



**RISK MANAGEMENT FRAMEWORK
AND USER GUIDE**

**OCTOBER 2021
V5**

Risk Definition

Risk is defined as the **possibility that an event will occur, which will impact on our service delivery**. A 'risk' is made up of an event, which if left unmanaged will have an impact on the Council and our service delivery.

What is Risk Management?

Risk management is the process of identifying risks, evaluating their potential impact and mitigating them. The aim is to minimise the severity of their impact and likelihood of occurring where possible.

Defining a Risk

When defining a risk it should be very clear what the risk is to the Council and/or service delivery. If you have defined the risk and it is still not clear what the risk is it requires further refinement. The risk should be given an explicit risk title. Risks can lead to many different consequences e.g. – financial, reputational, performance. At this point you should use Risk Categories (table below) to help categorise the risk identified.

Risk Type

There are three main risk types, they are:

- **Strategic** - risks that have implications to the operation of the organisation for example Health and Safety, Systematic IT Failure and GDPR.
- **Operational** - risks that affect the successful delivery of individual service objectives/delivery plans which are controlled by a single portfolio.
- **Project Risks** – risks that prevent the successful delivery of a project or programme on time and on budget and to achieve the desired outcomes e.g. a capital investment project for a new school

Risk Categories

Category	Examples
Regulatory	<ul style="list-style-type: none">- Non-compliance with legislation- Data Protection/Freedom of Information Acts/ Human rights,- TUPE regulations- Health & Safety- Legal challenges- Corporate Governance- Licences- External Regulatory- Equality Act 2010
Environmental	<ul style="list-style-type: none">- Recycling / Green issues- Energy efficiency, Pollution, Carbon emissions- Climate Change; flooding and adaptation- Land use- Waste Strategy- Land and Property
Financial	<ul style="list-style-type: none">- Financial performance and management- Efficiencies- Financial procedural rules- Ability to meet financial commitments, including internal budgetary pressures

Category	Examples
	<ul style="list-style-type: none"> - Insurance cover/claims - Procurement - Contract standing orders - Fraud
Reputational	<ul style="list-style-type: none"> - Negative publicity - Legal challenges - Member support - Local/General election changes - Community Leadership - Project failure - External regulatory reports - Democratic Governance/Management - National Policy change
Social Impact	<ul style="list-style-type: none"> - Welsh Language - Social Justice - Equality Act 2010 - Impact on customer - Access to services - Safeguarding - Consultation/engagement/communication - Customer Feedback - Community cohesion - Community Strategy
Service Delivery	<ul style="list-style-type: none"> - Effective operations - Equipment, technology, information, employees - Performance - External Regulatory - Fraud
Health & Safety	<ul style="list-style-type: none"> - Vehicles - Hazardous Chemicals - Working Environment - Customer Health and Well-being - Plant Equipment

Escalation of Risk Protocol

When does a risk need to be escalated?

- When the risk tolerance¹ level is breached – this will be informed by risk evidence²
- When risk mitigation (action) cannot be resolved within the portfolio and;
 - a Council Plan/Strategy priority is compromised and/or
 - service operations or performance will be seriously compromised and/or
 - the financial, legal or reputational position of the Council might be compromised and/or
 - an emergency situation might develop

What is the process for dealing with escalation?

1. Accountable officers escalate risk to their respective Senior Management Team when risk cannot be mitigated or its rating managed/lowered

¹ Risk tolerance is the level of risk that the Council is willing to accept to achieve its service delivery.

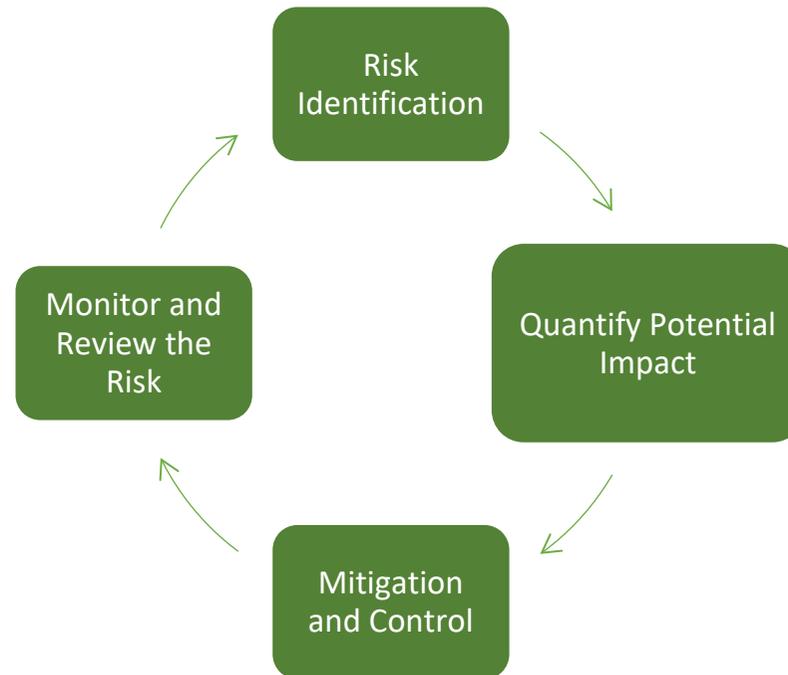
² Risk evidence is used to assess and manage risk, this includes performance indicators, financial data, actions and milestones.

2. Senior Management escalate to the Chief Executive Officer/Chief Officer Team if the risk cannot be mitigated or its rating managed/lowered
3. The Chief Executive Officer/Chief Officer Team escalate to Cabinet and Overview and Scrutiny where they believe the risk in its current state/predicted state is of corporate significance



Reassurance of process & management

- Officer 1:1s Chief Officers/line reports with Chief Executive
- Chief Officers to determine if aggregate risk needs to be referred to Chief Officer Team & corporately owned
- Risk Management is a standing item on all Senior Management Team Meetings (SMTs) agendas
- Revised Risk Management Framework and User Guide reported to Governance and Audit Committee – for periodic reviews
 - Case studies pulled out and challenged/scrutinised
- All risks of significance have been allocated out to relevant Overview and Scrutiny Committees
- Mid-year and Annual review by Governance and Audit Committee to ensure effective risk management
- Regular periodic review of portfolio risks (operational and strategic)
- Periodic reviews by internal audit



- **Step 1: Risk Identification** – Risk identification is a continuous process which is embedded in Council Planning, Portfolio Business Planning, Project Management and day to day service delivery. Risk should be identified by using qualitative (milestones & actions) and quantitative (performance indicators, financial) data. This is called Risk Evidence and will be used to quantify the risk scoring and also be used to measure against risk tolerance.
- **Step 2: Quantify Potential Impact** – What would the impact of the risk be without any mitigating controls or actions? Using the risk matrix below score the risk evidence gathered to provide the impact severity and likelihood. Definitions can be found for impact severity and likelihood below.

Risk Matrix & Definitions

Impact Severity	Examples					
Catastrophic	<ul style="list-style-type: none"> No confidence in Senior Management / Leadership Formal WG intervention/exercise of their powers Multiple fatalities Complete/critical service failure Exceedingly negative <i>national</i> publicity Serious impact on workforce across more than one Portfolio 			<ul style="list-style-type: none"> Legal action almost certain, unable to defend Serious financial impact to budget, not manageable within existing funds and may impact on reserves Non-compliance with law resulting in imprisonment Over £3m 		
Critical	<ul style="list-style-type: none"> Limited confidence in Senior Management/Leadership Significant service failure Negative <i>national</i> publicity Impact on workforce across more than one Portfolio Legal action almost certain and difficult to defend 			<ul style="list-style-type: none"> Serious financial impact to budget, manageable across the authority Negative external regulatory reports impacting on Corporate Governance Single fatality Over £1m but less than £3m 		
Significant	<ul style="list-style-type: none"> Significant service under performance Negative <i>local</i> publicity Expected impact on workforce, but manageable within Portfolio contingency arrangements Legal action expected Expected financial impact to budget, manageable within Portfolio 			<ul style="list-style-type: none"> Non-compliance with law resulting in fines Negative external regulatory reports Extensive, permanent/long term injury or long term sickness Over £100k but less than £1m 		
Marginal	<ul style="list-style-type: none"> Some risk to normal service delivery but manageable within contingency arrangements Legal action possible but unlikely and defensible Possible financial impact to budget, manageable within service 			<ul style="list-style-type: none"> Non-compliance with regulations / standards or local procedures resulting in disciplinary action First Aid or medical treatment required Previous risk mitigated by completed action plan Up to £100k 		
Likelihood	Unlikely	Very Low	Low	High	Very High	Extremely High
Definition	Highly unlikely, but it may occur in exceptional circumstances. There is no evidence to suggest that it will happen.	Not expected to occur. There is little evidence to say it is likely to happen.	There is a small possibility that it may occur. There is evidence that it will happen.	There is a good possibility that it may occur. There is clear evidence which supports that it will happen	There is strong possibility it will occur. There is evidence which support an expected occurrence	Highly likely to occur. There is clear evidence which supports a definite occurrence
Likelihood of risk happening						

Impact Severity	Catastrophic	Y	A	R	R	B	B
	Critical	Y	A	A	R	R	R
	Significant	G	G	Y	A	A	R
	Marginal	G	G	G	Y	Y	A
		Unlikely	Very Low	Low	High	Very High	Extremely High
Likelihood of risk happening							

- **Step 3: Mitigation and Control** – What are you going to do about it? - Management controls, action plans, day to day processes which are already or need to be put in place to either reduce the risk or keep the risk from escalating further (may not always be able to reduce the likelihood with management controls, however we would always look to reduce the impact). Apply the identified mitigation (action) and control measures. Have clear evidence (performance data, financial data, action and milestones) which indicate the mitigation (action) and control measures are working effectively. Reassess the risk against the Risk Matrix & Definitions above to give a current risk assessment.
- **Step 4: Monitor and Review the Risk** – Risks are to be regularly reviewed at the appropriate levels (Team Meetings, Senior Management Team, and Chief Officer Team Meetings). Performance of the associated controls, actions and measures should be monitored regularly. Risk monitoring is live and needs to be continuously monitored and escalation process followed where an increase in risk has been identified.

Capturing Risk

A risk method statement is to be completed for all risks and scored. The risk method statement is to be stored in an identified folder and uploaded onto the Performance Management System. The risk method statement should be completed by the risk owner/lead officer and have a supporting officer identified. When risk reviews take place the risk method statements should be reviewed at the same time. The detail on the risk method statement should be sufficient so that in the event the risk owner leaves the organisation or changes job role, the replacement would be able to read the method statement and have an understanding of the current position of the risk and all of its details and management controls.

Accountability for Risk

The basic requirements of the Risk Management Framework are:

- Chief Officer Team owning and leading the process.
- Ownership and understanding at every level and by every officer.
- Defined allocation of responsibilities and strong reporting lines.
- Risk identification evaluation and assessment.
- Mechanism for escalation and de-escalation.
- Active involvement by elected members.
- A monitoring role.

Statutory Officers

Head of Paid Service, Statutory Monitoring Officer, S151 Officer, Chief Officer - Education and Youth, Chief Officer - Social Services all have a responsibility to:

- Ensure that risks are managed within their relevant statutory roles
- Set strategic risk management levels
- Monitor and review risks within statutory roles

Chief Officer Team is responsible for:

- Setting strategic risk management initiatives/projects/action plans
- Discussing the appropriate level of risk for the Council (risk appetite)
- Identification and assessment of significant levels of risks
- Challenging the outcomes of risk management
- Monitoring and reviewing the Council Plan
- Assurance of Business Continuity Planning

Role of Elected Members

- Cabinet are responsible for:
 - Ensuring that the Council's risks are managed effectively
 - Setting the appropriate level of risk for the Council
 - Recommends the Council Plan to Council, its priorities and objectives with risks identified
- Overview & Scrutiny committees are responsible for challenging the detail of individual risks related to priorities or service/functions. All high level risks (red/black and increasing) are to be reviewed by the relevant scrutiny committees for assurance and monitoring of mitigating actions to reduce risk levels. This will be included in the forward work programme.
- Governance and Audit Committee is responsible for reviewing the effectiveness of the Council's Risk Management processes and systems. Governance and Audit Committee to receive a bi-annual risk monitoring report detailing risks being considered by scrutiny committees and their assurance

Role of Officers

It is the responsibility of Chief Officers and Performance Leads to ensure that Risk Management is implemented effectively in their areas.

Specific responsibilities are:

- Implementation of the Risk Management process and related policies.
- Ensuring that continuous risk identification, evaluation and escalation takes place and that action plans are developed, implemented and subjected to regular monitoring and review.
- Ensuring that all risks are updated in line with the Council's business planning and risk management arrangements.

Service Managers are responsible for:

- Informing Chief Officers of risks and completing relevant risk assessments.
- Maintaining the management of risks identified on a regular basis.
- Sharing relevant information with colleagues in other service areas.
- Providing feedback on their experience of strategy implementation and perceptions of strategy effectiveness to the senior management team.

All employees have a responsibility to:

- Maintain an awareness of risk factors in their workplace.
- Comply with Council policies and procedures.
- Notify their line manager of identified risk and suggested mitigation (action).
- Report all incidents to their manager/supervisor of risk tolerance breach.



Risk Method Statement

Step 1: Risk Identification

What do you want to achieve:	Insert here what you are trying to achieve? What is your ambition? What is your objective?
Risk Title:	<i>What is a short concise title of the risk? i.e. 'Council Tax Income'</i>
Risk Description:	<i>What is the name of the Risk? i.e. 'The Risk is....'</i>
Risk Type:	Strategic / Operational / Project
Risk Category (APPENDIX A):	Regulatory, Environmental, Financial, Reputational, Social Impact, Service Delivery, Health and Safety
Risk code:	What is the code you wish to allocate the risk? i.e. 'CF01, ST01, PE01
Lead Officer (Risk Owner):	Who is the Lead Officer for this Risk?
Service Area:	<i>Which service area does the Risk belong to?</i>
Council Plan/Strategy Link:	What Link does the Risk have to Council Plan / Strategies / Projects?
Performance Lead:	Who is the accountable Performance Lead?
Supporting Officer:	Who is the Supporting Officer (secondary contact) for this risk?

Step 2: Quantify Potential Impact

Use Risk Matrix (appendix B) to complete below:	Likelihood	Impact	Risk Score (Raw)
Raw Risk Assessment (without any management controls):	Choose an item.	Choose an item.	Choose an item.

Step 3: Mitigation and Control

Use Risk Matrix (appendix B) to complete below:	Likelihood	Impact	Risk Score (Target)
Target Risk Assessment: <i>(Think about your appetite for these risks. Give each one a target risk score that reflects the level of risk you'd be happy to accept)</i>	Choose an item.	Choose an item.	Choose an item.
Supporting Comments:	<i>Include any details here which will support your target score. This is the area you our setting your tolerance for this risk</i>		

Use Risk Matrix (appendix B) to complete below:	Likelihood	Impact	Risk Score (Controlled)
Current Risk Assessment (with current management controls):	Choose an item.	Choose an item.	Choose an item.
Management Controls:	<i>How is this Risk being managed and controlled? List all controls/actions you currently have in place to reduce and control the risk</i>		
Indicators: (which indicators will show you these expected controls ARE working and therefore your assessment of progress towards target risk score is reasonable)	<i>List all key indicators which show current controls are working effectively</i>		
Action Plan required: (If your current risk score is higher than your target risk score (ie current controls don't reduce the risk to a level you're happy with), list the additional actions needed to reduce the risk further)	<i>here is your action plan - the information here will depend on the degree of difference between current and target</i>		
Action Plan Indicators: (which indicators will show you these expected controls ARE working and therefore your assessment of progress towards target risk score is reasonable)	<i>Should be a list, specifics and not just we plan to have a meetings - these should show an impact on current performance and therefore a reduction /increase in current score</i>		

Step 4: Monitor and Review

Frequency of Reporting:	Choose an item.		
Reporting to (DMT, COT, Cabinet etc.):	Where will you be reporting the Risk to?		
Date Risk reviewed:		Next Risk review date:	
Risk reviewed by:		Risk review agreed by Lead Officer:	

Impact Severity	Catastrophic	Y	A	R	R	B	B
	Critical	Y	A	A	R	R	R
	Significant	G	G	Y	A	A	R
	Marginal	G	G	G	Y	Y	A
		Unlikely	Very Low	Low	High	Very High	Extremely High
Likelihood of risk happening							