Risk Management Policy

Stevenage Borough Council

2025

DRAFT

Date created	July 2025
Approved by	Chief Executive/Portfolio Holder for Risk
Owner	Strategic Director
Version	003
Author	Joe Maggs, Corporate Performance and Improvement Officer
Business Unit and Team	Corporate Policy and Performance
Policy Review Date	July 2027 (All policies should be reviewed every 2 years or earlier if there is a change in legislation)
Equality Impact Assessment Date	July 2025

For translations, braille or large print versions of this document please email equalities@stevenage.gov.uk.

Contents

1. Risk Policy Statement 3
2. Purpose 4
3. Scope 4
4. Legal Framework 4
5. Equalities 5
6. Data Protection 5
7. Policy 5
   7.1 Introduction 5
   7.2 Key Concepts 6
   7.3 The Benefits Of Effective Risk Management 6
   7.4 The Risk Management Framework 7
   7.5 Key Responsibilities Regarding Risk Management 11
8. Consultation 13
9. Monitoring and Review 13
10. References and Resources 13
11. Acronyms and Definitions 13
12. Appendices 14
13. Version History 14

DRAFT

1. Risk Policy Statement

The Council recognises that it has a responsibility to manage the risks it faces effectively in order to:

- Ensure that statutory obligations and policy objectives are met
- Prioritise areas for improvement in service provision and encourage meeting or exceeding customer and stakeholder expectations
- Safeguard its employees, clients and service users, members, and all other stakeholders to whom the council has a duty of care
- Protect its property and assets including buildings, equipment, vehicles, information and all other assets and resources
- Identify and manage potential liabilities
- Maintain effective control of public funds and the efficient deployment and use of resources to achieve 'value for money'
- Preserve and promote the reputation of the council
- Support the quality of the environment
- Engage effectively with its partner organisations and wider community
- Learn from previous threats, opportunities, successes, and failures to inform the future management of risks.

Risk management is an integral part of the Council's corporate governance arrangements and has been built into the management processes as part of the Council's overall framework to deliver continuous improvement. All Members and officers have a responsibility and a role to play in managing risk.

The Council will seek to achieve effective risk management by:

- Implementing a Risk Management Framework that is fit for purpose and which complements the other governance processes of the Council
- Equipping all employees and elected members with the skills required to identify and assess risk and communicate this appropriately and effectively
- Acknowledging that increasingly risks are shared across partner organisations, which can increase the complexity of analysis and reporting, and that assurances regarding the level of risk may need to be sought from third parties as well as internal sources
- Annually reviewing the effectiveness of risk management and reporting the results as part of the Annual Governance Statement
- Considering on a continuous basis that the council's approach remains in line with good practice, whilst reviewing the Policy and Framework formally every two years.

Signed:

Leader of the Council …….

Chief Executive ……

DRAFT

2. Purpose

2.1 This policy sets out the Council's approach to managing risk and replaces the previous Risk Management Policy (2023) (v002). The policy aims to enable the effective management of risk, including strategic, operational, partnership and project risks. Effective management of risks supports the achievement of the Council's objectives.

3. Scope

3.1 It is the responsibility of all Members and employees to be aware of risk in carrying out their duties and ensure that risks are taken in a structured and well managed manner. Officers are accountable for the delivery of this policy within their areas of responsibility, and for encouraging partners to act accordingly.

3.2 A robust risk management culture requires a widespread understanding of, and commitment to, risk management principles. Members and staff from all service areas need to be familiar with the Council's risk management arrangements and their own role and responsibilities.

4. Legal Framework

4.1 Stevenage Borough Council is responsible for ensuring that its business is conducted in accordance with the law and to proper standards and that public money is safeguarded, properly accounted for, and used economically, efficiently, and effectively. The Council has a duty under the Local Government Act 1999, to make arrangements to secure continuous improvement in the way in which its functions are exercised, having regard to a combination of economy, efficiency, and effectiveness.

4.2 In discharging this overall responsibility, Stevenage Borough Council is responsible for putting in place proper arrangements for the governance of its affairs, facilitating the effective exercise of its functions, which include arrangements for the management of risk.

4.3 The Council is statutorily required to produce an Annual Governance Statement each year which provides a comprehensive overview of how the organisation has maintained effective governance, managed risks, and ensured accountability during the financial year.

4.4 The CIPFA/SOLACE Delivering Good Governance in Local Government Framework sets the standard for local authority governance in the UK. The concept underpinning the framework is to support local government in developing and shaping an informed approach to governance, aimed at achieving the highest standards of governance in a measured and proportionate way.

4.5 Having effective Risk Management arrangements is a key aspect of the above-mentioned framework. Principle F of the framework identifies that public bodies should manage risks and performance through robust internal control and strong public financial management. This risk management policy and associated processes outlined in the Risk Management

DRAFT

Guide will enable the Council to have in place the arrangements and behaviours expected of public bodies as set out in the framework.

4.6 The Annual Governance Statement is produced each year following a review of the Council's governance arrangements which includes a review of the management of the Council's risk arrangements against the requirements of the framework.

5. Equalities

5.1 Under the Equality Act (2010) the Council has a legal duty to fulfil the requirements of the Public Sector Equality Duty (PSED). Through this duty and in the application of this policy, the council will carry out its functions in a way that:

a. Removes discrimination, harassment, victimisation and any other conduct that is unlawful under the Equality Act (2010)
b. Promotes equal opportunities between people who have a protected characteristic(s) and those who don't
c. Encourages good relations between people who have a protected characteristic(s) and those who don't

Further information on the Council's fulfilment of the Equality Act (2010) is set out in the Equality, Diversity and Inclusion (EDI) Policy (2022) and Reasonable Adjustment Policy (2024).

6. Data Protection

6.1 The Council regards respect for the privacy of individuals and the lawful and careful treatment of personal information as very important to delivery of services.

6.2 The Council will ensure that it treats personal information lawfully and proportionately as set out in the General Data Protection Regulation (GDPR) and Data Protection Act (2018). For further information on the Councils approach to handling information please see Data Protection Act (stevenage.gov.uk)

7. Policy

7.1 Introduction

Good corporate governance requires mechanisms to be in place for the identification and management of risk. There must be a clear focus on managing risks that can prevent the Council from achieving its priorities as set out in the Council's Making Stevenage Even Better (MSEB) Corporate Plan (Strategic Risks), delivering services as planned (Operational Risks) and fulfilling its statutory duties. This Policy seeks to provide a mechanism for the management of these risks.

DRAFT

7.2 Key Concepts

Risk:

7.2.1 Risk is a word and concept that is used in many everyday scenarios. In relation to Council business and activities, risk can be defined as the effect of uncertainty on objectives. In practical terms, a risk can be thought of as a potential (uncertain) event that could impact our strategic or operational priorities.

7.2.2 It is important to note from this definition that risks are events that have not yet happened (if the event has already taken place then it should be dealt with as an issue or incident) and also that the outcome of an uncertain event can be positive as well as negative.

7.2.3 When a risk is identified, it should be recorded describing the possible event, cause and consequences. Further detail on the process of recording risks is provided later in this policy.

Risk management:

7.2.4 Risk management is the coordinated activities designed and operated to address risks and exercise internal control within the Council. It includes the identification and consideration of risks in the context of the Council's strategic plan and objectives.

Internal control:

7.2.5 A system of internal control is the framework of processes, policies, procedures, and practices applied to manage risks and ensure effective governance.

7.2.6 The Accounts and Audit Regulations 2015 requires the Council to have in place a sound system of internal control which includes effective arrangements for the management of risk.

Governance:

7.2.7 Governance (also referred to as corporate governance) refers to the systems and processes through which an organisation is directed and controlled. Effective governance enables clarity of strategic purpose and robust monitoring of performance and compliance. It ensures that an organisation acts in alignment with the interests of its various stakeholders and with accountability. Risk management and internal control are important components of a governance framework.

Assurance:

7.2.8 Assurance is the confidence that can be derived from objective information that an agreed course of action (whether a strategy or component of the internal control framework) is being implemented effectively and achieving its intended outcomes. It is a cross-cutting concept that supports good governance in general as well as effective risk management.

7.3 The Benefits Of Effective Risk Management

7.3.1 Risk management is fundamentally about making better decisions. It is an integral part of good planning and transparent decision making at both an operational and strategic level.

DRAFT

It is essential to the effective use of resources, providing assurance that the Council has a sound system of internal control and robust corporate governance arrangements. Management of risk also plays an important role in protecting the Council's reputation and assets and in managing key partnerships and projects.

7.3.2 A robust risk management culture requires widespread understanding of and commitment to risk management principles. Members and staff need to be familiar with the Council's risk management arrangements and their own role and responsibilities.

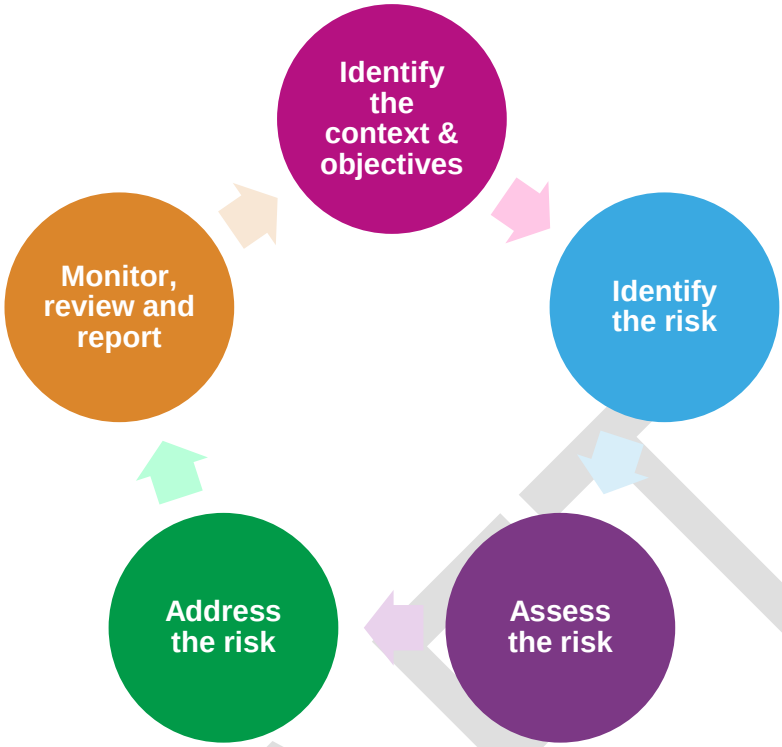
7.3.2 The benefits of a culture where consideration and management of risk is fully integrated in day-to-day decision-making are significant:

- Increased likelihood of achieving strategic and operational objectives
- Better planning and prioritisation of resources
- Early warning of potential problems
- Proactive approach to uncertainty
- Improved stakeholder confidence
- Better management of partnership arrangements
- Protection of Council assets
- Informed balance between innovation and risk avoidance
- Ability to identify and take advantage of opportunities
- Demonstrates good governance

7.4 The Risk Management Framework

7.4.1 The Council's risk management framework comprises five steps which form a continuous process:

DRAFT



Identify context and objectives

7.4.2 The first step is to consider the Council's strategic and operational objectives and the context in which it operates, including legal, social, political and cultural factors. This sets the scene for further consideration of potential risks and their component elements. A thorough understanding of the context and objectives ensures that risk management is grounded in the organisation. The environment in which the Council operates can change over time based on a range of internal and external factors, which is why it is important that this step is revisited as part of the continuous process.

Identify the risk

7.4.3 With the context and objectives in mind, the next step is to consider the activities and events that provide exposure to uncertainty and threaten strategic and / or operational priorities.

7.4.4 Once a risk has been identified, it should be defined (i.e. described) based on the following structure to ensure it captures the key elements needed to manage the risk and is consistent with other risks:

1. Risk event (e.g. There is a risk of x),
2. Cause (e.g. due to y),
3. Potential consequences (e.g. this would result in z).

7.4.5 Each risk should be categorised by service area and whether it relates to strategic, operational or programme/project delivery and assigned an owner that is appropriate for the level and scoring of the risk.

DRAFT

- Strategic risks: These concern the long-term strategic objectives of the Council (i.e. the Corporate Plan). There is a central strategic risk register for the Council where these are recorded.
- Operational risks: These concern the day-to-day issues that the Council faces as it works to deliver its strategic objectives. Operational risk registers exist at service level.
- Programme / project risks: These are the risks associated with specific programmes or projects and monitored at service level.

7.4.6 The Council maintains strategic and operational risk registers centrally, while programme / project risk registers are developed and held at a local level. The detail captured through this and the next two stages (assessing and addressing the risk) should be recorded in the relevant risk register.

Note: Please see the attached appendices 1 & 2 for further guidance and templates to assist with the process of identifying and documenting risks:

- *Appendix 1 – Risk management guide for staff*
- *Appendix 2 – Risk register template for project / programme risks*

Assess the risk

7.4.7 Once a risk has been identified and defined, the likelihood and potential impact of the risk should be calculated.

7.4.8 The assessment of both impact and likelihood is largely a matter of judgement. However, it should be informed by experience, data, subject matter expertise, and other reliable sources of intelligence to ensure a well-founded evaluation.

7.4.9 Risk scoring involves evaluating two main factors, impact and likelihood:

- Impact refers to the potential consequences of the event, expressed in terms of loss, injury, disadvantage, or other negative outcomes. This is assigned a numerical score on a scale from 1 to 5 (1 (insignificant), 2 (minor), 3 (moderate), 4 (significant), 5 (major)).
- Likelihood refers to the probability or frequency of the event occurring, described using qualitative or quantitative measures, depending on what is most appropriate. Again, these are rated on a scale from 1 to 5 (1 (rare), 2 (unlikely), 3 (possible), 4 (likely), 5 (almost certain).

7.4.10 Please see the associated risk management guidance for staff (Appendix 1) for more detail on the risk scoring criteria.

7.4.11 The risk score is calculated by multiplying the likelihood score by the impact score. The score can then be plotted on the risk score matrix (a 5x5 grid, as below) which will grade the overall risk as either ‘low’, ‘medium’, ‘high’ or ‘very high’. This process highlights the significance of each risk and its score relative to others.

DRAFT

		Likelihood				
Impact		1	2	3	4	5
	5	5 Medium	10 High	15 High	20 Very High	25 Very High
	4	4 Low	8 Medium	12 High	16 Very High	20 Very High
	3	3 Low	6 Medium	9 Medium	12 High	15 High
	2	2 Low	4 Low	6 Medium	8 Medium	10 High
	1	1 Low	2 Low	3 Low	4 Low	5 Medium

7.4.12 There should be three risk scores for each risk:

- Inherent / unmitigated: The risk score on the day it is identified, before any controls have been put in place.
- Current: The level of risk at the time of the latest review, taking into account actions taken to manage the risk.
- Target: The level of risk the Council is prepared to take in pursuit of its goals. The SLT will consider the appropriateness of the target scores for strategic risks on a regular basis.

7.4.13 Where there is more than one potential impact, the highest impact score should be used for the purpose of scoring the risk, but it is important that risk assessments are reasonable and proportionate to support effective risk management and strategic decision making.

Address the risk

7.4.14 The next step is to identify actions to manage the risk. Options for responding to risks fall into the following categories:

- Treat – Taking action to reduce the likelihood and/or impact of the risk.
- Transfer – Moving the risk to another party (e.g. by taking out insurance).
- Terminate – Ceasing to take the action that causes the risk.
- Tolerate – It may not be possible to mitigate the risk or all mitigations may be exhausted and a level of risk is accepted.

7.4.15 The aim is to minimise the risk (ideally to the target score) whilst ensuring that the level of risk accepted is balanced against the accepted cost / reward of taking the mitigating actions. All mitigating actions should be assigned an action owner and timescale for implementation (though some mitigating actions will effectively be recurring actions that should be reviewed on a periodic basis e.g. maintaining policies, ensuring training is undertaken, etc.). It can be helpful to approach

this step by thinking about which actions are preventative (to stop the risk materialising) and which are corrective (to reduce its impact if it does occur).

7.4.16 Once actions are identified, these should be captured on the risk register.

Monitor, review and report

7.4.17 The aim of this part of the process is to ensure that planned risk management actions are implemented and monitored as to their effectiveness and corrective action is taken when the performance does not match expectations. This regular review process should occur both in response to changes and, in the absence of changes, to confirm that the current assessments remain valid and appropriate. This is also an opportunity to consider whether risks should be escalated or de-escalated based on the latest scoring and strategic context.

7.4.18 For the Strategic and Operational risk registers there is a cycle of periodic reviews led by the Corporate Policy and Business Support team, however if a new risk arises, or there are significant changes to existing risks between the periodic reviews, officers should update the risk register accordingly.

7.4.19 The Corporate Risk Group meets quarterly to review the Council's risk management arrangements, the Strategic and Operational risks, as well as certain health and safety risks and compliance of the Council's facilities and estates. Following this, any areas of concern are escalated to the SLT as required. In addition:

- Assistant Directors are responsible for monitoring Service Level Operational Risk Registers at least 6 monthly (some risks will need more frequent review).
- Strategic risks are reviewed quarterly by the risk owner, Corporate Risk Group and SLT. They are also reported to Audit Committee.

7.5 Key Responsibilities Regarding Risk Management

7.5.1 All Council staff and Members have a role to play in effective risk management.

All Employees	Be aware of and comply with the risk management policy. Report any identified risks.
Council Members	Understand the key risks faced by the Council and the approach to managing these. Consider risks in decision making.

DRAFT

Chief Executive and Senior Leadership Team	Provide leadership and direction for risk management. Ensure that risk management is integrated into the Council's strategic planning and decision-making processes. Setting and demonstrating the organisational risk culture. Monitoring management of the strategic risks. Consider the Council's risk appetite in relation to current and emerging risks and opportunities.
Audit Committee	Seek assurance over the governance of risk, including leadership, integration of risk management into wider governance arrangements and the ownership of and accountability for risks. Keep up to date with the risk profile and the effectiveness of risk management actions. Monitor the effectiveness of risk management arrangements and support the development and embedding of good practice in risk management.
Corporate Risk Group	Oversee the development and implementation of the risk management policy. Review risk registers and ensure appropriate risk mitigation measures are in place.
Corporate Performance and Improvement Officer (Risk & Governance)	Develop and maintain the risk management framework. Provide updates regarding risk management activity to the Corporate Risk Group, SLT and Audit Committee. Provide training and support to staff and Audit Committee members on risk management practices.
Service Managers	Identify and manage risks within their respective departments. Ensure that risk management practices are followed by their teams.
Project / Partnership Managers	Ensure that the appropriate risk management arrangements are created and maintained relevant to the project or partnership arrangements and there is regular reporting to the relevant senior management / project board / partnership board.
Internal Audit	Conduct independent reviews of the risk management processes. Provide assurance on the effectiveness of risk management practices.

DRAFT

External Stakeholders and Partners	Collaborate with the Council on risk management initiatives. Provide input and feedback on risk management practices and policies.

8. Consultation

8.1 Due to the internal nature of this Policy, consultation is not required.

9. Monitoring and Review

9.1 This policy will be reviewed by the relevant Business Unit's Head of Service or Service Manager every 2 years (see page 1 for details of Business Unit) or earlier if there is a change in legislation. Where more than 10% of the policy content is changed the Assistant Director and appropriate Portfolio Holder will be required to decide if the policy needs to be formally reconsidered by the Cabinet or appropriate decision-making body.

9.2 Where there is a request for the content of the policy to be reviewed in response to a complaint, the relevant Business Unit's Assistant Director will be notified. If the Assistant Director agrees that a review of policy is required, this will be discussed with the appropriate Portfolio Holder. The Head of Service or Service Manager will be responsible for implementing a subsequent policy review.

10. References and Resources

- CIPFA Delivering Good Governance in Local Government: Framework (2016 Edition): https://www.cipfa.org/policy-and-guidance/publications/d/delivering-good-governance-in-local-government-framework-2016-edition
- Best Value guidance: Best value standards and intervention: a statutory guide for best value authorities - GOV.UK (www.gov.uk)
- The Orange Book - Management of Risk – Principles and Concepts: The Orange Book – Management of Risk – Principles and Concepts
- ALARM Risk Management Guide
- LGA Must know guide: Risk management: Must know guide: Risk management | Local Government Association

11. Acronyms and Definitions

EDI	Equality, Diversity and Inclusion
GDPR	General Data Protection Regulation
MSEB	Making Stevenage Even Better
PSED	Public Sector Equality Duty
SBC	Stevenage Brough Council

See also 'Key concepts' in sections 6.2 – 6.12, above.

DRAFT

12. Appendices

1. Risk management guide for staff
2. Risk register template for project / programme risks

13. Version History

Date	Outlined Amendments	Author
July 2025	Significant rewrite of most sections.	Joe Maggs (Corporate Performance and Improvement Officer)

DRAFT