, whilst a risk mitigation reduces the impact 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.

The next step is assessing the controls and mitigations in place to ascertain their effectiveness, otherwise known as the **current risk.**



Risk appetite

Assessing the current risk must be done with reference to the Council's **risk appetite**. Risk appetite is defined as the amount or level of risk that an organisation is prepared to accept, tolerate or be exposed to in pursuit of its objectives. An organisation should have an overall risk appetite though it is also important to note that different categories of risk may well require different approaches and risk appetites.

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

The risk appetite has been set in accordance with the Council's wider values and strategy and in consultation with the Audit Committee, senior management and the Executive. Its formal articulation helps establish the accepted boundaries for risk taking and ensures that accepted risks and activity are proportionate to the possible rewards and, ultimately, the achievement of corporate objectives.

Defining the limits of a risk appetite is about identifying at what point decisions regarding the management of a risk are escalated for decision and/or wider corporate awareness. Risk appetite forms part of the overall framework around which decisions are made at the Council. Our appetite for risk should not be static and inflexible but instead should serve as a guide in the decision-making process. The clear definition of a risk appetite – broken down by risk type or category – supports the maintenance of this flexibility, as does the periodic review of the risk management strategy and appetite to ensure it remains fit for purpose and relevant to the Council's objectives and wider risk profile.

The assessment of the current risk against the Council's risk appetite allows management to judge whether the controls and mitigations are adequate and appropriately applied to the level of risk that is faced. If they are **adequate** in accordance with the risk appetite, no further action is needed; the risk should be included on the assurance framework document (if not already), alongside the corresponding controls and/or mitigations for ongoing monitoring and awareness. A future review date should also be identified, as well as a risk owner.

Conversely, it is possible that the controls or mitigations may be excessive and disproportionate to the level of risk faced. It is in this regard, therefore, that a robust risk assessment process, informed by a clear definition of risk appetite, supports the effective and appropriate deployment of the Council's finite resources to manage risk.

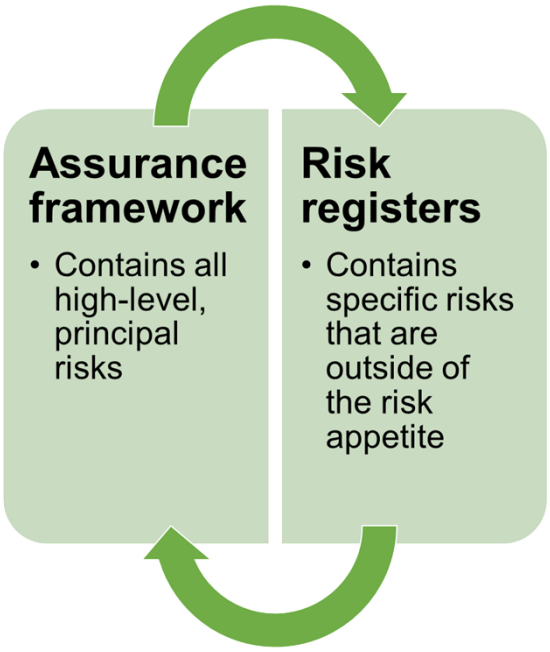
If the controls or mitigations are found to be **inadequate**, however, then consideration should be given to whether the risk should be included on the relevant **corporate risk register**.

Risk registers, at their simplest, are management tools used to record information on the risks that have been identified. It is in this regard that risk registers are similarly purposed to the Council's assurance framework.

Their distinctiveness from the assurance framework, however, is centred on the nature of the risks that they detail.

To explain, and as we have seen, the Council faces a considerable number of risks. These include risks inherent to the diverse range of services provided, but also those that stem from the environment in which the Council operates. Risks that have been assessed and which are regarded as sufficiently controlled and/or mitigated should be documented in the assurance framework.

It is important for purposes of governance, risk management and control, however, that primary attention is focused on risks of concern, as defined by their assessment against the Council's risk appetite.



The Council's risk registers should therefore **focus on those risks that are of concern** and are being actively **treated** or responded to by management. These are risks that are outside the usual course of management and may therefore require a wider corporate response, utilising services from across the three lines of defence.

The Council maintains two corporate level risk registers:

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

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

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

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

The creation and maintenance of corporate level risk registers does not preclude, however, other risk registers being created and maintained as useful management tools.

Projects and programmes, for instance, introduce change and therefore involve varying degrees of risk. The Council's project and programme management frameworks require projects and programmes to maintain risk registers to support effective project and programme governance.

Project and programme risk registers should give assurance that risks arising from them are being appropriately and effectively managed. Should this process raise a concern, then, in the same process as noted above, the risk may be considered for inclusion on the relevant corporate risk register. Risk registers are thus valuable sources of assurance and should be used in the compilation and maintenance of the assurance framework.

Risk treatment

Risk treatment is the collective term that refers to the various options that management have at their disposal to manage a risk.

The primary responsibility for risk management lies at the first line of defence – namely, service management. The first line 'owns' the risk and is responsible for designing processes, procedures and policies (known collectively as controls and mitigations) to manage risk.

The Council's utilisation of the three lines of defence model should be regarded as empowering first line management to manage and treat risks in accordance with the Council's overall risk management strategy and risk appetite. This is based on clearly articulated and well understood roles and responsibilities across the organisation, as well as management confidence to escalate concerns for wider corporate awareness and treatment when required.

Roles and responsibilities, including the Council's commitment to training management and officers in the core tenets of the risk management strategy are set out in detail in the accompanying methodology.

The effective, collective functioning of the three lines of defence should largely deal with risk management as part of business as usual, with risks identified and management processes designed to minimise and treat risk in accordance with the Council's risk appetite. The assurance framework serves as a key control within the three-lines of defence model inasmuch as it documents these risks, assesses their controls and mitigation as part of gaining assurance that risks are being treated appropriately. It is a key resource for the second and third lines in their assurance roles.

Previously unknown risks may emerge at any point, however, and present concern to management. Likewise, a previously identified risk may change substantively enough to render the controls in place inadequate against the corporate risk appetite, therefore changing its current score and raising cause for concern.

As we have seen, these risks, residing outside of business-as-usual arrangements, should be recorded on the relevant corporate risk register, with the **inherent, current and target risk score** clearly set out.

Whilst the inherent and current risk score have been defined above, the **target risk score** refers to where the Council is aiming to treat or manage the risk to. It sets out the desired end point of the risk management cycle. For purposes of governance and the exercising of effective internal control, the target risk score should be included in both the assurance framework and the corporate risk register.

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 risk appetite is crucial to completing this proportionately and effectively.

Consideration should also be given to the ability of the Council to influence the risk, in recognition that some risks are such fall outside of the Councill's scope for action.

Risk treatment options include:

- **Avoidance –** simply stop doing the activity that creates the risk, or elements therein.
- **Transfer –** transfer all or part of the risk to another party, such as to insurance or to an agency or contractor.
- **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.

Before a risk treatment option is selected, an options appraisal should be undertaken to inform the selection of the most appropriate and effective course of action. This appraisal forms a core component of management's primary risk management role at the first line of defence. Whilst there is no expectation that this options appraisal is formally documented and reported on, 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.

For the purposes of maintaining effective governance and control, all decisions taken must be done so under the authority of the appropriate individual authorised by the Constitution and scheme of delegation. This will usually be the risk owner.

Risk monitoring and reporting

Once a risk has been identified, assessed and treatment options chosen, it should be regularly monitored and reported on.

Effective risk reporting 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.

Risk monitoring and reporting helps ensure:

- That the corporate risk profile remains relevant and up to date and that there is a good awareness of it across the Council;
- That effective decision-making is maintained by providing timely information on risk, helping management and other stakeholders gain confidence that the right decisions are being made in accordance with the risk appetite; and,
- The ongoing the adequacy and effectiveness of internal controls and helps coordinate and effectively deploy other sources of assurance.

Taken together, robust risk monitoring and reporting is integral to the overall effectiveness of the risk management cycle and is a core component of effective corporate governance.

The assurance framework and corporate risk registers – serving as a comprehensive record of the risks faced by the Council – should be reviewed, at a minimum, on a quarterly basis by the identified risk owners, supported by the Projects and Business Assurance Team as part of their second line of defence responsibilities. However, risk owners are encouraged to review their risks on a more regular basis as part of the usual course of management.

Identified risks will have controls and/or mitigations documented, as well as the inherent, current and target risk scores. Risk monitoring should critically assess the latest situation and the current effectiveness of the controls and mitigations in place and consider whether the risk score has changed following risk management activities or a change in the inherent risk.

Risk monitoring should also provide updates on the implementation of the agreed controls and mitigations, which is particularly relevant for the risk registers which detail the risks of concern.

Other sources of assurance from the second and third lines of defence should be drawn upon in reviewing risks, such as that gained from recent internal audit reports or externally issued guidance notes.

Any resultant changes to risks should be recorded in the assurance framework or the relevant risk register. It is possible that – following a change in the risk environment – a risk may move from the assurance framework to the corporate risk register, or vice versa.

Risk reporting is a regular mechanism to provide key updates to key stakeholders and is the ultimate output of risk monitoring. High quality and timely reporting provides assurance to key stakeholders that the risk management cycle is working effectively and as intended.

It has the following benefits:

- The embedding of a consistent understanding of risks – existing and those that are emerging – across the Council, reducing uncertainty and promoting risk awareness;
- Monitoring progress in the management of risks to the target level;
- Enabling wider corporate awareness of the effectiveness of internal controls and providing information to support timely and informed interventions as required;
- Providing assurance to key stakeholders that risks are being effectively managed; and,
- Providing oversight of business activities, supporting responses to unplanned events that may threaten the delivery of corporate objectives.