West Lancashire Borough Council

Risk Management Tool Kit

Version 1: March 2021

Contents

1. Foreword

As Chief Operating Officer I am responsible for enabling the efficient and effective governance of significant risks, and related opportunities across West Lancashire Borough Council.

As we face increasing uncertainty and challenging times it is of increasing importance that we have robust management and are able to make difficult decisions over resource priorities. It is important that the maximum amount of resources can be channelled into achieving the Councils vision and priorities for West Lancashire.

Central to the ability to do this is the need for efficient and effective risk management which allows us to take advantage of more opportunities and make decisions that pay full regard to risk consideration.

The Council is risk aware not risk adverse, it needs to take full advantage of opportunities for improving services. Therefore, it needs to be pro-active and prepared in the way that it manages risk.

Risk Management is recognised as a key element in the management of the Council. By all staff having a better understanding of the importance and implementation of risk management it will make a huge contribution to improving overall corporate governance. In addition it will assist in ensuring that mandatory rules, regulations and obligations are complied with.

Better identification of risks and their management will result in better use of resources. If we all use the resources available to us more efficiently and effectively then the service to our customers can only improve.

Risk Management needs to be embedded in all activities of the Council and it's important that we align risk management activities with other policies, procedures and strategies to ensure effective operations and service delivery.

This toolkit has been developed to allow officers to identify risks which would prevent them from achieving their objectives (including failing to take advantage of opportunities) and to provide information and guidance on how these risks can be managed.

Jacqui Sinnott-Lacey

Chief Operating Officer

2. Introduction

Risk management is about making the most of opportunities by making informed decisions and about achieving objectives once those decisions are made. It is about being risk aware and not risk adverse.

The Council accepts that some level of risk is inevitable if it is going to achieve its objectives. It is important, however, that these risks are actively controlled, managed and monitored. One of the biggest risks that could face WLBC would be to not identify the risk in the first place and take no action at all.

Risk management is the process by which risks are identified, analysed, evaluated, treated, monitored and reported. It is part of the code of corporate governance which considers how well the authority carries out its duties and responsibilities against six key components:

1. Focusing on the purpose of the authority and on outcomes for the community and creating and implementing a vision in the local area
2. Members and officers working together to achieve a common purpose with clearly defined functions and roles
3. Promoting values for the authority and demonstrating the values of good governance through upholding high standards of conduct and behaviour
4. Taking informed and transparent decisions which are subject to effective scrutiny and managing risk
5. Developing the capacity and capability of members and officers to be effective
6. Engaging with local people and other stakeholders to ensure robust public accountability

Risk management is not a new process; it is a formalisation of processes that are already in place. Risk is a part of everyday life and you will undertake many conscious and sub conscious risk assessments every day. Risk management is integral to a well-managed Council; it is something that managers undertake every day. It is so intrinsic to their jobs that often they do not realise they are doing it. It is crucial that the aims and objectives of Services or the Council as a whole can be clearly linked with the risks involved. Risk management should be embedded within the strategic planning, decision making and core processes of the Council.

The process has been made as simple as possible, and jargon has been kept to a minimum. There may be some terms that you may not be familiar with; therefore a list of the more common terms has been included at Section 18, Key Definitions, for your guidance.

This toolkit is a working document for managers and staff to use in maintaining the documentation required to support their Service and the Council's Corporate Risk Registers. Although risk owners will be tasked with updating risk registers and managing risks, risk management is the responsibility of all Council employees.

This toolkit should be read in conjunction with the Council's Risk Management Policy.

3. Attitude to and Principals of Risk Management

We are able to be risk aware, not risk adverse, by ensuring that risk management is an integral part of our planning and review processes, including the evaluation of new opportunities.

Effective risk management enhances:

- the likelihood of us delivering our objectives;
- our reputation;
- our financial sustainability;
- our planning and decision-making activities;
- our leadership, management and governance;
- our core business;
- our ability to innovate.

The approach adopted to risk management ensures that our risk management activities are:

- Proportionate to the level of risk that we are prepared to accept.
- Aligned with other Council activities.
- Comprehensive, systematic and structured.
- Embedded within the Council and our procedures.
- Dynamic and responsive to emerging and changing risks.

The approach that we have taken to risk management is that:

- Members and CMT are responsible for determining the risk appetite of the Council.

- Members and CMT are responsible for determining the nature and extent of the principal risks we are willing to take in achieving our strategic objectives.

- Members and CMT are responsible for ensuring that the risks on the Corporate Risk Register fit within the definition of a Corporate Risk (section 11.2)

- Heads of Service are responsible for ensuring that corporate risks are added to and removed from the Corporate Risk Register as appropriate.

- Executive Overview & Scrutiny Committee and Cabinet receive twice yearly reports on the Corporate Risks facing the Council.

- Audit & Governance, Executive Overview & Scrutiny Committee and Cabinet receive an annual report on the Risk Management Policy (including the Council's Risk Management Strategy and Risk Appetite Statement) and Toolkit to approve these for the forthcoming year.

- Audit & Governance Committee monitor our risk management and internal control systems and Internal Audit periodically audit their effectiveness.

- The Corporate, Senior Management Team and Risk Management Champions are responsible for the implementation of risk management systems, and disseminating best practice throughout the Council.

- CMT receive quarterly reports on risks facing the Council.

- Heads of Service are responsible for carrying out live reviews of Service Risk Registers on a quarterly basis.

- Officers assigned to a risk are responsible for updating, maintaining, controlling and monitoring it.

- Control owners are responsible for communicating the effectiveness of controls to risk owners.

4. Councils Risk Management Policy

Our Risk Management Policy including our Strategy support our corporate aims and objectives.

The Council has a clear vision for West Lancashire:

West Lancashire together; the place of choice to live, work, visit and invest

Our priorities are:

- Create empowered, engaged and inclusive communities
- Support businesses to adapt and prosper
- Become a Greener West Lancashire
- Be a financially sustainable Council by 2023
- A clean, safe environment with affordable homes to buy or rent for everyone in West Lancashire
- Everyone to be healthy, happy, safe and resilient
- Everyone to be proud of their Council

Robust risk management will help to support delivery of this vision and associated priorities.

The Risk Management Policy sets out the Council's risk management aims and objectives and how these will be achieved. This document is subject to annual review to ensure that it remains up-to-date and continues to reflect our approach to risk management.

It is vital that we develop the use of risk management in our dealings with third parties such as through partnerships, contracts, and other new service delivery models.

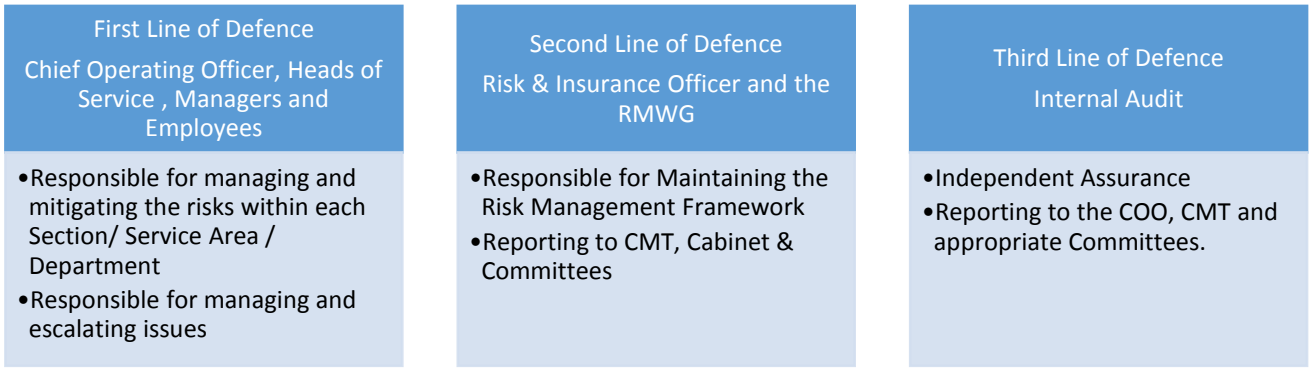
While these areas contain significant risks for the Council, they also have the potential to provide significant opportunities if well managed. The use of risk management to mitigate risks while also exploring opportunities is key to ensuring that these working arrangements contribute positively to service delivery.

5. Three Lines of Defence Model

The Council operates a Three Lines of Defence Model which provides assurance that Risks are being actively managed and controlled. By having the three lines of defence in operation it allows us to safeguard against breakdowns in risk management. It also emphasises that risk management is everyone's responsibility.

The Three Lines of Defence model distinguishes among three groups (or lines) involved in effective risk management:

- Functions that own and manage risks.
- Functions that oversee risks.
- Functions that provide independent assurance.



In addition to the three lines of defence there are then a further two functions:

4th Line of Defence - External auditors will be required to confirm and attest to the accuracy of financial records.

5th Line of Defence – Certain regulators will require compliance with the rules and regulations within their scope.

Our risk and control processes are structured effectively in accordance with the Three Lines of Defence model in that;

- Each line of defence are supported by appropriate policies and role definitions.
- There is coordination among the separate lines of defence to foster efficiency and effectiveness.
- Risk and control functions operating at the different lines share knowledge and information to assist all functions in better accomplishing their roles in an efficient manner.
- Lines of defence are not combined or coordinated in a manner that compromises their effectiveness.

A more detailed breakdown of the roles and responsibilities of each line can be found in Sections 6 – 9.

6. The Audit & Governance Committee

The Audit and Governance Committee Terms of Reference are included at appendix C.

The purpose of the Audit and Governance Committee is to support the Council's Corporate Governance responsibilities and to provide independent assurance in relation to internal control, risk management and governance.

The Audit and Governance Committee has a strong focus on risk and internal control as well as on good financial management.

The Committee is comprised of eleven members drawn from across the political parties in accordance with the rules of proportionality. The Chair is from the leading party and does not have Cabinet responsibilities but is on the Corporate and Environmental Overview and Scrutiny Committee as a member.

The Audit & Governance Committee meetings are held in public, although there are occasionally private reports received where the public are excluded.

7. Corporate Management Team(CMT)

The Corporate Management Team is comprised of the Chief Operating Officer, Directors and Heads of Service. Risks are reported to CMT on a quarterly basis.

8. Risk Management Working Group (RMWG)

The RMWG is comprised of the Head of Finance and Audit, representatives from Internal Audit, the Risk and Insurance Officer and Risk Management Champions. Other officers may be invited to attend as appropriate.

Coordinated by the Risk and Insurance Officer the RMWG is responsible for maintaining and developing the Risk Management Framework.

The RMWG meets twice yearly and more frequently if required, to consider the following;

- Issues and improvements to the Risk Management Framework,
- Risk management training requirements,
- Risks facing the Council,
- Disseminating good practice requirements for risk management,
- How to further improve and embed risk management culture within the Council, to support its decision making process, strategies and operations.

9. Risk Management Champions.

Risk Management Champions are responsible for maintaining and developing the Risk Management Framework within their Service, supported by the RMWG.

The Risk Management Champion's role is to:

- Attend meetings of the RMWG or nominate a suitable substitute when unable to attend.
- Disseminate information discussed at the RMWG to their Service and feedback to the group accordingly.
- Support their Head of Service in implementing the Risk Management Framework within their Service.
- Raise any issues regarding risk management with the Risk and Insurance Officer.
- Advise the Risk and Insurance Officer if any risk management or Pentana training is required within their service.
- Give advice and guidance to managers/officers within their Service on preparing risk assessments for committee reports.
- Provide advice and guidance to those updating risks on the Pentana system.
- Help to promote and embed Risk Management within their Service in order to engage staff in the management of risk.

10. Context to Risk Management

Formally incorporating risk management into day-to-day management increases the focus on what needs to be done (and not done) to meet objectives. It ensures;

- Conformity with applicable rules, regulations and obligations.
- Assurance is provided that risk management and internal control activities are sufficient.
- Appropriate risk based information is available to support decision making.
- The achievement of an effective and efficient strategy, tactics, operations and compliance, to ensure the best outcome and volatility of results.

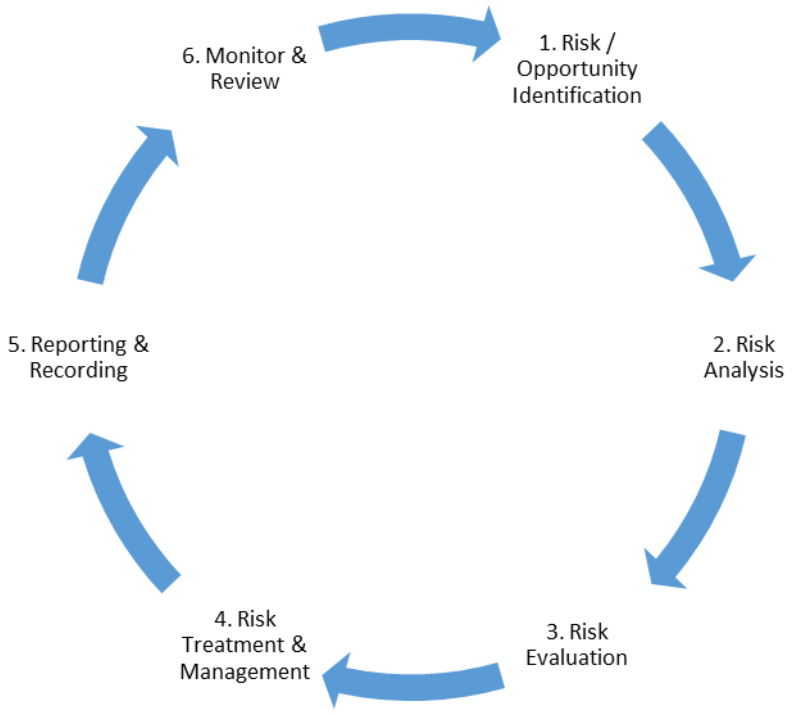
This results in:

- Improved efficiency in the delivery of services
- Enhanced risk reporting
- More satisfied stakeholders
- Better management of change programmes
- Support for innovation
- Fewer complaints
- Greater control of insurance costs
- The provision of evidence to support Assurance Statements
- Better information available for decision making
- Enhanced ability to justify actions taken
- Protection and enhancement of our reputation
- Reduced risk of mistakes
- Conformance with Council policies across all areas of risk
- Improved management performance (good risk management is good management)
- Consistent approach avoiding potentially damaging errors
- Compliance with legislation, rules and regulations
- Securing funding (funding bodies including the government are increasingly interested in the effective management of risk)
- Improved contingency arrangements as set out in our business continuity plan
- A reduction in the risk of fraud and corruption
- Enhanced ability to identify new opportunities and the challenges associated with current opportunities

- Being able to anticipate the risks that could affect performance and put in place actions to minimise disruption
- Better assessment of overall resource needs
- The ability to quickly foresee and respond to change.

11. The Risk Management Process

Our risk management processes has 6 key stages:



11.1 Risk / Opportunity Identification

The starting point for the identification of risks and opportunities should be to examine the Councils, Directorate, Service or project's objectives and required outcomes. It is important that officers carry out risk identification and examine all identified risks and link them to the appropriate Council, Service or project objectives and outcomes. If a risk cannot be clearly linked to an objective or outcome then serious consideration should be given as to whether this risk needs to be borne at all.

Risk Management should feature on the agenda of quarterly DMT meetings and therefore managers should be aware of emerging risks or changing risk context.

It is important that all members of staff are involved in the risk management process. Managers should ensure that there is a process in place for employees to actively report any risks as and when they arise, and also for them to report when the extent of the risk changes.

Officers assigned to risks i.e. risk owners should update Pentana with any new risks that have been identified and continue to keep risks updated with real time updates.

Some risks will be identified on an on-going basis but will be rectified almost immediately and will therefore not form part of the formal risk register e.g. a missing sign on an emergency exit should not be included, but should be rectified as soon as possible. If, however, it was noted that emergency exit signs were being stolen on a regular basis, this fact should be recorded.

There are many ways of identifying risk:

- Experience
- Checklists and questionnaires
- Inspections of premises
- Audits (Internal e.g. internal audit, health & safety or external)
- Risk assessments
- Equality analysis
- Directorate / Service / team meetings
- Workshops and brainstorming
- Internal control processes
- Day to day operations
- Local / National or Social Media
- Alterations to legislation
- Performance Indicators
- Service Action Plans
- Insurance claims / losses information

The list below is provided as a guide and is **not designed to be all encompassing**, but is intended to give you a starting point to identify risks. The risk identification stage should be repeated regularly to ensure that new risks arising are identified and brought into the risk profile as appropriate.

Categories of risk:

Reputational risks - Arising from all risk types / categories which are considered to have an impact on how the Council is viewed by both internal (e.g. staff) and external stakeholders (e.g. citizens, suppliers).

Legislative / Regulatory/ Compliance risks - Arising from current and potential changes and the organisation's regulatory environment.

Examples of issues to look for in local government:

- Preparedness for new, and compliance with existing, legislation and regulations including European law / regulations, e.g. H&S regulations
- Exposure to regulators - e.g. auditors / inspectors
- Localism Act and the various rights this gives local people such as Community Asset Transfers

Financial risks - Arising from the budgetary, financial planning and control framework.

Examples of issues to look out for in local government:

- Financial situation such as areas of significant over or under spending
- Flexibility to allocate budgets to address areas where control weakness is identified
- Level of reserves and budgetary control

- Monitoring and reporting systems
- Fraud / mal-administration and corruption

People risks - Arising from the need to be managerially and professionally competent and for staff to be satisfied.

Examples of issues to look out for in local government:

- Professional / managerial standing of key officers
- Stability of officer structure - particularly at the top
- Key staff changes and personalities
- Turnover, absence, stress levels, illness
- Workforce planning
- Equalities issues
- Managing major changes

Health & Safety Risks – Arising from the need to provide a safe environment for staff, citizens and all stakeholders.

Examples of issues to look out for in local government:

- Is appropriate training given to staff?
- Is there a safer way of working?
- Have staff got the appropriate equipment?
- Commitment to health, safety and well-being of staff, partners and the community
- Potential physical hazards such as monitoring the condition of trees on WLBC owned land or pathways, and slips and trips on WLBC owned land

Operational risks - Arising from the need to effectively deliver services which meet the needs and expectations of customers and residents.

Examples of issues to look out for in local government:

- Is service delivery effective?
- Do residents, taxpayers, businesses and partners receive the services they require when they need them? Are expectations being managed?
- Extent and nature of consultation with / involvement of community, e.g. community groups, local businesses, focus groups, resident's panels, etc.

Environmental risks - Arising from inherent issues concerned with the physical environment.

Examples of issues to look out for in local government:

- Nature of environment
- Waste disposal and recycling issues
- Pollution issues, e.g. fly tipping,
- Extreme weather conditions, e.g. flooding, storms etc.

Physical risks to Systems & Assets - Arising from physical hazards associated with systems, property, vehicles, plant and equipment.

Examples of issues to look out for in local government:

- Nature and condition of assets e.g. buildings and other property owned, dilapidation of leased property
- Testing of systems to ensure efficiency

Political risks - Arising from the political situation.

Examples of issues to look out for in local government:

- Political make-up (majority party, hung council, key opposition parties)
- Decision-making structure (cabinet with leader, council and council manager, traditional committee structure)
- Leadership issues (lack of strong leadership, concentration of power into the hands of a few, imbalance of power)
- Election cycles (power shifts, undue influence on electioneering)
- Central Government initiatives impacting on Local Government

Partnership / Contractual risks - Arising from the nature of the partnerships and contracts.

This looks at the particular risks which are faced when delivering services in conjunction with potential partners, e.g. contractual terms and conditions.

The types of risks that can arise are around service delivery, investment of time, money and expertise, meeting organisational objectives, fair procurement, risk of financial and reputational risk.

It is necessary to ensure that corporate governance arrangements are robust; particularly in terms of ensuring effective performance management and that liability and accountability frameworks are explicitly agreed in advance.

Examples of issues to look out for in local government:

- Key strategic partners - from public, private and third sectors, and County strategic partnerships
- Joint ventures
- Outsourced services

11.2 Risk Analysis

This is the process of reviewing the risks identified so that similar risks can be grouped and classified according to the likelihood of them occurring and the impact they could have.

Measures of Likelihood

Score	Descriptors
Certain	Almost certain, is expected to occur in most circumstances. Greater than 80% chance.
Probable	Likely, will probably occur in most circumstances. 50% - 80% chance.
Possible	Possible, might occur at some time. 20% - 50% chance.
Unlikely	Unlikely, but could occur at some time. Less than a 20% chance.

Measures of Impact

Score	What is the worst that could happen?
Low	Minor loss, delay, inconvenience or interruption, very minor damage to reputation and very minor health & safety issues. Opportunity to innovate/make minor improvements to performance missed/wasted. Short to medium term effect.
Medium	Waste of time and resources. Good opportunity to innovate/improve performance missed/wasted. Moderate impact on operational efficiency, output and quality. Minor health & safety risk, short term damage to reputation. Medium term effect which may be expensive to recover from.
Significant	Major impact on costs and objectives. Substantial opportunity to innovate/improve performance missed/wasted. Significant impact on output and/or quality. Significant damage to reputation and moderate health & safety consequences. Medium to long term effect and expensive to recover from.
High	Severe / Critical impact on the achievement of objectives and overall performance. Critical opportunity to innovate/improve

	performance missed/wasted. Huge impact on costs and/or sustained damage to reputation. Major health & safety issues. Very difficult to recover from and possibly requiring a long term recovery period.

The descriptions are applied as follows:

The first time that a risk is assessed the likelihood and impact of the risk against the Council's risk classification categories will need to be considered as if no controls exist; this will give the inherent risk.

You can then take the next step of considering the likelihood and impact of the risk based on an evaluation of the effectiveness of existing controls to give the residual risk i.e. the current risk. This step is then repeated for all future assessments.

There will need to be consideration of what the target risk is. This is the level of risk that you are aiming to manage the risk down to, over time. This will need to be considered at each future assessment.

Risks must be assessed against each appropriate category.

The table below gives examples of how the **impact** score can be determined for each category.

Risk Type/ Category	Low	Medium	Significant	High
Reputational	Single adverse article in local media or specific professional journal that is not recirculated (e.g.: through social media). WLBC may be one of a number of agencies referred to.	A number of adverse articles in regional media mentioning WLBC. Some circulation via social media. Single request for senior officer / Member to be interviewed on local TV or radio. Adverse reaction by West Lancs residents in social media / online forums. Short term reduction in public confidence.	Series of front page / news headlines in regional or national media. Wider recirculation via social media. Sustained adverse reaction by West Lancs residents in social media. Repeated requests for senior officer / Member to be interviewed on local TV or radio. Long term reduction in public confidence	Sustained adverse publicity in regional media and / or national media coverage. Extensive / prolonged recirculation via social media channels. Repeated requests for Leader / Chief Operating Officer to be interviewed on national TV or radio. Possible resignation of senior officers and or elected members. Total loss of public confidence.
Legislative / Regulatory / Compliance	Failure to meet internal standards.	Minor breach of statutory legislation / regulation. Breach of best practice requirements.	Single breach in statutory duty. Challenging external recommendations / improvement notice.	Several breaches in statutory duty. Enforcement action and improvement notices. Critical report. Censure by regulator; breach of legal or contractual obligation.
Financial	Impact on in year budget pressures to be resolved within Service.	On-going financial pressures which require corporate resolution and should be addressed through the budget setting process.	Significant financial pressures leading to alternative approaches to service delivery.	Inability to continue as a going concern and leading to potential external intervention.
People	Short term low staffing level that temporarily	Medium term low level / insufficient experienced staff to	Late delivery of key objective / service due to lack of experienced	None delivery of key objective / service due to lack of experienced staff.

	reduces service quality. Some minor staff dissatisfaction	deliver quality service. Low staff morale.	staff. Very low staff morale.	
Risk Type/ Category	**Low**	**Medium**	**Significant**	**High**
Health & Safety	Minor injury requiring no first aid treatment or medication.	Short lived / minor injury or illness that may require first aid or medication. No overnight hospitalisation.	Injury that requires short term hospitalisation. Small number of work days lost.	Injury that requires medium to long term hospitalisation. Fatalities and / or incidences of permanent disability or ill health. Risk of prosecution from enforcement agencies.
Operational	Some short term disruption to a non-critical service to citizens / customers. No significant effect on customer satisfaction. Low chance of fraudulent activity occurring.	Short term disruption to a critical service or prolonged disruption to a non-critical service. Noticeable to customers and affecting their satisfaction with the service provided. Medium chance of fraudulent activity occurring.	Sustained disruption to a critical service or more than one non critical service. Circumstances defined in the Business Continuity Plan as requiring notification of the Emergency Planning Officer. Customer satisfaction seriously affected. High chance of fraudulent activity occurring.	Inability to perform critical services. Events leading to Central Government intervention in running of a WLBC Service. Very High chance of fraudulent activity occurring.
Environmental	Superficial impact on environment with cosmetic remediation.	Environmental damage with short term remediation. Less than 3 months.	Environmental damage with medium term remediation.	Major environmental damage, reversible with long-term remediation.
Physical Systems & Assets	Minor property, asset or facilities damage and minor disruption to systems.	Significant but temporary damage or disruption to assets, property, facilities or systems.	Sustained damage to property, assets, facilities or systems. Repair or replacements lasting more than 1 month.	Long term or permeant loss or disruption to critical property, assets, facilities and systems.
Political	Minor disruption to service provision which leads to need to notify political members for awareness.	Moderate disruption to service provision and / or objective delivery, leading to regular involvement of political member responsible for the Service.	Major impact on costs and objectives of service delivery, leading to regular review by Members Committee and constant updates to Lead Member for the Service	Critical disruption to delivery of objectives leading to resignation of political members elected position within the Council leading to elections process, delay in achievement of objectives whilst vacant roles filled.

All risk categories must be considered but there will be few, perhaps no, risks you identify that will have a quantifiable impact across all categories. You need only consider against those categories where the risk may impact.

Carrying out risk assessments using agreed risk classification categories will allow us to identify accumulations and interdependencies of risk.

To determine the likelihood, you could:

- look at past records
- consider personal relevant experience (and intuition)
- look at industry-relevant experience of the risk

- consult published literature on the risk
- do some testing or experiments (for example, market research)
- use economic or statistical models to make forecasts
- use experts in the area of that risk to make judgements.

11.3 Risk Evaluation

The Councils full risk appetite statement is set out in pages 8-10 of the Risk Management Policy and summarised in the following chart.

Risk Type	Risk Appetite
Reputational	3
Legislative / Regulatory / Compliance	2
Financial	3
People	3
Health & Safety	1
Operational	2
Environmental	3
Physical Systems & Assets	3
Political	2

Key

Ratings	Risk Appetite	Meanings
1	Low	Residual risk only acceptable in extreme situations (e.g. where the risk has a very low impact and likelihood)
2	Medium	Residual risk is managed down on a cost-benefit basis. A medium amount of risk is acceptable however, on balance, control is weighted higher than acceptance.
3	Significant	Residual risk is accepted to significant levels. Significant implies a pure cost-benefit approach.
4	High	Residual risk is accepted to high levels

Once the inherent risks have been classified they need to be mapped onto the matrix as shown in the example below. The colours are a “traffic light” system that denotes the risk appetite of the Council.

The mapping will need to be repeated to record the current risk too as this will show how controls in place have influenced the level of risks e.g. the inherent risk could place a risk within the red zone as a critical risk, but because controls in place are evaluated as being effective and consistently applied the current risk could fall within the green (comfortable) zone. The mapping should then be repeated to record the target risk to provide a view of how much further it is aimed to reduce the level of risk to.

It is important to keep in mind that we are more concerned with whether the current risk is within our risk appetite than how it scores. What really matters is that we can clearly identify what else we need to do to reduce the risk so that it falls within our accepted risk appetite level. Ask yourself is the current risk tolerable?

You will need to assess the likelihood and impact for each appropriate category and then plot the score in terms of likelihood and impact.

If for example you have a risk with a potential high environmental risk, but only a low financial impact this does not mean that Penatna will average the overall impact to medium. There can be no trade-off of impacts. The Council has decided that each of the risk impact categories is individually scored independently of how they affect others. For example, a high reputational impact is not made more acceptable by the Council not having suffered a financial loss to get to that point. Your impact score will be equivalent to the highest score you have assessed in any single domain, which will then also act as a guide to where you may best focus your risk treatment (see Section 11.4).

WLBC Impact / Likelihood Matrix

		Impact			
		Low	**Medium**	**Significant**	**High**
Likelihood	**Certain**	**4**	**8**	**12**	**16**
	Probable	**3**	**6**	**9**	**12**
	Possible	**2**	**4**	**6**	**8**
	Unlikely	**1**	**2**	**3**	**4**

Level of Concern	Action Required
Critical	Urgent attention required at highest level to ensure risk is reduced to an acceptable level. Action planning should start without delay. Progress on actions should be reported to the Chief Operating Officer and / or the Leader.
Concerned	Requires mitigation and a contingency plan. Report on progress to CMT.
Cautious	Acceptable level of risk however the risk requires mitigation /consideration. Reviewed at Head of Service level.
Comfortable	Acceptable level of risk. Keep under review but no action required unless changes occur.

11.4 Risk Treatment & Management

This aspect of the process involves:

- Setting the risk appetite. CMT and Members make a decision on the degree to which risks are acceptable. This can vary from risk aversion through to risk taking, and will depend upon the nature of the service. The result of this is to set the level at which

risks can be tolerated and therefore accepted. The Council's risk appetite is shown on the risk matrix by the identification of which risks are comfortable (green zone), cautious (yellow zone), concerned (orange zone), and critical (red zone). The Council's Risk Appetite Statement is a set out on pages 8-10 of the Risk Management Policy and should be considered before carrying out your risk assessment.

- Assessing whether to accept (tolerate), control (treat), transfer (share), or terminate the risk, or how to respond to the opportunity, based on the availability of resources;
- Documenting the reasons for the decision taken;
- Implementing the decision;
- Assigning ownership to manage the risks / opportunities and controls to specific officers

Controls are the tools that managers use to manage their departments. They are the methods used by managers to assure them that they are achieving their business aims, meeting service objectives and delivering the outcomes required, and that the service is being provided in the most efficient and effective way. The cost and robustness of existing or additional controls is a key consideration at this point and needs to be balanced against the potential consequences (reputational, financial or otherwise) if the event occurred. The cost of implementing and operating a control should not normally exceed the maximum potential benefit.

Approaches to treating risks

Tolerating risks means that you intend to manage the risk within your existing management routines. Risks should only be accepted where officers believe that the current risk is tolerable i.e. the risk falls within the green (comfortable) or yellow (cautious) category of the matrix.

Risks may also have to be tolerated where there is no option but to tolerate a risk associated with delivering an essential public service. In this case it is recommended that a contingency plan is put in place to deal with the risk should it occur.

Treating risk means that you identify additional action(s) to be taken that will reduce the likelihood and / or impact if the event occurs. Controls can be:

- **Preventative** which are designed to limit the possibility of an undesirable outcome being realised. Examples include, physically restricting access to hazardous chemicals, insisting on two signatories, ensuring segregation of duties exist within a system, implementing authorisation limits, or restricting levels of access on IT systems. These controls will help reduce risk levels from the outset.

- **Corrective** which are designed to limit the scope for loss and reduce any undesirable outcomes that have been realised. They may also provide a route of recourse to achieve some recovery against loss or damage. Examples include barriers should hazardous chemicals escape, rotation of staff, passwords and other access controls.

- **Directive** which are designed to ensure that a particular outcome is achieved. They are based on giving directions to people on how to ensure that losses do not occur. Examples include procedure manuals, guidance notes, instructions and training. Such controls advise on how to carry out processes safely but if they are not adhered to they will not prevent risk events occurring. Insurance and contracts are also examples of directive controls.

- **Detective** which are designed to identify occasions when undesirable outcomes have been realised. Their effect is, by definition, 'after the event' so they are only appropriate when it is possible to accept that the loss or damage has occurred. Examples include health monitoring and screening, audit reviews and reconciliations.

Transferring risk means using an insurer or other third party to cover all or part of the cost or losses should a risk materialise. However, care needs to be taken to accurately specify the risks to be covered. Making arrangements with others such as joint working, partnerships or contracting out to provide services could also be used to transfer/ share risks. However, other risks can arise from these arrangements and the responsibility of providing the service could remain with the Council. When transferring or sharing risks with other parties, ensure that risk registers detail where liability and accountability lies between parties.

Terminating risk means ceasing to carry out the activity because modifying it or controlling it would not reduce the risk to an acceptable level.

It may be however be impossible to terminate some risks i.e. the delivery of essential public services. In this case the action you need to take is to ensure that we have a contingency plan in place so that should the risk occur we can deal effectively with the consequences. See section 14 below for information on business continuity management.

11.5 Reporting and Recording

It is imperative that risks are recorded on the appropriate risk registers on the Pentana Risk System, the Council's corporate risk management software. Risks must continue to be regularly monitored and actively managed until they are realised.

Every risk should be assigned to a risk owner who is identified on the risk register. The risk owner (the officer named in the "assigned to" category) is the designated member of staff who carries the ultimate responsibility for agreeing and delivering the action plan to control the risk and for monitoring progress against it.

It is the responsibility of the risk owner to ensure that their risk is on Pentana, that it is kept updated and that the risk is escalated through the appropriate channels when necessary. It is also their responsibility to make sure that their risk is linked to their service action plan and performance indicators if appropriate.

Controls must be allocated to a control owner to enable us to identity the responsibility for a control.

The Council's risk register has several key elements to it and officers are expected to record those elements detailed below on their service risk register.

Please see flowchart for permissions required to add a risk to Service and Corporate Risk Registers at Section 12.

Risk identification phase

1) Code & Title

Code: This is a unique identification number used to identify and track the risk in the risk register e.g. Insurance Risks have the prefix INS, then the first risk identified in this category has a unique ID of 01. Create an appropriate code for your risk.

Title: A brief description of the potential risk. For instance, “Failure to produce the annual statement of accounts on time and to a high standard.”

2) Risk Ownerships

Ensure that all ownerships in the section are assigned.

Assigned to - Assign the risk to the risk owner, i.e. the officer who has day to day responsibility for managing the risk. The risk is the responsibly of the assigned officer. They are the Risk Owner.

Managed by **-** The person ultimately responsible for managing the risk, agreeing and delivering the action plan to control the risk and monitor progress against it.

Risk Champion – Allocate to the Risk Management Champion for your area. A list of Risk Champions are available on the risk management page of the intranet.

3) Assignment of a risk to a risk category

Corporate Risks should be allocated to the Corporate Risk Register by assigning them to category "CORP Corporate Risks". You should discuss the risk with your Head of Service to ensure that they agree with allocating the risk to the Corporate Risk Register. (See Section 12)

The Corporate Risk Register records significant risks that are likely to affect more than one service. It also records major corporate and directorate initiatives, procurement or projects. It is a key part of the corporate planning process. It includes, for example:

• Major safety risks that could result in fatalities to residents/stakeholders or staff

• Major financial risks

• Risks that could prevent the Council from meeting its strategic objectives

• Major risks to the Council’s reputation

• Risks relating to overriding issues of corporate concern.

Project Risks should be assigned to a specific project risk register.

If you require a new risk category to be set up then please contact the Risk and Insurance Officer

Risk analysis phase

4) Potential effect

Refers to any effect associated with an action that is possible, in certain circumstances. The effect may refer to a threat or damage that may be caused to or by the Council e.g. bad publicity, loss of income, negative effect on local residents/stakeholders and staff.

It may also refer to the potential opportunities that the risk may create e.g. jobs, facilities for local residents, income generation, opportunities for staff development.

5) Internal Controls

Controls are activities designed to prevent, reduce or eliminate the risk from occurring (see section 11.4).

Detail the controls that are in place to reduce the inherent risk score to the current risk score and detail who the controls are assigned to.

Record the further controls that are required to reach the target risk and detail who the controls will be assigned to.

Individual controls should be scored as not effective, partially effective or fully effective. Enter a description to detail more information about the specific control and a note to explain why the internal control has been scored at its current level of effectiveness. Record where the evidence that the controls are operating effectively can be found.

As actions are taken to move a control from not effective to partially or fully effective, remember to refresh the control detail.

6) Latest Note

Detail briefly the current position of the risk e.g. has a report gone to Cabinet / Council, is a periodic review about to take place, has a project manager been appointed, is the risk being audited.

Risk Evaluation Phase

7) Current Risk Review Date

The date that you reviewed the risk. Even if no change is required to the risk this date should be updated so that those looking at the register can see that the risk has recently been considered and remains unchanged.

8) Inherent Risk Matrix

Consider the Council's risk matrix and where the inherent risk sits in relation to likelihood and impact of all categories then plot the score.

9) Current Risk Matrix

Consider the Council's risk matrix and where the residual risk i.e. the current risk sits in relation to likelihood and impact of all categories then plot the score. The score should illustrate how the risk scored at the time of the review.

10) Target Risk Matrix

What we can do further to reduce the risk down to an acceptable level. Use the Council's risk assessment to calculate the likelihood and impact score.

11) Service Action Plans & Performance Indicators

Once risks have been updated on Pentana consider whether your Service Action Plan needs to be amended to take account of the work that still needs to be carried out to bring the risk down to an acceptable level. The aim is to shift the risk from critical to comfortable in the prioritisation matrix; at a reasonable cost. Action plans and risks can be linked on the Pentana system and it is recommended that where appropriate, or where the risk is a Corporate Risk that it is linked to an action and vice versa.

Performance indicators can assist in providing feedback for the risk management process. This has the advantage of helping to prioritise actions. Linking risk management to performance indicators assists in ensuring risk management is embedded in the Council. Performance indicators that fall short of expectations or target can indicate the effect of risk events or slowly operating control failures.

11.6 Monitor and Review.

It is necessary to monitor the risks, controls and any documented actions and to regularly report on the progress being made in managing risks, or taking advantage of opportunities, so that the achievement of the Council's aims and objectives is maximised and losses are minimised.

In addition there needs to be an assessment of the effectiveness of risk management actions put in place to reduce the likelihood / impact of adverse risk events occurring. Alternative action will need to be taken if the initial action has proved ineffective.

Reviewing risk registers to ensure they remain up-to-date and relevant should also be done as;

- Previously identified risks will change over time; some may become less of a hazard, for example once all the affected staff have been trained. Others may become more likely if a key milestone is approaching, such as the end of a funding stream.

- It may become necessary to escalate a risk if the situation has changed or the initial assessment has proven to be inaccurate. Conversely it may be possible to downgrade a risk.

- New risks identified or opportunities arising will need to be added.

- It may be appropriate to deactivate risks.

- Monitoring progress and reviewing the risk registers should take place on at least a quarterly basis, and more frequently if there are many changes or the project is progressing rapidly.

Documenting the review of the risk register, service action plans and performance indicators is also necessary, but need not be onerous. The fact that the review has been carried out should be recorded on Pentana along with a note of any changes made. The Corporate Risk Matrix provides a mechanism for escalating risks or highlighting changes that more senior management needs to be aware of.

Deactivation of Risks (See flowchart at Section 13)

When a risk is realised it may be deactivated from the Pentana system however risks should never be deleted so that an audit trail of the management of the risk exists.

It is important that risks are not deactivated until we are satisfied that the risk no longer presents.

Before risks are deactivated from Service Risk Registers the risk owner must obtain their line mangers permission to deactivate the risk. Text should be entered into the notes section advising who deactivated the risk, who approved the risk for deactivation and the reason(s) why the risk was deactivated.

Before risks are deactivated from the Corporate Risk Register the risk owner must obtain permission from their Head of Service to deactivate the risk. Risk owners must also make the Risk and Insurance Officer aware that the risk is being deactivated so that this can be reported to the appropriate Cabinet & Committees. Text should be entered into the notes section advising who deactivated the risk, who approved the risk for deactivation and the reason why the risk was deactivated.

It is recommended that risks and risk management are standard agenda items at quarterly DMT meetings.

Although the exact process used will differ between management teams, the following is an example of how officers may wish to approach the review:

1. Go through the risks listed in the register to consider whether each risk is:

a. Still valid.
b. If the situation has changed in the interim period regarding the mitigating actions / controls you have in place or if it stays the same.
c. Record in the internal controls any details of further mitigating actions that are being carried out now.
d. Update the latest notes, what has changed since the last review
e. Use the likelihood and impact definitions to determine the amended current risk
f. Update the Service Action Plan and Performance Indicators accordingly.
f. Escalate the risk, if in the light of the review it is more serious than was first thought and requires more senior management action.
h. Decide if any risks should be deactivated, and if so minute the reason for the decision in the notes section.

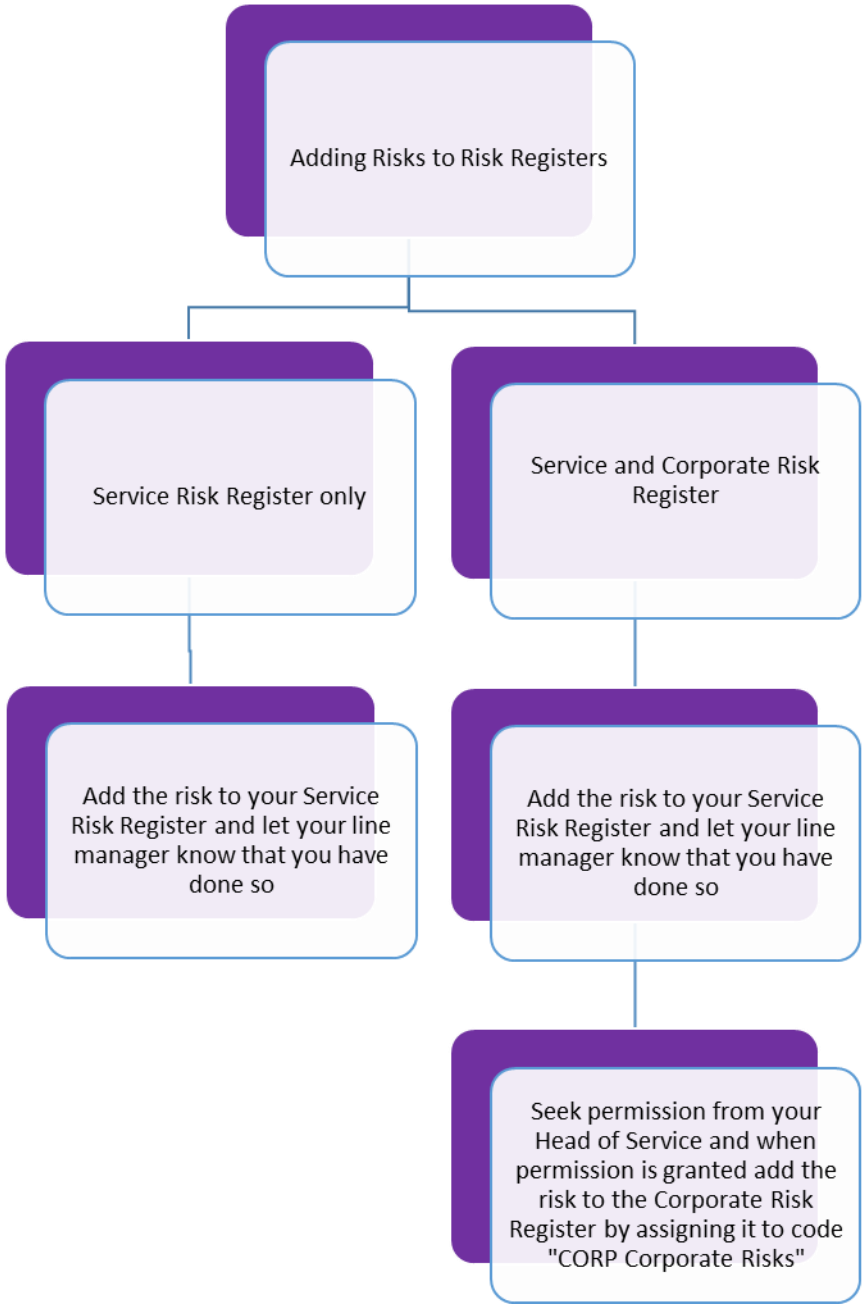
2. Identify if any new risks have arisen, for example:

a. From an adverse event occurring.
b. By something new happening, e.g. a new partner organisation to work with, a new project starting, new / different way of delivering services.
c. As a result of an ongoing management review, e.g. unexpected demand for a service, etc.
d. From changes in legislation or other external factors.

3. Use the likelihood and impact definitions to determine the inherent and current risk associated to any new risks, and capture the mitigating actions / controls currently in place.

4. Determine whether any risks on the Service Risk Register should be added to or removed from the Corporate Risk Register.

12. Flowchart Procedure for Adding Risks to Risk Registers



13. Flowchart Procedure for Removing Risks from Risk Registers

14. Business Planning & Budget Setting

One of the keys to successfully embedding risk management is ensuring that it is explicitly linked to business planning. In a properly embedded process, remedial action should take place to mitigate those risks which managers believe are insufficiently controlled, i.e. where the current risk exceeds the Council's risk appetite. The link to business planning is a development of the discussion in section 11.4. Managing under-controlled risks can require changes to the way services are delivered or structured, and this may require the allocation of additional resources.

Effective management of risks can only be achieved through the effective management of resources. Where control weaknesses are identified which create an unacceptable exposure to risk, resources should be allocated to 'plugging the gap'. This can take a variety of forms, depending upon the nature of the risk, the existing controls, and impact of the exposure.

Those controls currently in place may require strengthening, or new ones may need introducing. For example, it could be that an ICT solution is required to improve efficiency or enable additional monitoring; or possibly the feasibility of the service being provided by a partner instead of directly by the Council. These examples have a cost, some of which may be financial, some of which may have an opportunity cost. As a result, it is important that managers retain flexibility in their service and financial planning to enable developing risks to be managed. Of course the converse may also apply; the risk process could identify risks which are over-controlled. Savings may be achieved by reducing the control environment, saving money and / or enabling the re-direction of staff to other areas to improve service delivery.

The risk register and service action plan should be used to record these responses. The agreed actions can be logged on both documents, with more detail added on the action plan. This could also include a discussion of where the resources to fund the strengthening will come from. The result will be a concise analysis of the nature of the risk exposure, the response to the problem and the financing of the solution. Where budget variances occur as a result of the additional expenditure, a concise and robust explanation should be available to support this.

It is important to use the knowledge we have acquired through management of our risks to inform and shape our future actions. Action plans should be updated with the results of risk assessments which have been previously undertaken. Risk management should not be viewed in isolation, but should be used as an important tool in informing the business planning process. What we learn now should help us identify what we will do in the future, how we will achieve it, and the problems we may encounter. This will ensure that the risks and mitigations already identified are considered and included in subsequent action and business continuity plans. The benefit will be that business and service action plans are as relevant and accurate as possible, and contribute effectively to the achievement of objectives and the delivery of the outcomes and services required.

13. Annual Report & Annual Governance Statement

There is an Annual Report & Annual Governance Statement (which includes a statement on internal control) signed off by the Leader of the Council and the Chief Operating Officer. These are published by July following the financial year end. The Annual Governance Statement is included within the Council's Financial Accounts.

Directors and Service Heads are specifically asked about risk management within the assurance statements they complete which provide supporting evidence for the Annual Governance Statement. Using risk management will also assist Directors in completing other aspects of their directorate assurance statements.

Although the arrangements for preparing the directorate assurance statements are well established, it is imperative that the process continues to be driven down the organisation.

It is important that we encourage and where necessary demand the wider use of statements across directorates, to assist in demonstrating compliance and accountability.

14. Training

The Council acknowledges that risk management training for staff is crucial to the effectives of embedding Risk Management. It strives to ensure that all employees have a basic understanding of risk management and how the Council's Risk Management Framework operates.

Employees undertake risk management training as part of the induction process. Two presentations are available, one for Senior Management and Risk Coordinators and one for all staff. New employees should watch the appropriate presentation. If appropriate they should also watch the presentation on how to use the Pentana Risk System. These presentations may also be watched by any member of staff who requires refresher training.

Training for Officers will be arranged and provided annually by the Council's Risk and Insurance Officer. Such training may be outsourced or provided in house.

Training for Members will be arranged and provided every two years by the Council's Risk and Insurance Officer. Such training may be outsourced or provided in house.

Please contact the Risk and Insurance Officer if any risk management training needs are identified within your department and training will be arranged.

15. Useful Contact Points / Information

Head of Finance, Procurement and Commercial Property
James Pierce

Finance & Audit Manager
Mike Kostrzewski

Risk and Insurance Officer
Rebecca Spicer

Internal Audit
Jacqui Pendleton – Internal Audit Manager
Melanie Moorey – Internal Auditor
Kath Westby – Internal Auditor
Jo Guest – Internal Auditor

Emergency Planning Officer
Jenny Jones

Partnership & Performance Officer
Alison Grimes

16. Definitions

Assurance

A positive declaration, given by a Director, that the risks within their service area are being managed effectively.

Control Owner

A control owner is accountable for implementing and maintaining the effectiveness of specific controls as recorded in a risk register, in a position description or in organisational policies and procedures. Control owners may also be responsible for designing or modifying controls to improve their effectiveness.

Corporate Risk Register

This records significant risks that are likely to affect more than one service. It also records major corporate and directorate initiatives, procurement or projects.

Cost

Of activities, direct and indirect, involving any negative impact, including money, time, labour, disruption, goodwill, and political and intangible losses.

Cross Cutting Issues

Topics that affect all aspects of a programme (i.e. cut across) and therefore need special attention. They should be integrated into all stages of programmes, plans and projects

Event

An incident or situation, which occurs in a particular place, during a particular interval in time.

Hazard

A source of potential harm or a situation with a potential to cause loss.

Impact

The probable effect on the Council if the risk occurs or the opportunity is not taken.

Inherent Risk

The likelihood and impact of the risk if no action is taken or existing actions cease.

Likelihood

How often a risk is expected to materialise

Loss

Any negative consequences, financial or otherwise.

Management Assurance

The opinion given by managers, based on evidence they have obtained from reviewing and improving the controls in place, regarding the adequacy of the management of risks and the achievement of service objectives within their area of responsibility.

Monitor

To check, supervise, observe critically, or record the progress of an activity, action or system on a regular basis in order to identify change.

Objective

A fundamental service delivery aim.

Organisation i.e. Council or Partner

A company, firm, enterprise or association, or other legal entity or part thereof, whether incorporated or not, public or private, that has its own function(s) and administration.

Residual Risk

The remaining level of risk after effective mitigating action has been taken to manage the likelihood and or impact of the risk. Often referred to as the current risk.

Risk

An event / series of events happening or action(s) taken that will prevent the Council from achieving its planned objectives, in part or in full. A risk can also be the failure to take advantage of opportunities to optimise the Council achieving its planned objectives.

Risk Acceptance

An informed decision is taken to accept the impact and the likelihood of a particular risk.

Risk Analysis

A systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.

Risk Appetite

The amount of risk that the Council is prepared to accept, tolerate or be exposed to - see the Council's Risk Appetite Statement.

Risk Assessment

The overall process of risk analysis and risk evaluation.

Risk Avoidance

An informed decision not to become involved in a risk situation.

Risk Capacity

The capability of the organisation to take risk.

Risk Control

That part of risk management that involves the implementation of policies, standards, procedures and physical changes to eliminate or minimise negative risk.

Risk Exposure

How much is actually at risk

Risk Evaluation

A decision point in which we decide whether to respond or not to respond to the risk.

Risk Financing

The methods applied to fund risk treatment and the financial consequences of risk.

Risk Matrix

Risk matrix is a means of summarising risk profile.

Terminate

Terminating a risk means ceasing to carry out the activity.

Tolerate

Tolerating a risk means managing the risk within existing management routines.

Transfer

Transferring a risk means using an insurer or third party to cover the cost or losses should a risk materialise.

Treat

Treating a risk means that you identify additional action(s) to be taken that will reduce the likelihood and / or impact if the event occurred.

Virement

Movement of funds between budget codes within the financial year.

Appendix A

Risk Architecture - Roles & Responsibilities & Reporting Lines

The roles and responsibilities of individuals and groups to implement the framework and processes are as follows:

- Cabinet Members - work with CMT, Directors and Heads of Service to provide information regarding the management of corporate risks and opportunities. Cabinet Members are also involved with risk management within service provision in the directorates as per their portfolio.

- Members - involved via Regulatory Committees, the Overview and Scrutiny process and through other Committees. Also involved in other roles such as their membership of project boards.

- Audit & Governance Committee - to support the Council's Corporate Governance responsibilities and to provide independent assurance in relation to internal control, risk management and governance.

- Corporate Management Team (CMT) - scans for new risks to the Council and the region of West Lancashire. Gives a view of the medium to long term risks to the region, including assumptions in respect of government policy, financing, business transformation and partnership working. CMT ensures that the people, policies and resources of the Council are utilised efficiently and effectively so that the priorities and strategic outcomes of the Council are delivered. CMT have the draft Corporate Risk Register updates reported to them before they go to Executive Overview & Scrutiny and Cabinet. CMT are able to challenge the update information provided by directors, and recommend re-wording or deletion of risks as appropriate.

- Chief Operating Officer - leads on the wider corporate governance agenda of which risk management is a part. Receives assurance statements on internal control from Directors and is one of the signatories to the Annual Governance Statement.

- Directors and Heads of Service - integral to the risk management process, providing leadership for the process. Responsible for feeding risks into the Corporate Risk register via their Service Risk Register. The risks to be identified include those arising from corporate initiatives, business change, major projects, cross-cutting issues, the external environment, including legislative changes, partnership working and from assessing the wider implications of their directorate's service provision. There is a particular duty for the Directors and Heads of Service to reduce the impact of high risks that are likely to occur. They also need to make arrangements for embedding risk management throughout their Directorate and Service, which will assist them in providing assurance to the Chief Operating Officer each year.

- Service Management Teams - carry out service risk assessment as part of service action planning and internal / external reviews e.g. External Audit inspections and reviews, Health & Safety Inspectorate etc., and taking account of corporate risks. Have responsibility to put in place actions to take advantage of opportunities / reduce risks and to Monitor and review the effectiveness of the actions.

- Risk Management Champions - nominated by each service to assist in embedding risk management. They are a point of contact to disseminate the information from the Risk Management Working Group to their teams.

- Risk Management Working Group (RMWG) - comprised of service Risk Management Champions, responsible for assisting in maintaining and developing the Risk Management Framework.

- Internal Audit - The internal audit team may review and report on the directorate and corporate risk management processes and the wider corporate governance agenda. Issues guidance and information.

- Risk Owner – the officer "assigned to" the risk. They are responsible for the risk, updating Pentana and escalating the risk when appropriate.

- Control Owner - Responsible for ensuring that the control functions effectively and for letting the risk owner know if it appears that the control is starting to function less effectively.

- Risk & Insurance Officer- facilitates and advises on the corporate risk management process. Develops, in conjunction with colleagues, practical approaches for implementing risk management, sources and provided risk management training. Ensures the timely purchase of adequate insurance for the transfer of risk, where appropriate.

- All staff - have a responsibility for identifying opportunities as well as hazards / risks in performing their day to day duties and taking appropriate action to take advantage of opportunities or limit the likelihood and impact of risks. This includes making their manager aware of opportunities or hazards / risks identified.

Appendix B – Risk Management Work Plan

Risk Management Cycle Work Plan 2021 -2022

	Risk Management Policy (including Strategy & Risk Appetite Statement) & Toolkit	*Service Action Planning*	*"Real Time" Review of Service Risk Registers by Heads of Service*	*Risk Monitoring by CMT*	*Cabinet Report / Update*	*Executive Overview & Scrutiny*	*Training*	**Risk Management Working Group Meetings**
April		SAPs agreed and implemented		Risk Reporting to CMT			*Training for Members & Officers	
May								
June			Service Registers reviewed					RMWG Meeting
July				Risk Reporting to CMT (approval prior to Cabinet & Exec O&S)				
August								
September			Service Registers reviewed		Risk Register reported to Cabinet	Risk Register reported to Executive O&S		
October	Reviewed and updated if required			Risk Reporting to CMT				
November		SAP guidance issued						
December			Service Registers reviewed					RMWG Meeting
January	Endorsed by CMT, Reported to Audit & Governance and Executive Overview & Scrutiny			Risk Reporting to CMT (approval prior to Cabinet & Exec O&S)				
February								
March	Approval by Cabinet if required	Proposed SAPs finalised	Service Registers reviewed		Risk Register reported to Cabinet	Risk Register reported to Executive O&S	Review & Update On Line Training Sessions	

* Training for staff is provided annually and Members provided every two years

Appendix C

Terms of reference of the Audit & Governance Committee

Functions

Audit Activity

1. To consider and approve the Internal Audit Charter.
2. To consider the Audit Manager's Annual Report and Opinion.
3. To consider reports dealing with summaries of Internal Audit Activity.
4. Where requested by the Audit Manager, to consider issues arising from specific internal audit reports.
5. To consider reports from the Audit Manager on agreed recommendations not implemented within a reasonable timescale.
6. To require the attendance at meetings of the Audit and Governance Committee, of any elected Member or Officer of the Authority in relation to internal audit reports.
7. To consider the external auditor's Annual Letter and other reports as requested by the external auditor.
8. To scrutinise Treasury Management activities.

Regulatory Framework

9. To monitor Contract Procedure Rules, Financial Regulations and other provisions of the Constitution in so far as they contribute to the effectiveness of the Council's internal controls.
10. To comment on the scope and depth of external audit work and to ensure it gives value for money.
11. To consider any issue relevant to its responsibilities and functions referred to it by the Council, Cabinet, and any committee of these bodies, the Chief Executive or Chief Officers.
12. To monitor the effectiveness of risk management and corporate governance processes in the Council.
13. To monitor the effectiveness of the Councils policies in relation to its Anti-fraud and Corruption Strategy and complaints process.
14. To review the production of the Authority's Annual Governance Statement.
15. To approve the Authority's Annual Governance Statement and commend it's signing to the Leader and Chief Executive.
16. To consider the Council's arrangements for corporate governance and in particular in relation to the Local Code of Corporate Governance and recommend actions to promote best practice.
17. To consider the Council's compliance with its own and other published standards and controls in so far as these contribute to the adequacy of its framework of internal control.
18. To monitor (quarterly) the use of RIPA powers.

Accounts

19. To approve the Statement of Accounts.
20. To consider The External Auditor's Report to those charged with Governance on issues arising from the audit of the accounts.
21. To review the annual statement of accounts. Specifically, to consider whether appropriate accounting policies have been followed and whether there are concerns arising from the financial statements or from the audit.

Other Delegations

- The Committee shall exercise the full powers, duties and functions of the Council as set out above in numbers 1, 14 and 18.
- The Committee will not be able to transact the powers, functions and duties reserved to Council, Cabinet, Overview and Scrutiny Committees, Standards Committee and other regulatory Committees.

Appendix D

Amendments to the Toolkit

Date	Amendment Made	Name and Title of Officer