Risk Management Strategy

Contents page

1. <u>Introduction</u>

1.1   Risk management can be defined as '*the process of identifying risks, evaluating their potential consequences and determining the most effective methods of controlling or responding to them'*.

1.2   The council's risk management objectives and approach are stated in the Risk Management Policy. This strategy explains the processes required to implement the policy and provides simple templates designed to evaluate the effect of a risk.

1.3   The purpose of risk management is to:

- Improve performance
- Promote a risk aware culture to avoid unnecessary liabilities and costs, but to encourage the taking of calculated risks in pursuit of opportunities that benefit the council
- Promote corporate governance by integrating risk management and internal control
- Preserve and protect the council's assets, reputation and staff.

1.4   This policy/strategy will be reviewed every three years, or earlier in the light of new guidance, to ensure it remains relevant to the needs of the council. The next review will take place no later than March 2022.

2. <u>Legal framework and relevant legislation</u>

2.1   Risk management is an integral part of internal control, and for local government a statutory requirement, defined in the Audit & Accounts Regulations 2003, as amended by the Accounts and Audit (Amendment) (England) Regulations 2006. Paragraph (1) of Regulation 4 (responsibility for financial management) states:

'The relevant body shall be responsible for ensuring that the financial management of the body is adequate and effective and that the body has a sound system of internal control which facilitates the effective exercise of that body's functions and which includes arrangements for the management of risk.'

2.2   Regulation 6 requires relevant bodies to conduct an annual review of the effectiveness of their system of internal audit. CIPFA's guidance on the Review of the System of Internal Audit, published in January 2009, defines the system of internal audit as:

'The framework of assurance available to satisfy a local authority that the risks to its objectives, and the risks inherent in undertaking its work, have been

properly identified and are being managed by controls that are adequately designed and effective in operation.'

2.3   Risk management represents a part of the governance arrangements which are required to be reported on in the annual governance statement incorporated in the council's annual statement of accounts.

2.4   In addition to the above requirements there are several other specific duties that the council is obliged to observe including, as examples, responsibilities arising from the Civil Contingencies Act 2004, Health and Safety at Work Act 1974 and equality impact assessments under the Equality Act 2010.

3. <u>Process of managing the risk</u>

3.1 Risk management overview

3.1.1   Risk management consists of initially defining the risk appetite and then applying four basic processes:

1. Identifying risks
2. Evaluating
3. Minimising, controlling and responding
4. Monitoring and reporting

3.2 Risk appetite

3.2.1   This is '*the amount of risk that an organisation is willing to seek or accept in the pursuit of its long-term objectives'*. The council's risk appetite is defined in the Risk Management Policy as '*open*', which means that the council is '*prepared to consider all delivery options and select those with the highest probability of productive outcomes, even when there are elevated levels of associated risk'*.

3.3 Identify the risk

3.3.1   The purpose of this stage is to identify anything that might affect the achievement of the council's objectives and assess what that effect might be. The question to ask is 'What might possibly present itself in the course of delivering the objectives, which has the capacity to threaten or improve the success?' Once identified, the extent to which it might affect the objectives needs to be considered.

3.3.2   A number of approaches are taken to identify risks to the council at the earliest opportunity and ensure that they are managed from a very early stage. These include:

- Regular monitoring of the Corporate Business Plan.

- Regular monitoring of committee and performance monitoring reports.
- Regular reviews by Management Team to ensure all strategic and corporate risks have been recorded on the Strategic and Corporate Risk Register and accurately assessed.
- Annual reviews to ensure operational risks have been recorded in service plans.
- Robust processes at the commencement of projects, particularly major ones, and ongoing monitoring.
- Use of Internal Audit and peer reviews.
- Horizon scanning informed by professional and advisory bodies such as the Local Government Association.

3.4 Evaluate the risk

3.4.1 This stage develops a greater understanding of each risk, its impact and the likelihood of those consequences. It provides an input to risk evaluation and to decisions on how risk will be managed.

3.4.2 The categories for likelihood and impact are shown below.

Likelihood

Score	Definition
1 – Rare	The event may occur only in exceptional circumstances
2 – Unlikely	The event could, but is not expected to, occur
3 – Possible	The event might occur at some time
4 – Likely	The event will probably occur in most circumstances
5 – Almost Certain	The event is expected to occur in most circumstances

Impact

Score	Impact on service	Personal safety	Financial loss	Legal and Regulatory	Corporate objective	Environmental impact	Reputation
1	Little	No injury	<£25,000 or 1% of budget	Minor civil litigation or regulatory criticism	No effect on delivery	None or insignificant	No damage
2	Some	Minor injury	>£25,000 or >2.5% of budget	Minor regulatory enforcement	Little effect on delivery	Minor damage	Minimal damage (minimal coverage in local press)
3	Significant	Violence or threat of serious injury	>£175,000 or >5% of budget	Major civil litigation and/or public enquiry	Possible impact on delivery	Moderate damage	Significant coverage in local press
4	Service not available for 2-7 days	Extensive or multiple injuries	>£500,000 or >10% of budget	Major civil litigation and/or national public enquiry.	Significant impact on delivery	Major damage	Coverage in national press
5	Service not available for >7 days	Fatality	>£1m or >15% of budget	Section 151 or government intervention or criminal charges	Non delivery	Significant damage locally or nationally	Requires resignation of Chief Exec, Exec Director or Leader

3.4.3 Apply the definitions of likelihood and impact to establish the risk score and rating using the risk matrix below. This will determine what level of action is required and who by.

Risk Category	How the risk should be managed
Very High Risk (15 – 25) (Red)	Immediate action required. Senior management must be involved.
High Risk (10 – 12) (Orange)	Senior management attention needed and management responsibility specified.
Medium Risk (5 – 9) (Green)	Manage by specific monitoring or response procedures. Responsibility to be allocated by Management Team to a named service manager.
Low Risk (1 – 4) (White)	Manage by routine procedures, unlikely to need specific or significant application of resources.

Risk matrix

	5 Almost Certain	(5) (Green)	(10) (Orange)	(15) (Red)	(20) (Red)	(25) (Red)
LIKELIHOOD	4 Likely		(8) (Green)	(12) (Orange)	(16) (Red)	(20) (Red)
	3 Possible		(6) (Green)	(9) (Green)	(12) (Orange)	(15) (Red)
	2 Unlikely			(6) (Green)	(8) (Green)	(10) (Orange)
	1 Rare					(5) (Green)
		1 Insignificant	2 Minor	3 Moderate	4 Major	5 Extreme

IMPACT

For example, a risk that is 'likely' to occur, and has a 'minor' impact will score 4 x 2 = 8 which is a 'medium' risk.

3.5 Minimising, controlling and responding

3.5.1 When deciding how to manage risks, the cost effectiveness of implementing proposed controls needs to be considered. There is little benefit to be gained from pursuing a course of action if the cost of controlling a risk outweighs the benefits to be gained.

3.5.2 There are four basic ways of responding to risk:

Avoidance	Deciding not to continue or proceed with the activity in view of the level of risk involved. This may be as a result of the cost of mitigating the risk being too high, or the consequences being too adverse. (Note: statutory requirements cannot be avoided).
Transfer	Involves another party bearing or sharing the risk, a typical example being the use of insurance. (Note: ultimate responsibility to undertake statutory requirements remains with the Council even if third party provision is engaged).
Mitigate	Ensuring existing controls are effective by periodic review and testing, and implementing additional controls where necessary.
Acceptance	Certain risks cannot be adequately treated by any of the above. In such cases, there is no alternative but for the Council to accept the residual risks concerned. Details of how these risks and their possible effects are to be managed must be recorded in the risk register at Corporate, Service or Project level as appropriate, and subject to regular review.

3.6 Monitoring and reporting

3.6.1 Management Team reviews the Strategic and Corporate Risk Register at regular intervals to assess if any risk has increased, reduced or stopped altogether, or if new risks need to be added.

3.6.2 The Terms of Reference for the Audit Committee state that '*the purpose of an audit committee is to provide independent assurance of the adequacy of the risk management framework...',* and as such one of its functions is to '*consider the effectiveness of the council's risk management arrangements'.*

3.6.3 The committee will therefore receive regular updates on the strategic and corporate risk register and will consider the effectiveness of the Risk Management Strategy.

3.6.4 Reports to committees will include an appraisal of all associated risks and their implications. This is specified in the mandatory report template.

3.6.5 Where officers have concerns about risks they should be reported to the relevant director or Policy, Performance and Personnel. These concerns may for example include:

- Operational risks that have identified a potential strategic risk.
- Risks that have not been controlled within the pre-agreed timescales.
- Risks that have increased since initial evaluation.
- An identified risk occurs and results in failure/loss due to inadequate controls.
- Risks that may need to be moved to a new owner.
- Risks that become too unwieldy to manage at the current level.
- Risks that remain very high even after mitigations are implemented.
- Risks that impact on more than one service/project or function if the risk event materialises.
- Risks that move outside the appetite boundaries.

3.6.6 Management Team will determine whether risks move from the operational level to the strategic and corporate level.

4. Strategic and corporate risk register

4.1 Strategic risks

4.1.1 A strategic risk is defined as "An event or occurrence that would cause the council to be unable to operate or provide key services leading to a significant adverse effect on public wellbeing."

4.2 Corporate risks

4.2.1 A corporate risk is defined as "An event or occurrence that would lead to a significant adverse effect on the council's ability to provide important public services."

4.3 Strategic and corporate risk register

4.3.1 The Strategic and Corporate Risk Register records high level risks that pose a threat or opportunity to the council's ability to operate and deliver services that could have an adverse effect on public wellbeing and affect our ability to provide important public services or corporate business plan objectives.

4.3.2 Executive directors are responsible for identifying risks that have a strategic and corporate impact. The Senior Policy and Performance Officer should be notified of any such risk so that it can be added to the Strategic and Corporate Risk Register and included in the next review by Management Team.

4.3.3 The Strategic and Corporate Risk Register is held by the Policy and Performance Team and published on InSite. The table below sets out the format of the register and an explanation of each of the fields contained within the register:

Ref	This is a unique code for the risk.
Title	This is a brief title for the risk.
Description	This describes the vulnerabilities of the council.
Director	This is the lead officer for managing the risk.
The risk is that	This describes the consequences of the risk occurring.
Inherent risk without mitigation	This defines the likelihood, impact and resulting score for the risk without any form of mitigation or control.
Controls/mitigation	This describes the measures put in place by the council.
Current risk score	This defines the likelihood, impact and resulting score for the risk following mitigation or control.
Trend	This indicates the direction of travel of the current risk score compared with the previous 6 monthly review.
Latest update	This describes mitigation undertaken since the previous review.
Review date	This is the date of the current review.
Target risk score	This defines the likelihood, impact and resulting score for the risk that is deemed acceptable by the council following mitigation or control.

4.3.4 The register is reviewed by the Executive Directors on a 6-monthly basis. Any existing entries on the register are considered for changes to the nature of the risk, progress to be reported and any adjustments to the risk scores. Risks that are no longer relevant are removed and new risks considered in the context of current circumstances are added. The risk reference numbers are

not reallocated when risks are removed from the register, to enable the history to be maintained.

4.3.5 A 6-monthly overview of changes to the register is provided to the Audit Committee. Details of the 'Very High' risks are given together with a list of the 'High' risks.

4.3.6 The full register, as agreed by Management Team, is provided to the Audit Committee in hard copy, for reference.

5. Operational risks

5.1 An operational risk is defined as "An event or occurrence arising from inadequate or failed internal processes, people and systems, or from external events, leading to an adverse impact on service provision."

5.2 Operational risks should be recorded in service plans and reviewed annually.

6. Capital project risks

6.1 A risk register will be maintained for capital projects managed by Property Services.

7. Roles and responsibilities

7.1 Risk management is the responsibility of everyone. It is important that risk management becomes part of daily routines to ensure achievement of the council's objectives is not jeopardised by unrecognised risks.

7.2 All council employees and members are responsible for ensuring there are robust and fit-for-purpose systems of internal control and risk management in place; and they are aware of the risks that:

- they are empowered to take
- must be avoided or reported upwards.

7.3 Members

7.3.1 The Leader of the Council is responsible for acting as lead councillor for risk management.

7.3.2 The Audit Committee has specific responsibility for the scrutiny of risk management. The committee receives the triennial review of the Risk Management Policy and Strategy and half-yearly reports on the update of the Corporate Risk Register. It is the committee's responsibility to ensure that risks are being actively managed.

7.3.3 The risk management policy and strategy are approved by Cabinet.

7.4 Management Team

7.4.1 Ultimately Management Team is responsible for managing risk. The responsibility cannot be devolved down, although actions to mitigate risk can be assigned to officers.

7.4.2 Executive Directors must inform the Section 151 Officer of any financial viability or resilience issues as soon as they emerge so that any appropriate action that may be required can be taken.

7.4.3 In addition, Management Team should:

- Nominate a member of Management Team with overall responsibility for risk management, currently the Chief Executive
- Identify risks within their respective directorates through section and project meetings.
- Take ownership of risks within their respective directorates and assign a responsible officer to all significant service risks
- Receive regular updates on identified and any new significant emerging risks within their directorate
- Ensure that the risk management process is reviewed on a regular basis.

7.5 Section 151 Officer

7.5.1 The Section 151 Officer has a responsibility to monitor the viability and resilience of the council's finances and take appropriate action if required to ensure the ongoing financial sustainability of the council. The officer must be informed of any potential financial risk arising from project or service activities as it emerges.

7.6 Service managers

7.6.1 Service managers are responsible for raising awareness of the risk management strategy in their own service area and notifying their executive director of any significant risks.

7.6.2 Service managers, in conjunction with their executive director, should:

- Lead reviews of the operational risks relating to their services
- Ensure a responsible officer is assigned to manage significant risks
- Identify resources to address the highest priority risks
- Monitor progress on a regular basis
- Review the risks on an annual basis and when new situations arise
- Ensure committee reports include an appraisal of all associated risks and their implications.

7.7 Project managers

7.7.1 Managers of major and capital projects are responsible for raising awareness of the strategy in their own projects and should monitor the project risk register on a regular basis. Any significant risks should be notified to the relevant executive director.

7.7.2 Project managers, in conjunction with their executive director, should:

- Lead reviews of the operational risks relating to their projects
- Ensure a responsible officer is assigned to manage significant risks
- Identify resources to address the highest priority risks
- Monitor progress on a regular basis
- Review the risks on an annual basis and when new situations arise.

7.8 Directors of council owned companies

7.8.1 Councillors and senior council officers are appointed as company directors on council owned companies such as West Norfolk Housing Company Ltd. There is a responsibility upon board directors to consider the risk management arrangements in place for these types of company.

7.9 Policy, Performance and Personnel

7.9.1 This service has responsibility for coordinating the implementation of the risk management strategy and reviewing the policy and strategy. This will include updating the corporate risk register, reporting where required to Management Team, Audit Committee and Cabinet and supporting ongoing communication and development.

7.10 Internal Audit

7.10.1 Audit of the risk management process is independently reviewed by Internal Audit to avoid a conflict of interest. Internal Audit can provide the Audit Committee with independent assurance as to the robustness of the council's risk management arrangements.

7.10.2 Internal auditors will consider any potential unidentified risks during their audit work and bring any issues to the attention of management where necessary.

7.10.3 The council's Fraud and Corruption Risk Register is maintained by Internal Audit. This forms part of the internal control environment and mitigation measures.

7.11 Health and safety risk management

7.11.1 The ongoing management of these types of risks is covered by the council's Health, Safety and Welfare General Policy.

7.11.2 Each directorate is responsible for undertaking their own annual risk assessments with support from the Corporate Health and Safety Group.

8. Risk management training

8.1 Risk management training will be provided to relevant officers with the aim of ensuring that they have the skills necessary to identify, appraise and control the risks associated with the services they provide and projects that they manage. Elected members will receive training on risk so that they can consider the implications of risk whilst engaged with council activities.

9. Health implications

9.1. The strategy is a key part of the council's governance framework and will contribute towards wider health policies through mitigation measures.

10. Equalities implications

10.1 The strategy is considered to have no equalities implications.

11. Reference documents

11.1 The strategy supports the council's Risk Management Policy.

12. Additional information or resources

12.1 The related Risk Management Policy and Strategic and Corporate Risk Register can be found in the risk management section of InSite.

12.2 Further information can be obtained from Policy and Performance.

13. Implementation/distribution

13.1 The strategy will be distributed to senior managers and all staff/members via Internal Affairs, the Members Bulletin and InSite.

Policy name	Risk Management Strategy			
Policy description	The risk management approach described in this strategy is key to identifying, assessing, mitigating, managing and reviewing risks to the achievement of the council's objectives.			
Responsible Officer	Ged Greaves, Senior Policy and Performance Officer			
Version number	Date formally approved	Reason for update	Author	Review date
1	March 2016	Refresh		March 2019
2	TBC	Planned refresh	Ged Greaves	March 2022