Guildford Borough Council

Risk Management Strategy and Policy 2022-2025

Origination/author:	Stephen Benbough, Strategy & Communications Manager
Policy Owner – Service:	Strategy and Communications
This document replaces:	Risk Management Strategy and Framework
Executive approval:	April 2022
Last Review Date:	n/a
Next Review Date:	2023 (annually)

Contents

Part A: Guildford Borough Council Risk Management Strategy

Introduction

The Risk Management Strategy sets out our approach to risk management at a strategic level, whilst the Risk Management Policy in Part B of this document, and the guidance documentation accompanying it, set out the approach at an operational level.

Risk can be defined as “an uncertain event that, should it occur, will have an effect on the Council’s objectives and/or reputation.” It is the combination of the probability of an event (likelihood) and its effect (impact). Risk management is the “systematic application of principles, approaches and processes to the identification, assessment and monitoring of risks.”

The purpose of this Strategy is to briefly outline the current position of the Council relating to risk management and give a high-level view of how we will improve those processes and our approach to risk management.

The scope of the Risk Management Strategy and Policy covers the corporate processes behind risk management. It does not replace risk processes used for health and safety, business continuity or emergency planning, but instead supports those activities by establishing a framework for their escalation if appropriate.

Our commitment to risk management

The Council recognises that risk is unavoidable, and sometimes necessary to achieve its objectives. Risk management is an integral part of good management and governance, and the Council has a legal duty to have risk management arrangements in place. We are committed to ensuring risk management is part of our decision making with structures and processes in place to ensure the risks are identified, assessed and addressed in a consistent way and in accordance with the appetite and objectives of the Council.

Council-wide ownership and accountability for managing risk is critical to the success of our services and the achievement of our corporate objectives. We require all internal services to actively anticipate and manage their business risks, identify opportunities and mitigate any threats in line with their risk tolerances. This ensures a consistent approach where the risk profiles of each service are transparent to provide a whole organisation portfolio approach to risk management.

The next few years will continue to present significant challenges for the Council in delivering its services. The challenges will mean that we need to develop a different model for local government through differing methods of service delivery including commissioning services, partnership-working or exploring alternative service delivery models. Whilst these changes create opportunities; they also create risks and uncertainty. As new ways of working emerge, the risk management process will need to adapt to respond to these.

The Council’s attitude to risk is to operate in a culture of creativity and innovation, in which all key risks are identified in all areas of the business and the risks are understood and managed, rather than avoided.

Current position

In February 2021 KPMG produced an audit report reviewing the Council's processes and controls for risk management. Since then, the Council has developed a new framework for risk management including this strategy and policy, and risk register templates to strengthen our arrangements.

Outcomes of risk management

The desired outcome for risk management is the effective management of risk across the whole organisation resulting in the anticipation and resolution of risks before they become issues, and the leveraging of potential opportunities. We aim to ensure that we have the correct level of control in place to provide sufficient protection from harm, without stifling opportunity and development.

The main objective for this Strategy and Policy is to outline, implement and maintain a consistent approach to risk management across the Council, including common methods of risk identification, assessment and monitoring. In addition, the new framework included in the Policy will set out the governance and reporting processes at the various levels of risk management. As the new framework embeds across the organisation, the results will be: a common understanding of the Council's risk management processes; better identification, assessment and monitoring of risks, and improved risk governance processes.

How will we achieve these outcomes?

To achieve the outcomes set out above we will:

- Implement and maintain a robust and consistent risk management approach that will identify and effectively manage strategic, service and programme/project risks.
- Ensure accountabilities, roles and responsibilities for managing risks are clearly defined and communicated within risk registers.
- Consider and manage risk as an integral part of business planning, service delivery, key decision-making processes, and project and partnership governance.
- Communicate risk information effectively through a clear reporting framework.
- Increase understanding and expertise in risk management through targeted training and the sharing of good practice.

To measure the performance of this Strategy the Risk Management Group will develop indicators relating to the effect of mitigations on risk RAG ratings. The results of further external audit reviews will also be considered when assessing the performance of the Strategy. In the longer-term, the impact of risks materialising will reduce as a result of an effective risk management framework, including financial penalties for breaches and/or insurance costs.

Monitoring of the Strategy and Policy

The Risk Management Strategy and Policy will be monitored and reviewed by the Risk Management Group to ensure our approach takes account of changing legislation, government initiatives, best practice and experience gained within the Council.

Approval of minor changes is delegated to the Strategy and Communications Manager in consultation with the Risk Management Group and the relevant Lead Councillor. More fundamental changes will be escalated to the Executive in line with the Council's strategy and policy review processes.

Key services

All services will be key to ensuring the risk management framework is implemented fully and successfully. Specific services will have a role in the Risk Management Group relating to the risk domains (Finance, Legal/Regulatory, Reputational, Health & Safety, Service Delivery). The Strategy, Performance and Events team has the key role in the maintenance and reporting of the risk management framework.

Part B: Guildford Borough Council Risk Management Policy

Introduction

The purpose of this Policy is to set out the approach to risk management at an operational level, to outline the roles and responsibilities relating to risk across the Council, and to illustrate the main reporting framework and key controls. It should be read in conjunction with the Risk Management Strategy (Part A) and will be reviewed and updated at the same time.

The scope of this Policy is outlined in the Introduction in Part A of this document (the Risk Management Strategy). The risk management approach and processes set out in this Policy will be underpinned by a set of more detailed guidance documents which contain further information on assessment of risks, operation of risk registers, and the risk matrix.

Risk categorisation

Risks will be categorised into high level risk domains within the risk register. Most risks will have impacts that span multiple risk categories and high-level risk domains allow risks to be categorised according to the biggest impact on the Council should the risk materialise. High level risk domains are useful to understand the general nature of a risk and to help ensure the right officers are monitoring and dealing with it.

Risks will be categorised into the following domains universally across the risk registers:

Financial – risks that could impact on the financial viability of the Council or the budget, or that could result in financial claims, fines or penalties.
Reputational – risks that could result in negative publicity or damage the Council's reputation.
Service Delivery – risks that could interrupt service delivery, particularly statutory, key or high priority services.
Health and Safety – risks that could impact the health and safety of employees, councillors, residents and/or service users or that breach the health and safety rules.
Legal/regulatory – risks that could expose the Council to legal challenge.

Where a risk does not fit into one of the above five categories the risk owner should temporarily assign it a category that enables it to be reviewed and mitigated appropriately. For example, this could be technological if it is an IT related risk, or information governance if it relates to data protection. As the Strategy, Performance and Events team monitors and supports the risk registers, the risk categories will be reviewed, and any emerging frequent categories will be added.

Risk Registers

This Risk Management Policy covers three main levels of risks: corporate, service and programme/project. The risk registers are aligned to these levels. It is important to define the levels of risk in order to deal with risk in the most appropriate way and through the most appropriate risk register.

Corporate

The highest level of risk is managed at this level. Risks included in the corporate risk register should be ones that could have an effect on the successful achievement of our long-term core purpose, priorities and outcomes. This includes:

1. risks that could potentially have a council-wide impact and/or
2. risks that could happen/apply to any service.

Service

This level relates to the operational risks within services. Risks at a service level that could influence the successful achievement of the service outcomes / objectives are service risks. Risks that have originated in other risk registers (programme/project) may also be service risks if they impact service outcomes. Service risks that culminate to have a corporate impact or that require escalation should also be reflected in the Corporate Risk Register.

Programme/project

This level concerns risks that could have an effect on the successful achievement of the programme or project's outcomes / objectives in terms of service delivery, benefits realisation and engagement with key stakeholders (service users, third parties, partners etc.). These could be risks from the initial mandate or business case stage in a programme or project, or they may arise during the project lifecycle. Programme/project risks that culminate to have a service or corporate impact, or that require escalation, may also be reflected in the Corporate Risk Register and/or Service Risk Register.

Risk appetite and tolerance

Risk appetite

Risk appetite is the level of risk an organisation is willing to accept and considers both the willingness to take risk and the level of control. The risk appetite should set the 'tone from the top' on the level of risk we are prepared to accept on the different risk domains.

Risk tolerance

After agreeing mitigating actions, the residual score of a risk will be assessed according to the corresponding risk tolerance. The outcome of this assessment will determine whether or not the risk is escalated.

Effective risk management

The Council's Risk Management Framework sets out the arrangements the Council has in place to ensure effective risk management throughout the organisation. This section sets out the process for managing risk effectively. The Council adopts this approach to ensure risks are properly managed and reduced to an acceptable level.

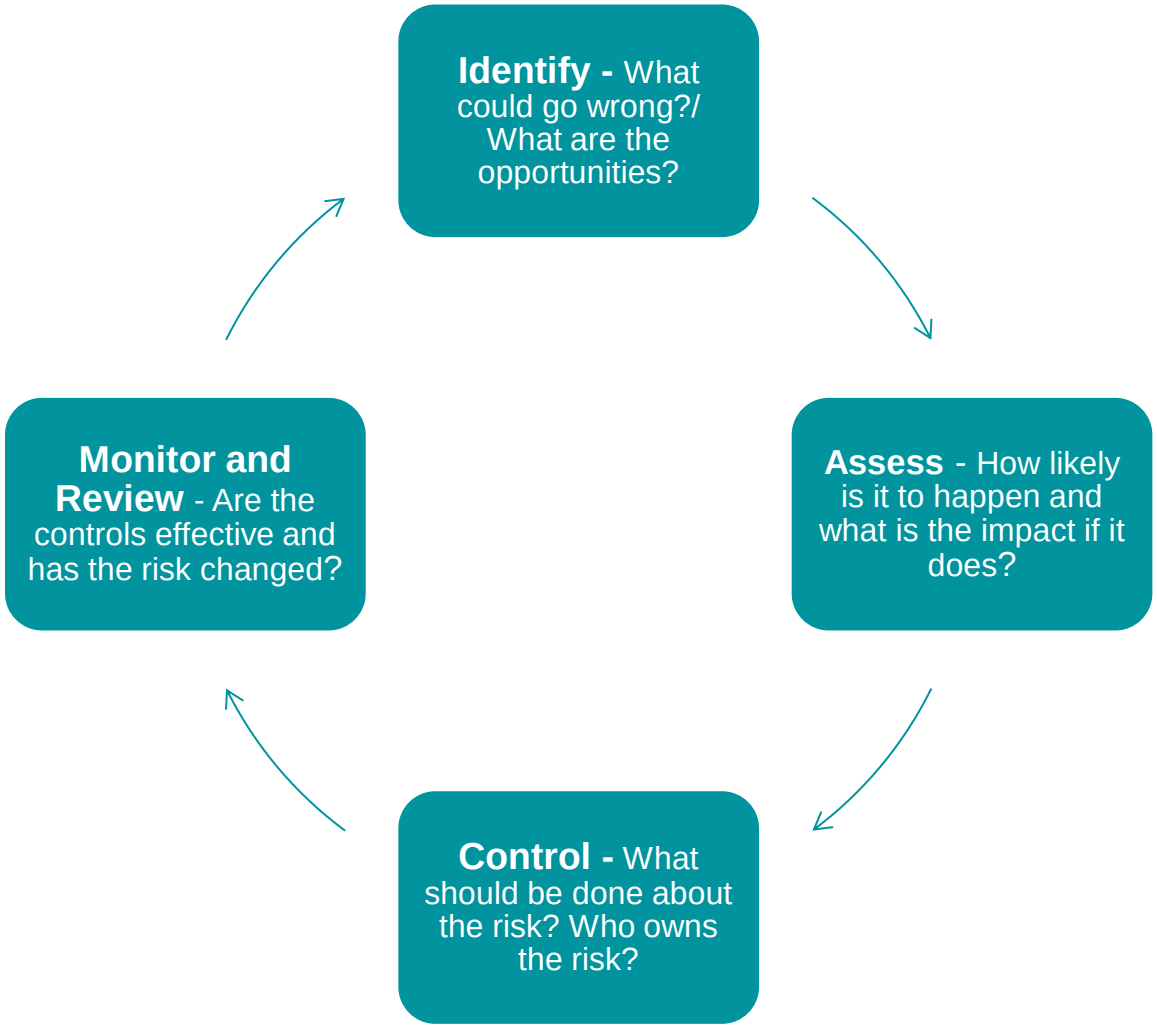

Figure 1: Process for managing risk across the organisation

Step 1: Risk identification

A risk is fully identified once it has been assigned a risk domain, defined, and assigned an owner.

There are different categories of risks that an organisation may face including financial loss, failure of service delivery, physical risks to people, and damage to the organisation's reputation.

Risk registers will categorise risks according to the following domains:

- Financial
- Reputational
- Service Delivery
- Health and Safety
- Legal/regulatory

In addition to being categorised as one of these domains, risks will need to be defined and described in enough detail to articulate and communicate the threat faced. Guidance on

defining risks can be found in the risk management scoring criteria and risk matrix at Appendix 3.

Lastly, all risks must have an owner assigned, in line with the risk roles and responsibilities found at Appendix 1. A risk owner is defined as a person with the accountability and authority to effectively manage the risk.

Step 2: Risk assessment

After identification, each risk is assessed according to the impact if it were to happen and the likelihood of it happening. Guidance on how to assess the risk can be found at Appendix 3. Depending on the results of the assessment, each risk is given a score and RAG rated according to the risk matrix in Appendix 3. This is done both for gross and residual risk. The first assessment (the gross risk) is based on the level of risk if no action is taken, and the second assessment (the residual risk) sets out the risk once mitigating actions have been taken into account. These assessments help prioritise risks as they can then be considered according to level of risk after mitigating action has been taken as opposed to the original, evaluated risk.

Step 3: Control of the risk

Once the risk has been identified and assessed it needs to be controlled and managed. Senior managers have overall responsibility for managing risk in their service area and to ensure that this is done in the most effective manner. Ownership and control of the risk may be delegated to the person (risk owner) directly responsible for managing the business activity specific to the risk.

Risk may be managed in one, or a combination of, of the following ways:

Avoid: A decision is made not to take a risk. Where the risks outweigh the possible benefits, avoid the risk by doing things differently e.g., revise strategy, revisit objectives or stop the activity.

Accept: A decision is taken to accept the risk. Management and/or the risk owner make an informed decision to accept that existing actions sufficiently reduce the likelihood and impact of a risk and there is no added value in doing more.

Transfer: Transfer all or part of the risk through insurance or to a third party e.g., contractor or partner, who is better able to manage the risk. Although responsibility can be transferred, in most cases accountability remains with the Council, so this still needs to be monitored.

Treat/Reduce: Implement further additional action(s) to reduce the risk by minimising the likelihood of an event occurring (e.g., preventative action) and/or reducing the potential impact should the risk occur (e.g., insurance). These will be recorded in the appropriate risk register and regularly monitored. Once they have been completed, where appropriate the residual risk level should be re-assessed.

Exploit: Whilst taking action to mitigate risks, a decision is made to exploit a resulting opportunity.

Step 4: Review and report

Risk management should be thought of as an ongoing process and as such risks need to be reviewed regularly to ensure that prompt and appropriate action is taken to reduce their

likelihood and/or impact. The risk registers are used to report on risk, to record mitigating action and to monitor results.

Embedding risk management within the organisation

For risk management to be effective and a meaningful management tool, it needs to be an integral part of key management processes, day-to-day working in service delivery and the culture of the whole organisation.

The Council will be open in its approach to managing risks. Lessons from events that lead to loss or reputational damage will be shared as well as lessons from things that go well. Discussion on risk in any context will be conducted in an open and honest manner.

Risks and the monitoring of mitigating actions should be considered as part of a number of the Council's significant business processes, including:

- Corporate decision making – significant risks, which are associated with policy or action to be taken when making key decisions, are included in appropriate committee reports.
- Budget planning – this annual process includes updating the corporate and service risk registers to reflect budget realities.
- Programme and project management – all significant projects should formally consider the risks to delivering the project outcomes before and throughout the project. This includes risks that could have an effect on service delivery, benefits realisation and engagement with key stakeholders.
- Procurement – Procurement Procedure Rules clearly specify that all risks and actions associated with procurement need to be identified and assessed, kept under review and amended as necessary during the procurement process.
- Contract Management – all significant risks associated with all stages of contract management are identified and kept under review.
- Insurance – the Council's Insurance team manages insurable risks and self-insurance arrangements.
- Health and Safety – the Council has a specific risk assessment policy to be followed in relation to health and safety risks.
- Service Planning – key risks will be escalated by Service Leaders to Directors through the Service Planning process.

Review and performance

As set out in the Monitoring of the Strategy and Policy section within this document, the Risk Management Group will have a key role in reviewing the efficacy of the Strategy and Policy, as well as the risk management framework.

The Strategy and Policy documents will be reviewed on an annual basis to ensure they are up to date and relevant.

Appendix 1 – Roles and Responsibilities

Roles and Responsibilities

	Corporate Risk Register	Service Risk Register	Programme/project Risk Register
Strategy & Comms Manager	Populate and update		
Strategy team	Maintain Risk Management Framework including guidance and support, monitor service risk registers, identify trends across the Council, support S&C Manager to maintain corporate risk register and support Risk Management Group in conjunction with the Risk Management Group.		
	Support maintenance	Support maintenance	Support maintenance
CMT/Directors	Own	Oversight through Risk Management Group reports	
Service Leads:	Contribute	Own and update	attend project board meetings
Risk Management Group:	To oversee risk across the Council, monitor service risk registers, identify trends across the Council, report areas of concern to CMT, agree, recommend and implement mitigation for corporate risks, undertake deep-drive reviews as recommended by CGS Committee in conjunction with the Strategy team.		
	Report the Corporate Risk Register to CMT and CGS Committee	Support Service Leads with escalated service risks	Support Service Leads with escalated programme/ project risks
CGS Committee	Monitor 6 monthly		
Prog/Project sponsors			Attend project board meetings, contribute to project risk management
Prog/Project Leads			Own, update, maintain, and present risk registers at project board meetings
Prog/Project management boards			Receive, monitor and comment

Appendix 2 – Risk Management Framework

Appendix 3 - Guildford Borough Council Risk Matrix and Scoring Guidance

			Impact			
			Small	Significant	Critical	Devastating
			1	2	3	4
Likelihood	Very high	6	6	12	18	24
	High	5	5	10	15	20
	Medium	4	4	8	12	16
	Low	3	3	6	9	12
	Very low	2	2	4	6	8
	Almost impossible	1	1	2	3	4

Likelihood definitions

Score	Likelihood	Indicators
1	Almost impossible	Less than 1% chance of occurring Has happened rarely/never before
2	Very low	1-10% change of occurring Only likely to happen once in three or more years May have happened in the past
3	Low	10-20% chance of occurring Reasonable possibility it will happen in the next three years Has happened in the past
4	Medium	20-50% chance of occurring Likely to happen at some point in the next one-two years Circumstances occasionally encountered
5	High	50-80% chance of occurring Almost certain to happen within next 12 months Regular occurrences frequently encountered
6	Very high	Above 80% chance of occurring Inevitable it will happen within the next 6 months No influence/control over event occurring

Impact definitions

Score	Impact	Indicators
1	Small	*Loss <£10k* Trivial breach or non-compliance Insignificant injury (first aid) Negligible disruption/unnoticed by service users Insignificant damage
2	Significant	*Loss up to £100k* Isolated legal action or regulatory breach Minor injury (medical attention) Small disruption/inconvenience to service One-off adverse local publicity
3	Critical	*Loss up to £250k* Sustained legal action or (limited) regulatory fine Serious injury (not life threatening)

		Substantial, short-term disruption/inconvenience to service Short-term, but wide-reaching adverse publicity
4	Devastating	*Loss >£500k* Major legal action or regulatory sanction Death(s) or multiple serious injuries Major, sustained disruption/serious inconvenience to service Major, long-term damage