Buckinghamshire Council

Risk Management Strategy

March 2020

# Contents

1. Introduction

Risk is part of everything we do. We live in an ever-changing world and the pace of change is increasing. This carries with it uncertainty and that uncertainty brings new opportunities and risks. How we manage those has never been more important in helping us meet our objectives, improve service delivery, achieve value for money and reduce unwelcome surprises.

Buckinghamshire Council believes in the value of effectively managing risk: it informs business decisions; enables a more effective use of resources; enhances strategic and business planning; and strengthens contingency planning. None of this is possible without a supportive risk culture. A positive risk culture, one which encourages openness and discusses real business issues in a realistic manner, is absolutely essential to the effective management of risk. Everyone, from the Cabinet and Corporate Management Team down, has a clear role to play in establishing and maintaining that risk culture.

As set out in the Buckinghamshire Council Corporate Plan 2020-23, the Council has defined four key priorities:
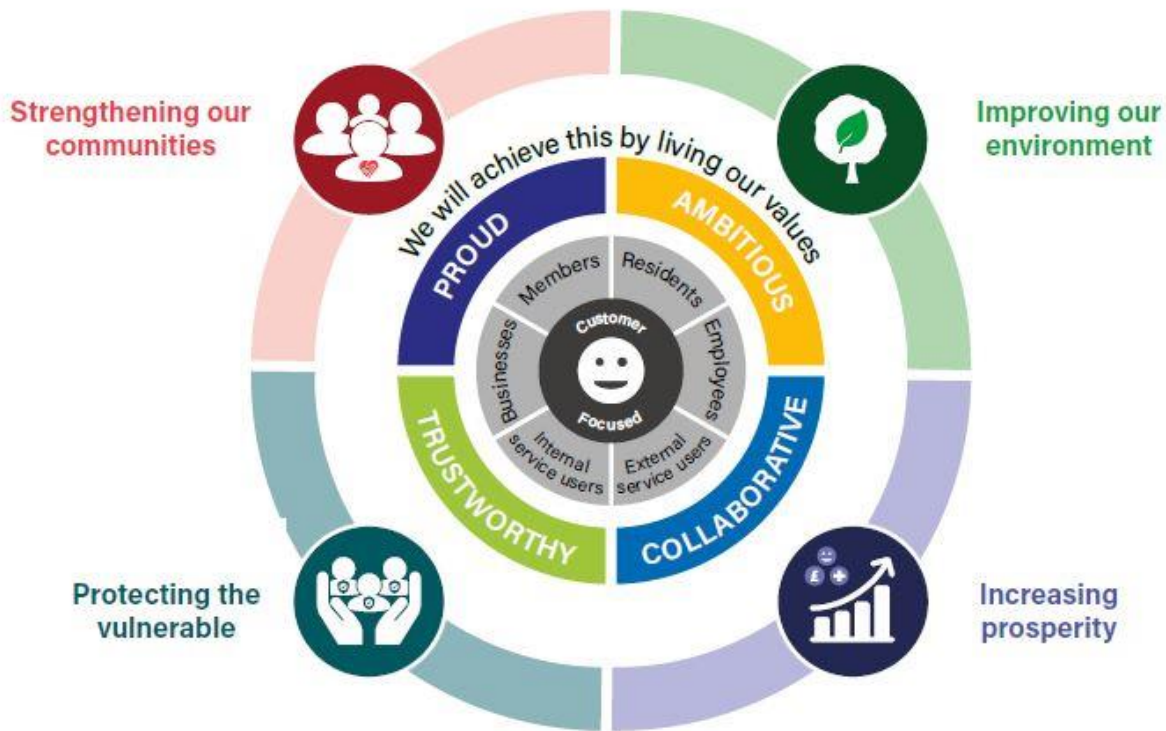
Fundamental to delivering these ambitions is the way the Council implements sound management of risks and opportunities. The Council is committed to adopting best practice in its management of risk to ensure risk is of an acceptable and tolerable level in order to maximise opportunities and demonstrate it has full consideration of the implications of risk to the delivery and achievement of the Council's outcomes, strategic aims and priorities.

The Council is clear that the responsibility for managing risk belongs to everyone across the Council and that there needs to be a good understanding of the nature of risk by all stakeholders. This is fundamental in making informed decisions and is becoming increasingly important as the Council pursues innovative ways of working in carrying out its service delivery.

The Council will adopt a robust approach to risk but strive to be risk aware - being prepared to accept risk at a tolerable level that can be managed and mitigated whilst ensuring that the most vulnerable are protected and there is increased collaboration with our partners, communities and residents.

This Strategy and its objectives are inherent to good governance practices and they have been endorsed by the Council's Cabinet and Corporate Management Team.

3

Chair of Audit and Governance Committee

Chief Executive

2. Aims and Objectives of the Risk Management Strategy

Risk management is an integral part of good management and is therefore at the heart of what we do. It is essential to the Council's ability to deliver public services and as a custodian of public funds. The current challenges facing local government means that now, more than ever, risks need to be identified effectively and managed carefully to mitigate adverse effects.

> *"Risk arises as much from failing to capture opportunities, as it does from a threat that something bad will happen."*

Effective risk management, including the identification and subsequent treatment of risks, can help the all areas of the organisation meet their objectives by demonstrating compliance, providing assurance, informing decision making and enabling value for money.

Risk Management is a useful tool for exploiting opportunities as well as safeguarding against potential threats, and acts as an early warning system. The Council is committed to the management of risk 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 or service users, members, pupils, tenants and all other stakeholders to whom the Council has a duty of care;
- Protect its property including buildings, equipment, vehicles, knowledge and all other assets and resources;
- Identify and manage potential liabilities;
- Maintain effective control of public funds and efficient deployment and use of resources achieving VfM;
- Preserve and promote the reputation of the Council;
- Support the quality of the environment;
- Learn from previous threats, opportunities, successes and failures to inform future management of risks.

The Risk Management Strategy provides a framework designed to support Members and Officers in ensuring that the Council is able to discharge its risk management responsibilities. The Risk Management Strategy aims to:

Establish a reliable basis for decision making and planning	Enable a robust risk manageemnt framework across the organisation	Increase the likelihood of achieving outcomes
Encourange a risk aware approach to enable innovation	Create an environment of "no surprises"	Provide those charged with governance with appropriate assurances

'If you don't have effective risk management, you don't have effective management.'

Chance or Choice: Guidance on Effective Risk Management and Internal Control in Local Government (SOLACE/ZM, 2000)

Key objectives of the Risk Management Strategy:

- Embed risk and opportunity management into the culture of the organisation;
- Develop a balanced approach to managing the wide range of business risks facing the Council;
- Manage risk in accordance with legislation and best practice; and
- Establish a common understanding of the Council's expectations on risk management with partners, providers and contractors.

3. Approach to Risk Management

Definitions

Risk is the '*effect of uncertainty on objectives*',* and an effect is a positive or negative deviation from what is expected. Therefore, the Council defines risk as:

Any potential development or occurrence which, if it came to fruition, would jeopardise the Council's ability to:

- achieve its corporate objectives and priorities
- provide services as planned
- fulfil its statutory duties, including the duty to make arrangements to secure continuous improvement and ensure financial stability

Risk Management is '*a coordinated set of activities and methods that is used to direct an organisation and to control the many risks that can affect its ability to achieve objectives**

*Source ISO 31000 'Risk Management – Principles and guidelines.

Risk Appetite

At its simplest, risk appetite can be defined as the amount of risk an organisation is willing to take in pursuit of its objectives. A well-defined risk appetite means members and officers are clear about which risks are acceptable and which risks should be avoided. Risk appetite should be at the heart of how we do business and sets the tone for the risk culture across the Council. Once it is properly understood and clearly defined, it can become a powerful tool to help take measured risks and improve overall performance and decision making.

The approach towards and appetite for risk can be:

- Averse - Preference for safe business delivery options that have a low degree of inherent risk and only a potential for limited reward.
- Cautious - Preference for safe delivery options that have a medium degree of residual risk and may only have limited potential for reward.
- Aware - Willing to consider all potential delivery options and choose the one that is most likely to result in successful delivery while also providing a good level of reward
- Hungry - Eager to be innovative and to choose options offering potentially higher business rewards, despite greater inherent risk.

[PLACEHOLDER: AGREE AND SET OUT THE RISK APPETITE]

The Council's risks appetite is determined by individual circumstances. In general terms, the Council's approach to providing services is to be innovative and to seek continuous improvement within a framework of compliance, delivering value for money and strong corporate governance.

Our aim is to have robust risk management at all levels across the organisation to encourage a less risk averse and more risk cautious/risk aware approach. This should enable innovation and opportunities to be taken within the Directorates whilst managing and addressing the barriers to success. However, the attitude towards risk will differ across the Directorates, from risk averse to risk aware. For example the Council's appetite for risk on matters of compliance with the law or safeguarding areas will be much lower.

Types of risk

Every organisation will face different types of risk - internal, external, strategic, and those arising from major projects, and the approach to managing them will differ.

Type of risk	Description	Examples
Internal	These are risks over which the organisation has some control, for example risks that can be managed through internal controls and, where necessary, additional mitigating actions. This often involves traditional risk management, such as risk registers, controls and assurance.	Fraud, health & safety, legal & regulatory, information security, data protection, safeguarding, contracts, people capability & capacity.
External	This focuses on big external events/perils and then considers how to make the organisation more resilient to such events. The approach to managing external risks is through considering the impact those external events could have on infrastructure, finance, people, operations and reputation. A common example is a business continuity plan.	Economic downturn, central government cuts, terrorist attack, extreme weather, cyber attacks
Strategic	This concerns the aims and priorities and aligns to the Council's Corporate Plan, identifying the principal risks to the achievement of those within a set timeframe.	These can be immediate impact risks to the organisation's ability to continue operating, e.g. loss of customer data; or slow-burning risks that grow and eventually prevent delivery of objectives, e.g. staff turnover or leadership capability.
Major programmes & projects	Major projects form such a critical part of the plans for many councils and should have their own risk management arrangements in place aligned to the Programme/Project Governance arrangements. Significant projects and/or risks should be escalated as required.	These risks will be specific to the major project in question, and could involve shifting requirements, budget overspend, slippage in delivery timeframes, failure to deliver.

Our approach to risk management is proportionate to the type of risk, decision being made or the impact of changes to service delivery/ strategies. Our risk management arrangements enable us to manage uncertainty in a systematic way at all levels of the council's business.

All key decisions presented to Cabinet must clearly show the key risks and opportunities associated with the decision/recommendations, the potential impact and how these will be managed. This helps promote informed decision making, particularly in an environment of uncertainty and change.

Risk Scoring

It is important that the organisation as a whole uses the same methodology to calculate risk to ensure that Buckinghamshire Council has an accurate overview of the risks that are posed. The risks are scored using two criteria scales that are then multiplied together to produce a total score by which the risk is assessed. The two criteria used are the Likelihood of an event occurring and the Impact that event could have. The criteria and methodology are set out in Appendix 2.

Identifying and ranking risks is important but the key element thereafter is to determine the strategy for managing them. The following table provides guidance on the level of management intervention that is likely to be necessary or appropriate.

Colour	Score	Action	Risk Control
Green	Very Low 1-3	Acceptable risk; No further action or additional controls are required; Risk at this level should be monitored and reassessed at appropriate intervals.	Tolerate/Accept or Treat and Control.
Green	Low 4-6	Acceptable risk; No further action or additional controls are required; Risk at this level should be monitored and reassessed at appropriate intervals.	Tolerate/Accept or Treat and Control.
Yellow	Moderate 7-12	A risk at this level may be acceptable; If not acceptable, existing controls should be monitored or adjusted; No further action or additional controls are required.	Tolerate/Accept or Treat and Control
Amber	High 13-20	Not normally acceptable; Efforts should be made to reduce the risk, provided this is not disproportionate; Determine the need for improved control measures.	Treat, Tolerate or Transfer.
Red	Extreme 21-30	Unacceptable; Immediate action must be taken to manage the risk; A number of control measures may be required.	All options can and should be considered.

4. Roles and Responsibilities

The Council recognises that it is the responsibility of all members and officers to have due regard for risk in performing their duties, and that they should not be afraid of identifying a risk or feel that identifying a risk is a failure or that we should try to eliminate risk unduly. To ensure risk management is effectively implemented, all Buckinghamshire Council Members and officers should understand the Council's risk management approach and embed risk management as part of their day to day activities.

Key roles in effective risk management are summarised as follows:
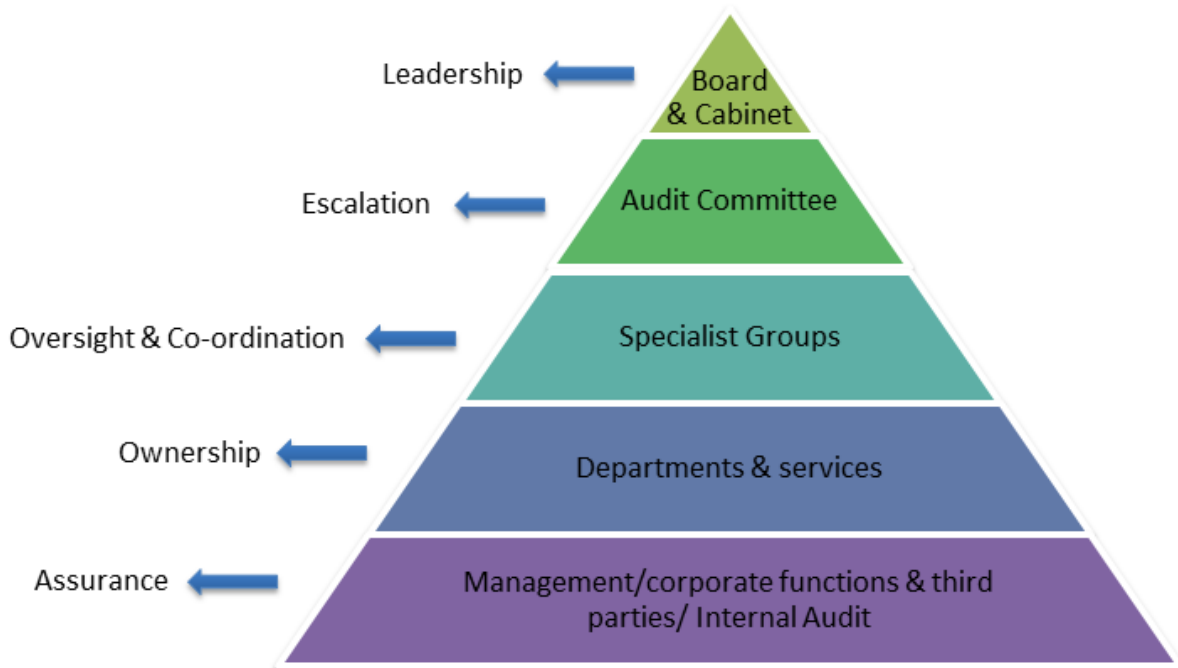
At Buckinghamshire Council, specific responsibilities with regards to risk are:

Who	Responsibilities (with regard to risk)
Leader and Members	Set the direction against political imperatives and articulate a high-level appetite for the risks to those imperatives. Has the ultimate accountability for the risk and related control environment. To endorse Council's Risk Management Policy and Risk Management Framework. Through the Audit & Governance Committee, the Council Leader and Members also have a responsibility to: • Oversee the effective management of risk by officers • Monitor the Council's risk management strategy and performance. Review regular reports from the CRMG on key issues affecting the Council. • Review and approve the Annual Risk Management Report submitted by the CRMG and the Annual Risk Assessment.
Audit & Governance Committee	Is responsible for overseeing the effectiveness of the council's risk management arrangements and has overall governance of the risk management process. Their role is to: • Approve the framework for risk management • Approve strategic risks and monitor progress • Monitor adequacy of management arrangements and directly raise queries with risk owners • Gain assurance of objectives being met • Delegation to sub-committee (Risk Management Group)
Corporate Management Team	Should set an appropriate tone from the top, for example by articulating risk appetite, championing and driving the effective management of risk and ensuring the risk function is supported in carrying out its role
Leadership Team (Corporate Directors & Service Directors)	Demonstrate visible commitment to risk management by: • Leading through actions - embracing risk based decision making aligned with strategic objectives • Having a clear understanding of the risks to the business • Ensuring assurance on the status of key risks and controls sought and followed through on a strategic and directorate level • Embedding of the policy and framework for managing risk
Risk Champions Group	Act as department risk 'champions', ensuring that risk management is given an appropriate profile and sufficient focus. • Play a lead role in the identification and monitoring of corporate risk • Receive updates on key risks & actions and assurances on effectiveness of risk management • Consider "very severe" and "serious" risks identified by projects, functional risk groups and department groups • Escalate new and emerging risks that may have a corporate impact to the Risk Manager and participate in ad hoc meetings of the Group to discuss such risks
Professional Leads/Specialist Groups	Are responsible for the facilitation and co-ordination of risk management activity in their specialist area across the council.
Managers	Should actively identify and manage risks as part of their everyday business, escalating them promptly as and when necessary • Identify, manage & monitor risks within their service area/team • Report and escalate risks in accordance with strategy • Monitor compliance and report exceptions to relevant Professional Lead
Risk Management function	Should support and facilitate the Council's management and oversight of risk. For example by building the organisation's risk capability and defining the organisation's risk management practices and framework.
Internal Audit	Should provide independent and objective assurance on the effectiveness of the organisation's risk management arrangements, and share good practice through comparative assessment
All members and officers	Manage risk effectively in their role and report risks as appropriate in accordance with procedures. Comply with polies and procedures and escalate exceptions appropriately.

5. Risk Reporting and Escalation

[PLACEHOLDER – CONTENT AND FREQUENCY OF RISK REPORTING TO BE AGREED IN-LINE WITH BUCKINGHAMSHIRE COUNCIL STUCTURE, ROLES & RESPONSIBILTIES AND AGREED WITH CORPORATE DIRECTORS AND IN LINE WITH CONSTITUTION/LOCAL CODE OF GOVERNANCE. EACH DIRECTORATE WILL HAVE A TAILORED RISK REPORTING/ESCALATION FRAMEWORK]

6. Culture, Awareness and Training

To ensure risk management is effectively implemented, all Buckinghamshire Council Members and officers should have a level of understanding of the Council's risk management approach and regard risk management as part of their responsibilities. Managing risk should be firmly embedded in everyone's thinking, behaviours and actions.

Having developed a robust approach and established clear roles and responsibilities and reporting lines, it is important to provide Members and officers with the knowledge and skills necessary to enable them to manage risk effectively.

A range of training methods are being developed to meet the needs of the organisation and include:

- Formal risk management training
- E-learning
- Risk workshops

Appendix 1 - Risk Appetite Matrix (example)

Risk levels Key elements	0 **Avoid** Avoidance of risk and uncertainty is a Key Organisational objective	1 **Minimal** (as little as reasonably possible) Preference for ultra-safe delivery options that have a low degree of inherent risk and only for limited reward potential	2 **Cautious Preference** For safe delivery options that have a low degree of inherent risk and may only have limited potential for reward.	3 **Open** Willing to consider all potential delivery options and choose while also providing an acceptable level of reward (and VfM)	4 **Seek** Eager to be innovative and to choose options offering potentially higher business rewards (despite greater inherent risk).	5 **Mature** Confident in setting high levels of risk appetite because controls, forward scanning and responsiveness systems are robust
Financial/VFM	Avoidance of financial loss is a key objective. We are only willing to accept the low cost option as VfM is the primary concern.	Only prepared to accept the possibility of very limited financial loss if essential. VfM is the primary concern.	Prepared to accept possibility of some limited financial loss. VfM still the primary concern but willing to consider other benefits or constraints. Resources generally restricted to existing commitments.	Prepared to invest for return and minimise the possibility of financial loss by managing the risks to a tolerable level. Value and benefits considered (not just cheapest price). Resources allocated in order to capitalize on opportunities.	Investing for the best possible return and accept the possibility of financial loss (with controls may in place). Resources allocated without firm guarantee of return – 'Investment capital' type approach.	Consistently focused on the best possible return for stakeholders. Resources allocated in 'social capital' with confidence that process is a return in itself.
Compliance/ regulatory	Play safe; avoid anything which could be challenged, even unsuccessfully.	Want to be very sure we would win any challenge. Similar situations elsewhere have not breached compliances.	Limited tolerance for sticking our neck out. Want to be reasonably sure we would win any challenge.	Challenge would be problematic but we are likely to win it and the gain will outweigh the adverse	Chances of losing any challenge are real and consequences would be significant. A win would be a great coup.	Consistently pushing back on regulatory burden. Front foot approach informs better regulation.
Innovation/ Quality/ Outcomes	Defensive approach to objectives – aim to maintain or protect, rather than to create or innovate. Priority for tight management controls and oversight with limited devolved decision taking authority. General avoidance of systems/ technology developments.	Innovations always avoided unless essential or commonplace elsewhere. Decision making authority held by senior management. Only essential systems / technology developments to protect current operations.	Tendency to stick to the status quo, innovations in practice avoided unless really necessary. Decision making authority generally held by senior management. Systems / technology developments limited to improvements to protection of current operations.	Innovation supported, with demonstration of commensurate improvements in management control. Systems / technology developments used routinely to enable operational delivery Responsibility for non-critical decisions may be devolved.	Innovation pursued – desire to 'break the mould' and challenge current working practices. New technologies viewed as a key enabler of operational delivery. High levels of devolved authority – management by trust rather than tight control.	Innovation the priority – consistently 'breaking the mould' and challenging current working practices. Investment in new technologies as catalyst for operational delivery. Devolved authority – management by trust rather than tight control is standard practice.
Reputation	No tolerance for any decisions that could lead to scrutiny of, or indeed attention to, the organisation. External interest in the organisation viewed with concern.	Tolerance for risk taking limited to those events where there is no chance of any significant repercussion for the organisation. Senior management distance themselves from chance of exposure to attention.	Tolerance for risk taking limited to those events where there is little chance of any significant repercussion for the organisation should there be a failure. Mitigations in place for any undue interest.	Appetite to take decisions with potential to expose the organisation to additional scrutiny/interest. Prospective management of organisation's reputation.	Willingness to take decisions that are likely to bring scrutiny of the organisation but where potential benefits outweigh the risks. New ideas seen as potentially enhancing reputation of organisation.	Track record and investment in communications has built confidence by public, press and politicians that organisation will take the difficult decisions for the right reasons with benefits outweighing the risks.
RISK APPETITE	NONE	LOW	MODERATE	HIGH	SIGNIFICANT	

Appendix 2 - Risk Methodology

Risk Scoring

Impact			Extremely Unlikely	Unlikely	Less Likely	Likely	Very Likely	Extremely Likely
	5	Severe	5	10	15	20	25	30
	4	Significant	4	8	12	16	20	24
	3	Moderate	3	6	9	12	15	18
	2	Minor	2	4	6	8	10	12
	1	Minimal	1	2	3	4	5	6
Score			Extremely Unlikely	Unlikely	Less Likely	Likely	Very Likely	Extremely Likely
			1	2	3	4	5	6
					Likelihood			

1-3	Very Low	Acceptable risk; No further action or additional controls are required; Risk at this level should be monitored and reassessed at appropriate intervals.
4 - 6	Low	Acceptable risk; No further action or additional controls are required; Risk at this level should be monitored and reassessed at appropriate intervals.
7 – 12	Moderate	A risk at this level may be acceptable; If not acceptable, existing controls should be monitored or adjusted; No further action or additional controls are required.
13 - 20	High	Not normally acceptable; Efforts should be made to reduce the risk, provided this is not disproportionate; Determine the need for improved control measures.
21 - 30	Extreme	Unacceptable; Immediate action must be taken to manage the risk; A number of control measures may be required.

Capacity to Manage	Description
Full	All reasonable steps have been taken to mitigate the risk and are operating effectively. The cost / benefit considerations on implementing additional controls have been considered and no additional actions are proposed.
Substantial	There are sound arrangements to manage the risk with some scope for improvement. Arrangements have had a demonstrable impact in reducing either the likelihood or consequence of the risk.
Moderate	There are a number of areas for improvement in arrangements that would help to demonstrate effective and consistent management of the risk.
Limited	There are significant areas for improvement in arrangements that would help to demonstrate effective and consistent management of the risk.
None	There is a lack of clear arrangements in mitigation of the risk.

Risk Rating – Likelihood

	Likelihood	Likelihood Descriptors	Numerical Likelihood
1	**Extremely Unlikely**	EITHER has happened rarely / Never before. OR less than 5% chance of occurring on or prior to proximity date.	Less than 5% chance of occurrence
2	**Unlikely**	EITHER only likely to happen once every 5 or more years. OR 5-20% chance of occurring on or prior to proximity date.	5% - 20% chance of occurrence
3	**Less Likely**	EITHER only likely to happen at some point within next 2-5 years. OR 20-45% chance of occurring on or prior to proximity date. OR circumstances occasionally encountered once a year.	20% - 45% chance of occurrence
4	**Likely**	EITHER likely to happen at some point within the next 2 years. OR 45-70% chance of occurring on or prior to proximity date. OR circumstances encountered few times a year.	45% -70% chance of occurrence
5	**Very Likely**	EITHER Likely to happen at some point within the next 12 months. OR 70-90% chance of occurring on or prior to proximity date. OR Circumstances encountered several times a year.	70%-90% chance of occurrence
6	**Extremely Likely**	EITHER Regular occurrence. OR Over 90% chance of occurring on or prior to proximity date. OR Circumstances that could give rise to the occurrence frequently encountered - at least monthly.	Over 90% chance of occurrence

Risk Rating – Impact

Score	Level	Service Delivery / Performance	Political / Reputation	Health and Safety	Technology / Data Protection	Financial
1	Minimal	Minimal service disruption in non-critical area of service for brief period (hours).	Contained within service area. Complaint from individual / small group / single supplier. No press interest. Minor delay in member objectives	Minimal injury or discomfort to an individual. Failure to report notifiable incident to the HSE.	Isolated individual personal detail compromised / revealed.	Costing <£1m.
		Commercial Plan Outcomes/ Objectives delayed by less than 1 month.	Complaint from an individual to a member or internal complaint from a member. Minor change to political landscape.		Minimal technological failure / security breach with minimal impact on day-to-day service delivery.	
2	Minor	Minor effect to an important service area for a short period (days).	Adverse local publicity / local public opinion aware. Lowered perception/standing with local suppliers.	Injury causing loss of working time to an individual. HSE Investigation leads to improvement notice served or threat of prosecution.	Some individual personal details compromised / revealed.	Costing = £1m to <£2.5m.
		Commercial Plan Outcomes/ Project / Objective fails to deliver on 1 important aspect. Delayed by up to 3 months.	Complaint or petition from a local group / delay to member objectives. Moderate change to political landscape.		Minor technological failure / security breach to the organisation's ICT assets impacting on the day-to-day delivery of services.	
3	Moderate	Moderate service disruption of an important service area for a period of up to a week.	Adverse national media interest and/or adverse publicity in professional/municipal press. Adverse local publicity of a major and persistent nature. Lowered perception/standing with national suppliers / professional / local government community.	Serious injury sustained by one or more individuals. Prohibition Notice served by the HSE that closes a key facility.	Many individual personal details compromised/ revealed	Costing = £2.5m to <£5m
		Commercial Plan Outcomes/ Major Project / Objective fails to deliver several key benefits. Delayed by 3 - 6 months.	Moderate criticism from local government community. Significant delay in member objectives. Significant change in political landscape.		Large technological failure / security breach with a significant impact on the organisation's ICT assets essential for the day-to-day operation of critical services.	
4	Significant	Significant service disruption, across several important areas of service for protracted period.	Adverse and persistent national media coverage. Adverse central government response, threat of removal of delegated powers. Public Enquiry. Officer(s) and/or Member(s) forced to resign. Council blacklisted by suppliers.	Serious permanent disablement of individual or several people. Prosecution under Corporate Manslaughter Act.	All personal details compromised/ revealed.	Costing = £5m to < £10m
		Commercial Plan Outcomes/ Complete failure of business critical project / objective. Delayed by over 6 months.	Significant and persistent criticism from central government. Major delay in member objectives. Major change in political landscape.		Significant technological failure / security breach with a detrimental impact on the organisation's ICT assets essential for the day-to-day operation of critical services.	
5	Severe	Complete service failure across all critical areas of service for protracted period.	Adverse and persistent international media coverage. Adverse central government response, threat of removal of delegated powers. Public Enquiry. Officer(s) and/or Member(s) forced to resign. Council blacklisted by suppliers.	Death of an individual or several people. Prosecution under Corporate Manslaughter Act.	All personal details compromised/ revealed and exposed to groups undertaking fraudulent activity.	Costing = £10m & over
		Complete failure to deliver Commercial Plan Outcomes/ business critical project / objective. Delayed by over 12 months.	Condemning criticism from central government. Complete failure to meet member objectives. Catastrophic change in national/international political landscape.		Severe and prolonged complete technological failure / full security breach with a detrimental impact on the organisation's ICT assets essential for the day-to-day operation of critical services.	