City & County of Swansea

Draft

Appendix B

Corporate Risk Management Framework

Purpose

This framework describes the specific risk management activities that will be undertaken within the City & County of Swansea. The aim is to help managers at all levels apply the principles consistently across their area of responsibility.

CIPFA state that *"Risk management is important to the successful delivery of public services. An effective risk management system identifies and assesses risks, decides on appropriate responses and then provides assurance that the chosen responses are effective."*

The Council recognises that it has a responsibility to manage risks effectively in order to reduce uncertainty in achieving its priorities and objectives and to benefit from opportunities. This framework applies to all Council staff and its principles should be applied when working internally or externally with partners and other stakeholders.

Definition of Risk

*"**Risk** is the threat that an event or action will adversely affect an organisation's ability to achieve its objectives and to successfully execute its strategies (CIPFA).*
2010*"*

Approval

Title	Date

Reference No.:	Version 1
Date:	6th March 2024
Author:	Strategic Delivery Unit
Website	http://staffnet/riskmanagement

Contents

1. Foreword

This framework aims to help employees, senior managers and elected Members to apply risk management principles consistently across their area of responsibility. The Risk Management Policy establishes the principles to guide decision making when applying risk management within the Council. This Risk Management Framework provides the practical method and structure for implementing the policy.

The intention of the framework is to help ensure that risk management is embedded into the culture of the Council, with members, managers and officers at all levels recognising that risk management is part of their jobs.

Clear identification and assessment of risks will improve corporate governance, corporate and service planning and performance and lead to more effective use of resources and direct improvements to the service to our customers.

The Council is increasingly involved in dealing with uncertainty and managing major change. We are under increasing pressure to deliver better services, increasingly in partnership with others, in new and innovative ways and within reducing budgets. All of this attracts risk which needs to be managed and controlled effectively if we are to achieve the desired outcomes.

The Council like all public bodies, as well as considering short and medium risks, will also have to understand and address the longer-term risks and challenges facing the Council and the community. We need to try and prevent risks from occurring and to mitigate their impact should they arise. We may need to work with others to prevent risks or to control and manage them. We need to be mindful that dealing with risks does not create risks and issues for other public bodies. Involving clients, customers and citizens in helping to prevent and to control and manage risks will help too.

Risk management is the process of identifying significant risks, evaluating the potential consequences and implementing the most effective way of responding to, controlling and monitoring them.

By being more risk aware, the Council will be better placed to avoid threats and to take advantage of opportunities when they arise.

Risk Management is everyone's business, but it will be championed and strongly led by the Cabinet's Cabinet, the Corporate Management Team, and Leadership Team.

Signed ……..

Rob Stewart
Council Leader

Martin Nicholls
Chief Executive

2. Definition of 'Risk'

Risk is the threat that an event or action will adversely affect an organisation's ability to achieve its objectives and to successfully execute its strategies (CIPFA).

3. Risk Management

Risk Management is the process by which risks are identified, evaluated and controlled and is a key element of the framework of corporate governance (CIPFA).

4. Corporate Commitment to Risk Management

The Council views the management of risk as an essential part of strong corporate governance. The approach is one of managing risk proactively and positively. Effective risk management helps improve services and outcomes, enhances accountability and ensures compliance with formal policies and procedures. Proactive and effective risk management is everyone's business.

5. Aims of the Risk Management Framework

The Council aims to be an exemplar of good practice and continue to meet its statutory responsibility to have in place satisfactory arrangements for managing risks, as laid out under The Accounts and Audit (Wales) Regulations 2014:

• Regulation 5 – Responsibility for internal control and financial management

• The Welsh Government wishes to emphasise that internal control, financial and risk management are corporate responsibilities which must be embedded in the processes of the relevant body as a whole.

The Well-being of Future Generations (Wales) Act 2015 requires public bodies to frame what risks they may be subject to in the short, medium and long term, together with the steps the public body will take to ensure they are well managed.

The Local Government and Elections (Wales) Act 2021 emphasises the importance of risk-aware governance through continuous performance review and self-assessment.

Through this framework, the Council aims to:

- ensure an effective risk management system is in place;
- Improve the ability of the Council to achieve its priorities and objectives.
- help employees, senior managers and Cabinet Members to apply risk management principles consistently across their area of responsibility;
- ensure that the risk management system identifies and assesses risks, decides on appropriate responses and then provides assurance that the chosen responses are effective;
- ensure that risk management is embedded into the culture of the Council, with employees, Members and managers at all levels recognising that risk management is part of their jobs;
- place greater emphasis on prevention rather than detection and correction;
- improve the identification, evaluation and control of strategic and long-term risks and operational risks;

- ensure that CMT, Cabinet, Governance & Audit Committee, external regulators and other stakeholders obtain necessary assurance that the Council is managing and mitigating its risks effectively;
- protect and enhance the assets and image of the Council;
- embed the Sustainability Principle (Well-being of Future Generations Act) and improve the Council's governance and decision-making processes and outcomes;
- capture strategic issues currently or imminently facing the Council and the actions being taken to manage them.

6. Risk Levels

There are two different levels within the risk register: strategic risks and operational risks.

Risks Levels

Strategic Risks are risks that could impact on the whole Council or could prevent the Council from achieving its corporate objectives or legal obligations.

Operational Risks are risks that could have a detrimental impact on a service or function and interfere with their delivery but would not have an impact on the whole Council and would not prevent the Council from achieving its corporate objectives or legal obligations.

7. Roles and Responsibilities

To implement this framework, specific roles and responsibilities for key stakeholders have been identified as outlined below:

Roles & Responsibilities

Leader

- Overall Cabinet responsibility for risk and resilience management.

Cabinet

- Approves the Council's Risk Management Policy and Framework.
- Shares ownership of strategic risks and issues with Corporate Management Team.
- Assesses / challenges the current and long-term risks associated with Cabinet reports.
- Sets the Council's risk appetite for each category of risk (see below).

Individual Cabinet Members:

- Share with the relevant Director ownership of specific strategic risks that are identified within their Cabinet remit.

Chief Executive

- Legal responsibility under the Local Government & Elections (Wales) Act 2021 to keep the Council's risk management arrangements and their operation under continuous review.

Corporate Management Team (CMT)

- Ensures an effective Risk Management Policy and Framework is embedded and is operating effectively across the Council.
- Shares ownership of strategic risks and issues with the Cabinet.
- Collectively reviews, monitors, and ensures control of strategic risks at least monthly.
- Ensures advice to Cabinet considers the current and long-term risks informs decision making.
- Champions risk management in the Council and leads by example.

Cabinet and CMT

- Share ownership of the Risk Management Policy and Framework and champions risk management throughout the Council.
- Shares ownership of strategic risks and issues and the response to them.
- Identifies and evaluates current and longer-term strategic risks during corporate planning and as they emerge.
- At Corporate Briefing meetings quarterly, reviews, monitors, and ensures control of strategic risks.

Directors

- Ensure the Risk Management Policy and Framework is embedded within their Directorates.
- Champion risk management throughout their Directorates.
- Identify and evaluate current and longer-term strategic risks and issues during corporate and service planning and as they emerge.
- Manage response to strategic risks and issues.
- Oversee response to operational risks.
- Review, monitor and ensure control of relevant strategic and operational Risks at least monthly.
- Ensure risks are escalated and de-escalated when necessary.

Heads of Service

- Ensure the Risk Management Policy and Framework is embedded within their Services.
- Champion risk management throughout their Services.
- Identify and evaluate operational risks during corporate and service planning and as they emerge.
- Manage response to operational risks.
- Review, monitor and ensure control of relevant operational risks at least monthly.
- Ensure operational risks are escalated and de-escalated when necessary.

Senior Information Risk Owner (SIRO)

- Ensure information risks are appropriately identified as strategic or operational risks.
- Ensure information risks are treated as a priority across all the Council.
- Provide Cabinet / CMT with assurance that information risks are being appropriately addressed.

Section 151 Officer

- The Section 151 Officer is responsible for advising the Council on key risks when setting the annual budget, certifying the adequacy of reserves and robustness of estimates, maintaining a balanced budget and on avoiding unlawful expenditure in order to prevent otherwise statutory intervention and ensure prudent financial management at all times.

Monitoring Officer

- The Monitoring Officer is responsible for advising the Council on key risks concerning lawful decision making, statutory obligations, standards of behaviour and codes of conduct in order to prevent illegality, maladministration and impropriety.

Project and Programme Managers

- Control, report and escalate programme / project risks above their agreed tolerance levels to senior management.

Managers and other Council officers

- Identify opportunities and manage risks effectively in their jobs, reporting any risk management concerns, incidents and 'near misses' to their line managers.
- Identify, evaluate, and control operational risks and ensure they are documented on relevant risk registers/trackers/reporting templates.
- Escalate worsening risks to Head of Service.

Internal Audit

- Provide an independent and objective opinion to the Council on the control environment (which comprises of risk management, control and governance) by evaluating its effectiveness in achieving the Council's objectives.

Governance & Audit Committee

- Challenge and provide independent assurance to the Members of the adequacy of the risk management policy and framework.
- Challenge and monitor the effective development and operation of risk management in the Council.
- Monitor progress in addressing risk related issues reported to the Committee.

Councillors

- Develop an understanding of risk management and its benefits.
- Be aware of how risks are being managed through the Risk Management Policy and Framework.
- Maintain an awareness of the risk management implications of policy decisions.

Responsible Officer on the InPhase system

- Manage, monitor, and control of an identified risk.

- Escalate risks for control and mitigation when necessary.
- Ensure risk scores and control measures are updated as soon as possible after a change in score or measure is agreed.

Updater On the InPhase system

- Update the risks recorded in the risk register.

InPhase Administrators

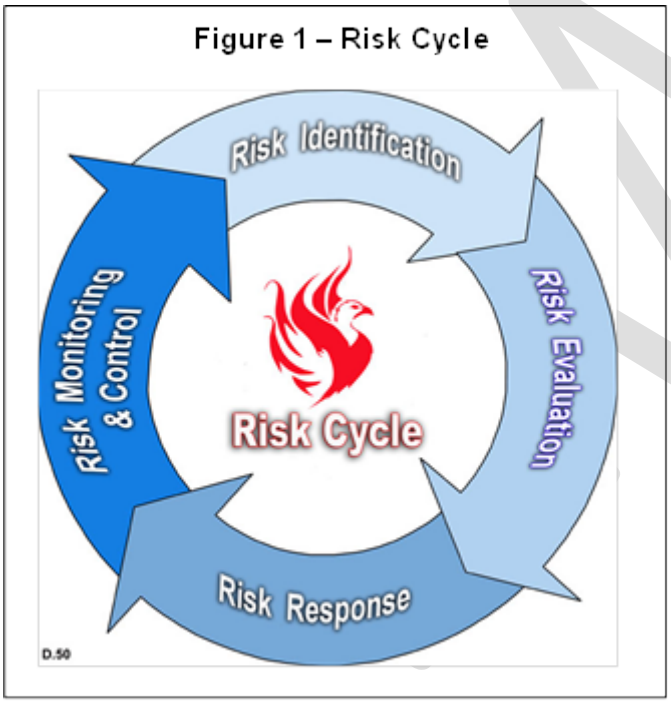
- Oversee the risk management policy and framework, quality assurance, maintaining policies and procedures and system administration and maintenance.

Risk awareness raising and training sessions will be provided for the workforce and for elected Members on identifying and reporting risks, including what to do if they identify a risk.

8. Risk Management Cycle

The Council implements a 'Four Step' Risk Management Cycle across the Council to provide a consistent approach to managing risk.

Figure 1 – Risk Cycle



Step 1 – Risk Identification

Step 2 – Risk Evaluation

Step 3 – Risk Response

Step 4 – Risk Monitoring & Control

8.1 Step 1 - Risk identification

The first step in risk identification is to understand the context within which the Council is operating and how this impacts on the Councils objectives and priorities.

Risks are formally identified and reviewed during annual corporate and service planning. including as part of the consideration of the threats to achieving our priorities and objectives.

The SWOT (Strengths, Weaknesses, Opportunities and Threats) tool and the PESTLE tool are useful tools to help scan the **current** and **future (long-term) organisational** and **external environment** in order to help **identify potential Strategic Risks**:

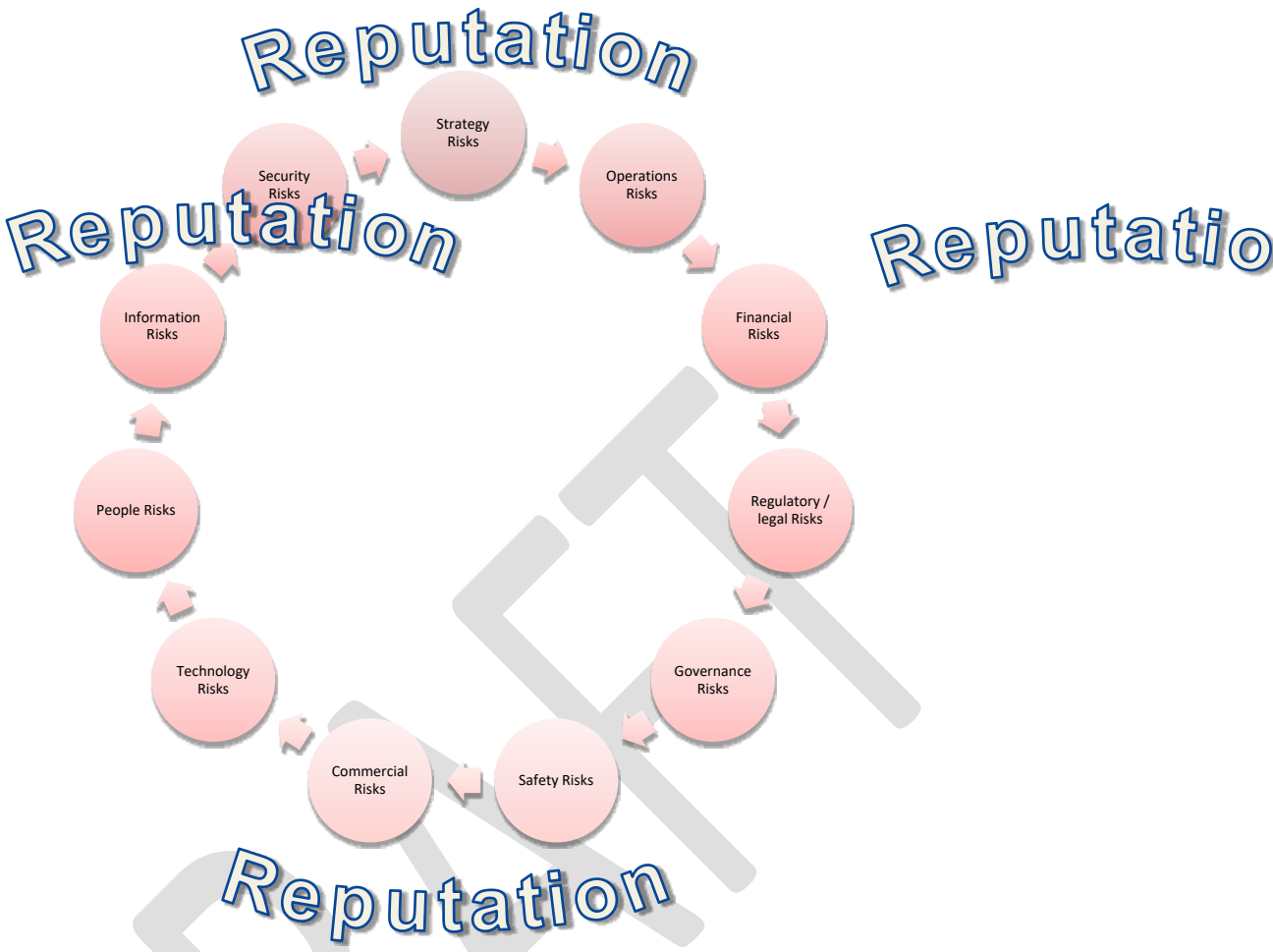
- **P**olitical forces, e.g. Brexit.
- **E**conomic factors (including financial), e.g. inflation rate.
- **S**ocial factors (including demographic / well-being), e.g. levels of deprivation.
- **T**echnological factors (including systems, information and data), e.g. cyber crime.
- **L**egal factors (including legislative),e.g. e.g. new regulations, laws.
- **E**nvironmental factors, e.g. climate action.

Operational risks can be identified during Service Planning by identifying the impact on the resources required to provide day-to-day services and meet operational targets and objectives. This is illustrated in fig 2 below..

Fig 2 – Identifying risks to achieving our priorities and objectives during service planning.

Note that new and emerging risks will also need to be recorded as they become known.

8.1.1 Risk Categorisation



Risk Categories
Strategy Risks arising from identifying and pursuing a strategy, which is poorly defined, is based on flawed or inaccurate data or fails to support the delivery of commitments, plans or objectives due to a changing macro-environment (for example, political, economic, social, technological, environment and legislative change). .
Service Delivery Risks arising from inadequate, poorly designed or ineffective/inefficient internal processes resulting in fraud, error, impaired customer service (quality and/or quantity of service), non-compliance and/or poor value for money.
Financial Risks arising from not managing finances in accordance with requirements and financial constraints, poor returns from investments, failure to manage assets/liabilities or to obtain value for money from the resources deployed, and/or non-compliant financial reporting.
Regulatory / Legal Risks arising from a defective transaction, a claim being made (including a defence to a claim or a counterclaim) or some other legal event occurring that results in a liability or other loss, or a failure to take appropriate measures to meet legal or regulatory requirements or to protect assets (for example, intellectual property.).
Governance Risks arising from unclear plans, priorities, authorities and accountabilities, and/or ineffective or disproportionate oversight of decision-making and/or performance..
Health and Safety Risks arising from safety deficiencies or poorly designed or ineffective/inefficient hazard management resulting in non-compliance and/or harm and suffering to employees, contractors, service users or the public. More information on Health & Safety Risk Assessments can be found at http://www.swansea.gov.uk/staffnet/riskassessments

Commercial Risks arising from weaknesses in the management of commercial partnerships, supply chains and contractual requirements, resulting in poor performance, inefficiency, poor value for money, fraud, and/or failure to meet business requirements/objectives.
Technology Risks arising from technology not delivering the expected services due to inadequate or deficient system/process development and performance or inadequate resilience.
Information Risks arising from a failure to produce robust, suitable and appropriate data/information and to exploit data/information to its full potential.
Security Risks arising from a failure to prevent unauthorised and/or inappropriate access to the estate and information, including cyber security and non-compliance with *General Data Protection Regulation* requirements.
Project / Programme Risks that change projects and programmes are not aligned with strategic priorities and do not successfully and safely deliver requirements and intended benefits to time, cost and quality.
Reputation Risks arising from adverse events, including ethical violations, a lack of sustainability, systemic or repeated failures or poor quality or a lack of innovation, leading to damages to reputation and/or destruction of trust and relations. All risks can cause reputational harm to the Council if not managed successfully.
Safeguarding Risks arising from failures to ensure the well-being of vulnerable individuals and to prevent harm.

Risk categorisation helps clarify the nature of risks, although in reality risks may be put into more than one category; attempts should be made to identify the main category that any risk should fall into.

The different categories of risk should help identify what type of risk we are dealing with. For Risk categories help **identify** and **classify** different types of risks faced by an organisation. By grouping risks into categories, it becomes easier to understand their nature and potential impact.

Use these categories to identify Strategic or Operational Risks.

8.1.2 Risk description

When identifying risks, use the knowledge and experience of those who know and understand the risk.

Aim to identify the risks to objectives.

Ask yourself the following questions:

- What can go wrong?
- How can it go wrong?
- Has it gone wrong before?
- When can it go wrong?
- Can we learn from experience elsewhere?

Use the following format to draft a risk description:

If ……. (what cause(s) that may give rise to a risk event) **then this will happen** …… (the risk event will happen) **with the undesirable consequence of** … (what the consequences are of the risk event occurring)

The risk description must be clear and precise and appropriate to the public domain. Here is an example of wording a risk using this format:

> **"If** *there is insufficient election staff training,* ***then*** *there is a risk that mistakes by inexperienced staff/staff not fully aware of procedures may be made at the polling station, leading to* ***(what we don't want)*** *voters not able to vote/results called into question".***"**

8.2 Step 2 - Risk Evaluation

The aim of risk evaluation is to prioritise individual risks so that it is clear which risks are most important and urgent. This will require and understanding of:

- The chances of it happening (**likelihood**);
- What would be the credible effect on objectives if it occurred? (**impact**).

The following table will help you assess risk impact for some risk categories:

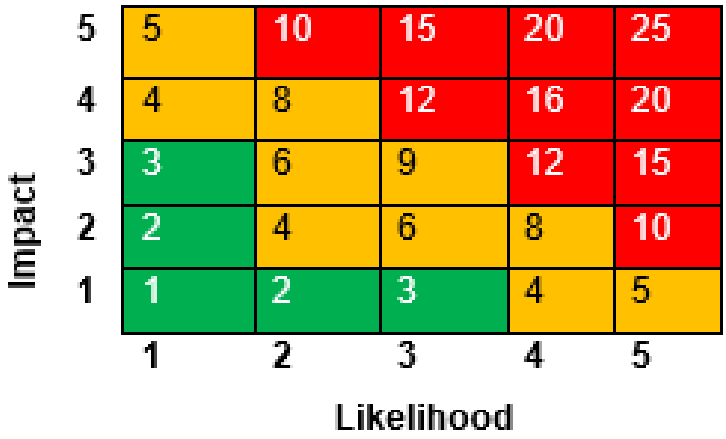
		Service delivery	**Financial**	**Reputation**	**Governance**	**Legal / Regulatory**	**Health & Safety, well-being**	**Commercial**	**Technology**	**Information**	**Security**	**Safeguarding**
1	**Very low**	Minor or short-term interruption to services.	Negligible loss	Minor concerns	Negligible loss of public confidence and trust in the Council; no legal or regulatory implications.	Very minor / near miss breach.	No injury or damage to well-being.	No weaknesses in the management of commercial partnerships, supply chains and contractual requirements.	No inadequate or deficient system/process development and performance or inadequate resilience	No fraudulent, unauthorised or negligent access, use, misuse or misplacing of information, records and data held that is confidential, commercial or otherwise sensitive.	No unauthorised and/or inappropriate access to the estate and to information / data.	Insignificant impact, no lasting impact. Unlikely to cause significant risk or to lead to complaints and easily and quickly resolved.
2	**Low**											
3	**Medium**											
4	**High**											
5	**Very High**	Unable to deliver services in the medium to long-term	Very significant financial loss	Very significant loss of trust, credibility and support	Very significant loss of public confidence and trust in the Council; very serious legal / regulatory implications	Very serious breach/loss contract/very high financial loss. Risk of imprisonment.	Real potential for serious injury or death.	Very serious weaknesses in the management of commercial partnerships, supply chains and contractual requirements	Very serious inadequacies / deficiencies in systems / process development and performance and resilience.	Very serious fraudulent, unauthorised or negligent access, use, misuse or misplacing of information, records and data held that is confidential, commercial or otherwise sensitive.	Very serious unauthorised and/or inappropriate access to the estate and to information / data.	Severe impact. Failure of corporate safeguarding to keep staff and residents safe. Possible risk of serious harm or death. Significant and long-term impact on reputation.

The following table will help you assess risk likelihood:

Likelihood		
1	**Very low**	Is not expected to occur (<5% chance)
2	**Low**	Small chance it will occur (5 to 20% chance)
3	**Medium**	Less likely not to occur than occur (20 to 50% chance)
4	**High**	More likely to occur than not (50 to 80% chance)
5	**Very high**	Is expected to occur (>80% chance)

- **Risk Matrix**

When evaluating the likelihood and impact of risks, the risk matrix (as shown in figure 3 below) can be used to help plot the risks.



You multiply the likelihood and impact scores together in order to get a risk scores, e.g. if a risk has a medium likelihood of occurring (3 = medium) and a high impact should it occur (4 = high), then it will be rated as RED and the score will be 12 (because 3 x 4 = 12).

At this stage, the risk score is known as the **'Inherent risk score'**. At this point in the process, this is the risk score **before** Risk Controls (Risk Controls are actions designed to mitigate the risk – see Step 3 Risk Response) are applied, i.e. the assessed likelihood and impact of the risk if we did nothing.

Within the Council, a RAG (Red, Amber, and Green) status will be used to evaluate these factors and it's important to recognise that each RAG colour represents a particular meaning as follows:

Red – Immediate Control - There are significant problems which will have a significant impact on the Council if it is not managed;

Amber – Close Monitoring - will affect the Council if it is not properly monitored and controlled;

Green – Regular Review - Going to plan but needs to be monitored on a regular basis.

When considering a risk's likelihood, another aspect is when the risk might occur. Some risk will be predicted to be further away than others and so attention should be focused on the more immediate ones first. This prediction is called the risk's **proximity**. Under the Sustainable

Development Principle, the Council should look to identify **longer-term risks** – See Section 8.3 Risk Response.

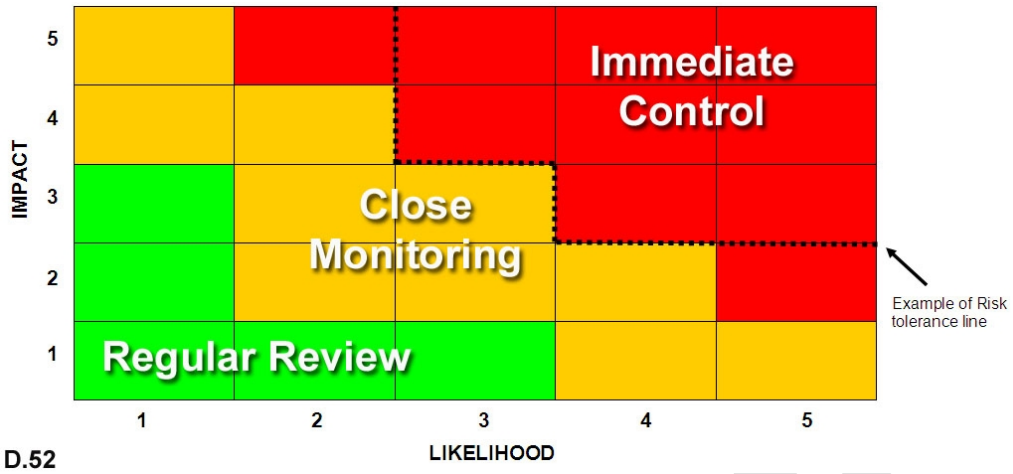


Fig 3 – Risk Matrix

8.2.1 Risk appetite

Risk appetite is the amount of risk the organisation is willing to take or accept in pursuit of its long-term objectives.

The Councils approach to taking risk (i.e., risk appetite) in that it will seek to minimise taking any unnecessary risks but also to reduce risk to an acceptable level to a public body. It also seeks to take risks to achieve its well-being objectives, but these will be properly considered before such risks are taken.

By articulating how much and type of risks which is acceptable it provides a basis for making judgements on the balance of the benefits and the taking of the risk.

The Council has set risk appetite levels for eleven categories of risk and these are be applied to all risks.

The following table provides definitions of risk appetites:

Risk Appetite	Description
Eager	Eager to be innovative and to choose options offering potentially higher rewards despite greater risk
Open	Willing to consider all potential delivery options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of reward, value for money, and moderate / high risk.
Cautious	Preference for safe delivery options that have a low degree of risk and may only have limited potential for reward.
Minimal	Preference for very safe business delivery options that have a low degree of risk and only have a potential for limited reward.
Averse	Avoidance of risk and uncertainty is a key organisational objective

The following table represents the **Council's Risk Appetite Statement**. It shows relative risk appetites for each of the categories of risk.

Risk Category	Possible Risk Appetite *(to be discussed and agreed by Cabinet / CMT)*
Strategy	Eager
Service Delivery	Cautious
Financial	Averse
Reputational	Cautious
Governance	Minimal
Legal / Regulatory	Minimal
Health & Safety	Averse
Commercial	Open
Technology	Cautious
Information	Averse
Security	Averse
Safeguarding	Averse

The risk appetite levels are indicative given the spread and complexity of risks within each category.

8.3 Step 3 Risk Response

The aim of this step is to prepare specific management responses, known as '**Risk Controls**', to the threats identified, ideally to remove or reduce the threat. Identify the actions that could affect either the cause or impacts of the risk. These risk controls are actions needed to mitigate the risk. Risk Controls need to be SMART.

Possible responses to risk should include a consideration of the four T's as follows to help identify appropriate risk controls:

- **Treat -** Treating the risk – This involves changing the likelihood of the consequences of the risk. This can be done in different ways:

    1. **Prevent**:
        - **Objective**: The primary goal is to **avoid** the occurrence of risks altogether.
        - **Actions**:
            - **Proactive Measures**: Implementing controls, policies, and procedures to prevent risks from materialising.
            - **Education and Training**: Educating stakeholders about risk awareness and best practices.
            - **Compliance**: Ensuring adherence to regulations and standards to prevent violations.
        - **Example**: Strengthening cybersecurity protocols to prevent data breaches.
    2. **Detect**:
        - **Objective**: To **identify** risks as early as possible.
        - **Actions**:
            - **Monitoring Systems**: Regularly monitoring processes, transactions, and activities.
            - **Alert Mechanisms**: Setting up alerts for unusual patterns or deviations.
            - **Audits and Reviews**: Conducting periodic audits to detect anomalies.

    - **Example**: Implementing fraud detection systems in financial transactions.
3. **Mitigate / Optimise**:
    - **Objective**: To **reduce** the impact or likelihood of risks.
    - **Actions**:
        - **Risk Mitigation Measures**: Implementing controls, safeguards, and risk-reducing practices.
        - **Scenario Planning**: Preparing contingency plans for various risk scenarios.
        - **Resource Allocation**: Allocating resources effectively to address risks.
    - **Example**: Developing disaster recovery plans to mitigate the impact of disasters.
4. **Recover**:
    - **Objective**: To **bounce back** after a risk event occurs.
    - **Actions**:
        - **Business Continuity Plans**: Having strategies in place to resume operations swiftly.
        - **Insurance Coverage**: Having insurance to cover losses.
        - **Post-Incident Analysis**: Learning from past incidents to improve future responses.
    - **Example**: Restoring critical services after a cyberattack.

Risk treatment strategies should be tailored to the specific context, organisational objectives, and risk appetite of the Council.

- **Transfer -** Transferring some aspects of risk to a third party, e.g. transferring financial risks (e.g., asset damage) by having assets covered by an insurance firm, or allocating risks to external partners through well-defined contracts.
- **Tolerate -** when the Council retains a risk because it falls within acceptable limits. It can be applicable when the likelihood and impact of the risk are low. Establishing tolerance levels helps prevent risks from exceeding defined thresholds. Responsible officers need to periodically review and monitor identified risks against these tolerance levels.
- **Terminate -** By doing things differently and thus removing the risk, where it is either feasible or practical to do so. It can also mean discontinuing processes or activities that create more significant risks than benefits, or risks that may be outside the Councils risk appetite or have severe impacts.

When considering how to respond to risks, the Sustainable Development Principle should be applied as outlined below:

- **Long-term**…looking at longer-term and emerging risks and looking to see how they may be prevented or their impact reduced, e.g. climate change.
- **Prevention…**looking to see how risks may be prevented from happening or their impact reduced should they occur.
- **Integration…**reviewing how risks, controls or responses may have a detrimental impact on the goals and objectives of other public bodies.
- **Collaboration…**reviewing working in partnership with others to help prevent, control or remove risks.
- **Involvement…**considering how involving stakeholders may help prevent, control or remove risks.

Once the Risk Controls have been identified, the '**residual risk score**' must be determined. The residual risk score is the score allocated to the risk once the risk controls have been applied, i.e. what is the level of risk now that risk controls are in place? You would expect the residual risk score to be lower than the inherent risk score. You can decide the residual risk score by referring to the risk matrix in Step 2.

Once the residual risk score has been identified, a '**target risk score'** must be calculated by referring to the risk matrix in Step 2. The target risk score is the score that the Council wishes to reduce the risk to. At this stage, any additional Risk Controls could be applied to help achieve the target risk score. Target risk scores should be tailored to the Councils risk appetite and risk tolerance applied to individual risks.

To help illustrate the different risk scores, the diagram below in Fig 4 shows **an example** of the risk matrix being used to plot inherent, residual and target risk scores.

Risk tolerance is distinct from risk appetite; it represents the amount of **residual risk** (see step 3 Risk Response) that an organisation is **willing to accept**. In other words, risk tolerance defines the acceptable deviation from the risk appetite once risk controls are in place. When identifying risk tolerance, a **risk tolerance line** could be plotted on the matrix to show that any risks above this line needs to be referred upwards for decisions. An example is plotted on fig 3 above and on fig 4 below.

Fig 4 – Scores plotted on Risk Matrix

The Risk Assessment Form attached at Appendix A can be used to guide and record the outcome from Steps 1, 2 and 3.

8.4 Step 4 Risk Monitoring and Control (implement, monitor and review)

During this step, planned risk management controls are implemented and monitored as to their effectiveness and corrective action is taken when responses do not match expectations.

Strategic Risks should be monitored on a monthly basis at CMT. Operational Risks should be monitored on a monthly basis at DMT/PFM and more frequently if necessary. The outcome from these risk reviews should be recorded in the Minutes and the Councils Risk Register updated when a change is agreed through these meetings. Directors and Heads of Service should

discuss relevant Strategic and Operational Risks with their relevant Cabinet Members during one-to-one meetings.

Strategic Risks will be reported quarterly to CMT, Cabinet (via Corporate Briefing) and to Governance & Audit Committee.

Risk Control Checklist

The following checks can be useful to help monitor and control the risk:

- ✓ Is the proximity of the risk still correct?
- ✓ Is the residual risk score (likelihood and impact of the risk occurring) still correct?
- ✓ Is the risk within the Councils risk appetite / tolerance?
- ✓ Are the risk controls in place the right ones?
- ✓ Are the risk controls in place accurate and up-to-date?
- ✓ Have the risk controls to the risk been implemented?
- ✓ Are the risk controls having the desired effect in meeting the risk target?
- ✓ Do additional risk controls need to be put in place to help control or mitigate the risk?
- ✓ Does the risk need to be escalated/de-escalated?

9. Risk Escalation / De-escalation

Risks would be escalated from operational level to strategic level when:

- A decision is required or actions need to be taken to mitigate risk that are beyond the authority or capacity of the Service or Directorate;
- When a broader view is required or the collective knowledge of the Service or Directorate is not enough to mitigate the risk.
- When the impact of a risk coming into effect is broader and goes beyond a single Service or Directorate.
- When the ‘tolerance line’ plotted onto the risk matrix has been crossed.
- When the Councils risk appetite has been exceeded.
- ‘Information only escalation’, i.e. when it is important that a higher body is aware of issues or risks that they may be required to take action on in the future.

A risk may be moved from Strategic to operational (de-escalated) for the following reasons:

- The risk can be controlled and managed at a lower level.
- The risk rating has decreased significantly or is not considered to be critical to the achievement of a well-being objective.
- The risk is below risk appetite boundaries.
- The risk will only affect one directorate / service unit and is better controlled locally.

Note – these guidelines must be exercised with some discretion and judgment from Heads of Service and Directors. For example, there may be political, reputational issues etc. that although may not be of the greatest corporate importance might still need to be escalated anyway.

10. Issues

In simple terms, an issue is an event that is happening or will happen imminently and will adversely affect an organisation's ability to achieve its objectives or deliver its legal obligations.

Issues will be recorded, managed and monitored within a Strategic Issues Register and reviewed by CMT on a monthly basis. Operational Issues will not be recorded on a register as these will be managed by Heads of Service as part of the day-to-day management of their service.

The process of identifying, recording, prioritising and dealing with / monitoring strategic issues consists of four steps:

- Identify and record strategic issues.
- Prioritise strategic issues.
- Create an action plan.
- Implement and monitor issue and action plan implementation.

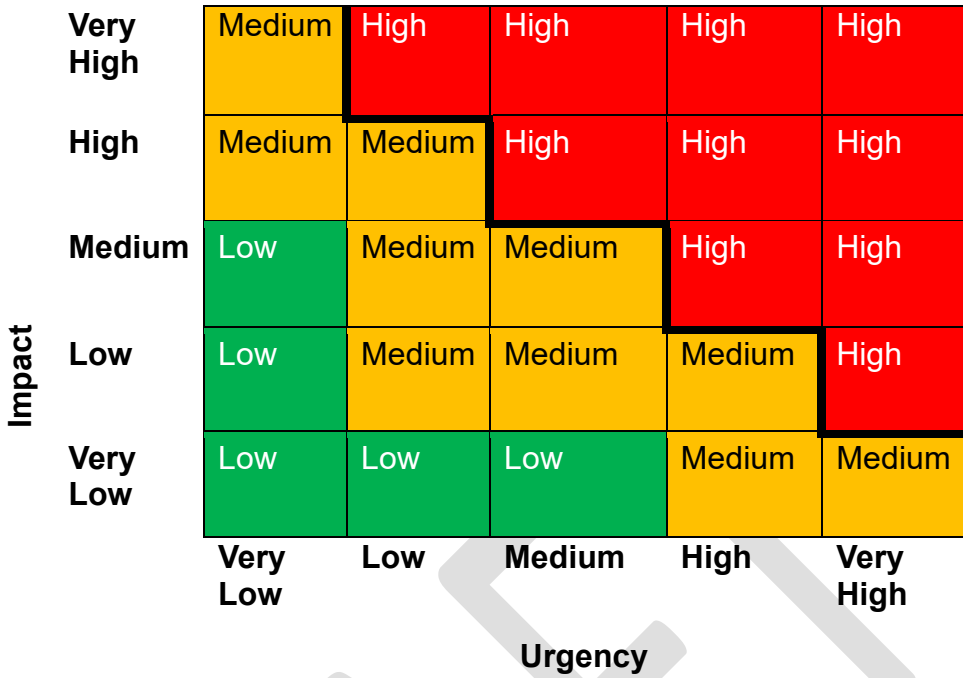
- **Step One: Identify and record issues**

  This step involves identifying the current strategic issues that are affecting or will imminently affect the Council's ability to achieve its corporate objectives or to meet its legal obligations and recording them in the Strategic Issues Register.

- **Step Two: Prioritise Issues**

  This step involves evaluating the impact and urgency of each issue using the Issues Matrix to rank them according to their impact on the Council's corporate objectives and legal obligations.

Issues matrix



High - Red – Urgent / Immediate resolution required.

Medium - Amber – Important resolution required.

Low - Green – Non-urgent resolution required.

- **Step Three: Create an issue action plan**

  This step involves assigning an issue owner, setting a deadline and deciding the required actions to resolve the issue.

- **Step Four: Implement and monitor**

  This step involves tracking the actions taken to address the issue and monitoring and reporting progress.

Appendix A - Risk Assessment Form

Directorate / Service / Project		Date	
Risk Category			
Risk Description (If…Then…We don't want)			
Responsible Officer			

Risk Assessment – before controls – Inherent Risk			
Impact Score		Overall Inherent Risk Score and RAG Rating	
Likelihood Score			

	List Risk Controls currently in place	Monitored by	How effective is the control? (S/M/W)*
1			
2			
3			
4			
5			
6			

Risk Assessment – with current Risk Controls – Residual Risk			
Impact Score		Overall Residual Risk Score and RAG Rating	
Likelihood Score			

	List additional Risk Controls to implement	By Whom? (name)	By When (date)
1			
2			
3			
4			

Risk Assessment – More Risk Controls – Target Risk			
Impact Score		Overall Target Risk Score and RAG Rating	
Likelihood Score			

* S = Strong, M=Medium, W=Weak