West Lancashire Borough Council Risk Management Toolkit

Version 3 January 2023

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 can 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 averse, 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 our activities 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
West Lancashire Borough Council

Contents

Section 1:
Introduction

1.1 Guidance & toolkit

1.1.1 Purpose and use

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 averse.

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.

The risk management 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 1.2 for your guidance.

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

1.1.2 Audience

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 key risk register. Although risk owners will be tasked with updating risk registers and managing risks, risk management is the responsibility of all Council employees.

1.1.3 How to use this toolkit

Section 1 introduces the toolkit, provides some definitions, outlines the importance of risk management, discusses risk management principals and landscape, and introduces the concept of risk management maturity.

Section 2 outlines the considerations and steps that need to be taken to implement the Council's risk management framework, including:

- governance and infrastructure
- our risk management process
- integration of risk management
- risk management culture

The appendices provide additional support materials.

1.2 Definitions

Accept	A risk response that accepts the risk and its likelihood and impact if it does occur.
Avoid	A risk response that seeks to eliminate a threat by terminating the risk.
Control owner	A control owner is the individual assigned for the implementation of the measures to mitigate the risk. They support and take direction from the risk owner.
Frequency	A measure of likelihood expressed as the number of occurrences of an event in a given time.
Impact	Impact to the organisation should the risk materialise.
Inherent Risk	The exposure arising from a specific risk before any action has been taken to manage it
Key Performance Indicator (KPIs)	A measure of performance that is used to grade and monitor progress towards an objective / goal.
Key Risk Indicator (KRIs)	An early warning indicator that can be used to monitor a change in the likelihood or impact of a risk and assist in the decision-making process for risk mitigation.
Key Risk Register	Records those risks which if they occur would have the greatest impact on the Council, the achievement of its vision, priorities, and activities. They are strategic high-level Council risks.
Likelihood	A qualitative description of the probability or frequency of that risk materialising.
Maturity level	A well-defined evolutionary plateau towards achieving a mature process.
Partnerships (Third parties)	Contractual relationship between two or more persons carrying out a joint venture, each incurring liability for losses and the right to share in the outcome.
Pentana	The Council's risk management information system. It records risks, service action plans and performance indicators.
Project	A temporary organisation that is created for the purpose of delivering one or more products according to a specified business case.
RAG Analysis	'RAG Analysis' describes a process whereby complex data can be displayed in 'traffic light' or Red-Amber-Green (RAG) format.
Residual Risk	The exposure arising from a specific risk after action has been taken to manage it and assuming that the action is effective

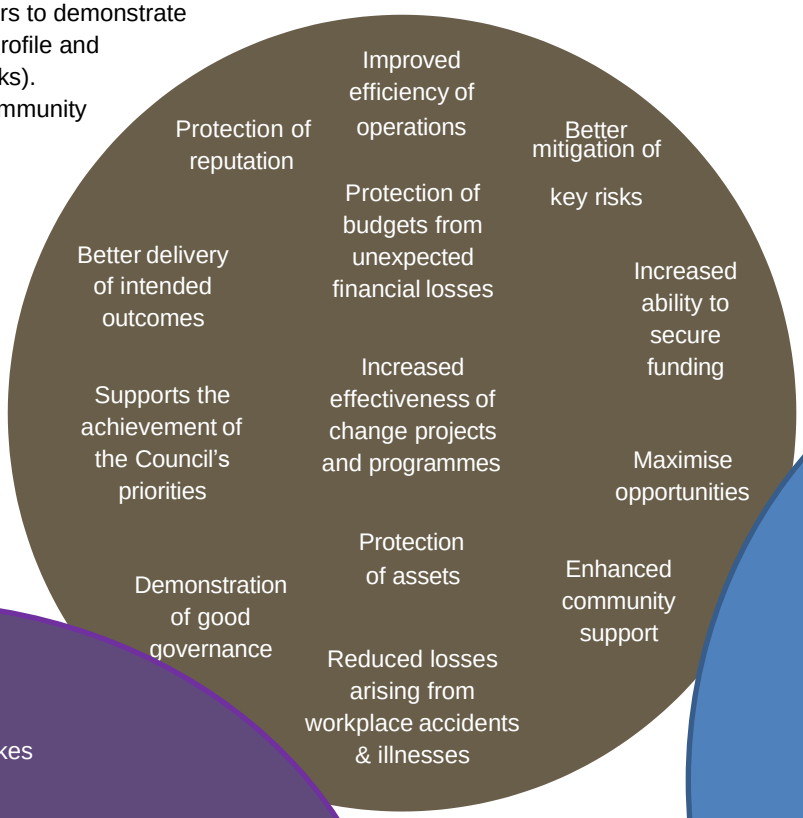
Risk	ISO 31000: Effect of uncertainty on objectives.
Risk Analysis	A systematic use of available information to determine how often specified events may occur and likelihood and impact of the risk occurring.
Risk Appetite	The amount of risk that the Council is willing to pursue or retain in pursuit of its objectives.
Risk Assessment Criteria	The terms of reference by which the significance of risk is assessed.
Risk Category	Represents a collection or group of risk types with a common denominator (e.g., strategic, operational, people, legal / regulatory, financial, reputational).
Risk Cause	A description of the source of the risk, i.e., the event or situation that gives rise to the risk.
Risk Management / Management of Risk	ISO 31000: Coordinated activities to direct and control an organisation with regards to risk. The culture, processes and structures that are directed towards the effective management of potential opportunities and threats to the organisation achieving its objectives.
Risk Map	A model that visually displays the relationship between the likelihood and impact of specific risks.
Risk Owner	A single individual who is nominated and responsible for the monitoring and updating of a risk. They are the officer "assigned to the risk".
Risk Perception	An individual's subjective view of risk, based on a set of values and / or concerns.
Risk Prioritisation	The process that allows risks to be ranked into a logical order by establishing how significant they are in terms of likelihood and impact.
Risk Register	A basic, ongoing working document that records the risk identification, assessment and sometimes action planning process. Stored on Pentana
Risk Response	Actions that may be taken to bring the risk to a level that is acceptable to the organisation. These responses fall into one of several risk response options.
Risk Universe	Consists of all the risks that potentially have an impact on an organisation at any level. The risk universe within this document has been tailored to local government.
Service Risk Register	Records operational risks which are faced in the day-to-day delivery of services. Service risks are those that could have an effect on the successful achievement of the service priorities, objectives, and activities
Stakeholder	Any individual, group or organisation that can affect, be affected by, or perceive itself to be affected by a risk.
Uncertainty	A condition where the outcome can only be estimated.

1.3 The business case

Risk management is a management tool and forms part of the governance system of every public service organisation. When applied appropriately risk management can bring the Council multiple benefits.

It can help us to achieve our vision, priorities, objectives, and better deliver on intended outcomes. It can also help managers to demonstrate good governance, better understand their risk profile and better mitigate risks (particularly uninsurable risks). Externally it can help the Council to enhance community support.

Some of the benefits that risk management can provide have been listed within the circles on this page.



These benefits make quite an impressive list.

- Are they achievable? *Yes*
- Are they guaranteed? *No*

The list is not exhaustive, and all these benefits are achievable if we all embrace our risk management responsibilities.

1.4 Principals & landscape

1.4.1 Risk management principals

The approach adopted to risk management ensures that our risk management is

1.4.2 The landscape of risk management

Public service organisations are undergoing a significant period of change and as a result new risk profiles need to be managed. Outlined below are factors contributing to this change:

- a difficult economic and financial climate
- increased pressure to develop effective partnerships with other public, private and third sector organisations to deliver outcomes and critical operations
- changing political agendas
- changing roles and responsibilities for public service organisations
- new technologies
- greater pressure for public service organisations to be creative / innovative to increase efficiencies.

Over the past few years public service organisations have been associated with large IT and infrastructure project failures, huge fines resulting from breaches of data protection and high-profile supplier failures.

Recognising the need to increase community confidence and effectively manage these new risk profiles, over recent years public service organisations have implemented a more structured approach to the management of risk.

Governance structures aim to ensure better anticipation of risk, especially across delivery partners, and focus on embedding risk management processes and creating a risk aware culture.

1.5 Risk maturity

Across all industries, sectors and organisations different levels of risk management maturity exists. Risk management maturity refers to the journey an organisation goes through when managing risk.

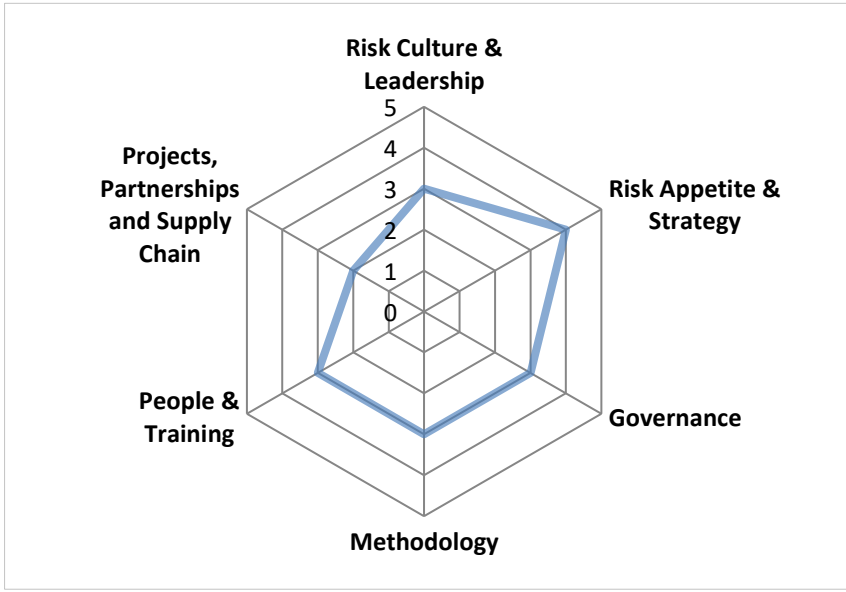
Undertaking a risk maturity assessment enables the Council to benchmark its current risk management capability and identify how and where improvements can be made.

To measure the maturity of risk management a performance model has been used which breaks down risk management activity into six categories that contribute towards effective risk management arrangements.

Risk Culture & Leadership	Exploring the attitude that Senior Officers and Members take towards the role and priority of risk management
Risk Appetite & Strategy	Reviewing the extent to which the policies for risk management support the organisation and how the appetite for risk is considered and utilised
Governance	Establishing how assurance is provided to stakeholders, the effectiveness of reporting arrangements and how risk is managed within departmental areas.
Methodology	Assessing whether effective risk processes and tools are in place to support the organisation
People & Training	Evaluating the level of risk management skills, knowledge, and capacity across the organisation
Projects, Partnerships & Supply Chain	Determining whether there are effective arrangements for managing risks within projects and with partners and suppliers

The model enables an assessment to be made around the extent to which risk management is having a positive effect on the Council. The five levels of maturity are as follows:

Level 1	Level 2	Level 3	Level 4	Level 5
Fragmented	In Development	Managed	Integrated	Transformational



The above figure indicates where West Lancashire Borough Council is judged to be based on the last external review which concluded in September 2022.

Maturity Assessment

The green highlighted section denotes where the Council scored on its last assessment in 2022. Further work in the 6 areas detailed below will ensure that the Council becomes more mature in its approach to Risk Management.

	Risk Culture & Leadership	Risk Appetite & Strategy	Governance	Methodology	People & Training	Projects, Partnerships & Supply Chain
Level 5 Transformational	Risk Management is actively championed by the CEO, Senior management and Members. There is a strong consideration of risk in all decision-making processes	Risk appetite is reviewed at least annually and is taken into account in key decision points including day-to-day operational, as well as strategic, decisions	There is active oversight of risk management from Members and senior management	Management of risk and uncertainty is well integrated with all key business processes and shown to be a key driver in business success	Staff are empowered to be responsible for risk management and the organisation has a good record of well managed risk taking	Risk management is a collaborative activity amongst all parties and shown to be a key driver in success delivery
Level 4 Integrated	Senior Management & Members constructively challenge risk information and consider risk within decision making processes	The organisation has formalised its risk appetite and statements exist for each principal risk category for practical use at key decision points	Governance arrangements are effective and aligned with other processes within the organisation	Risk management processes are used to support key business processes and service delivery	Suitable guidance is available, and a training programme has been implemented to ensure the continuation of risk management capability	Sound governance frameworks are established in these areas and common risk goals are identified amongst all parties
Level 3 Managed	Senior management & Members take the lead to apply risk management across the organisation and a register of key strategic risks is maintained	The concepts of risk appetite and tolerance are understood and utilised by senior management when discussing strategic risks	Formal reporting and assurance arrangements for risk management exist which are delivering value to the organisation and are consistently applied	Risk management processes are established and effective but are not being applied consistently across the organisation	A core group of people have the skills, knowledge and capacity to manage risk effectively and implement the risk framework across the organisation	Risk Managed in these areas is effective, appropriately resourced
Level 2 In Development	Senior management & Members are actively building the organisation's risk culture and a senior level 'risk champion' has been appointed	Risk Management strategies & policies are drawn up, communicated and being acted upon but Risk Appetite is not a concept actively used within the organisation, even if it is mentioned within the policy / strategy	Reporting and assurance exist but are currently being implemented or require development	Risk management processes exist but are currently being implemented or require development	The organisation is taking steps to increase the capacity and competency of individuals with risk management roles and responsibilities	Approaches for managing risk in these areas exist but are currently being implemented or require development
Level 1 Fragmented	Senior management & Members are aware of the need to manage risks	Risk Management is sporadic and unstructured within the organisation	The monitoring and reporting of risks is limited and only done when requested by senior management or Members	No formal process exists for risk management within the organisation	Key people are aware of the need to understand risk principles but there is a skills gap across the organisation	Key people are aware of potential risks factors in these areas

Section 2:

Implementing the Council's Risk Management Approach

2.1 Governance & infrastructure

2.1.1 Risk Management Policy & Strategy

Our risk management policy & strategy links with decision making to ensure it is completely aligned with what we are trying to achieve and how we are delivering this.

The risk management policy & strategy is accessible to all employees and is introduced as part of the induction process. It is reviewed annually.

It can be accessed via the risk management page of the intranet.

The purpose of our risk management policy is to concisely communicate why and how risk management will be implemented throughout the Council to support the achievement of priorities, objectives, and activities.

It is a formal acknowledgement of our commitment to managing risk. It includes

- the rationale for risk management
- details of roles and responsibilities
- WLBC's risk management process
- WLBC's risk appetite statement
- WLBC's corporate risk matrix
- Information on risk escalation

The purpose of the Council's risk management strategy is to provide a comprehensive overview of our risk management framework and to act as a reference point for those responsible for the execution of the risk management process.

2.1.2 Three Lines of Defence

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 (lines) involved in effective risk management:

1. Functions that own and manage risks.
2. Functions that oversee risks.
3. Functions that provide independent assurance.

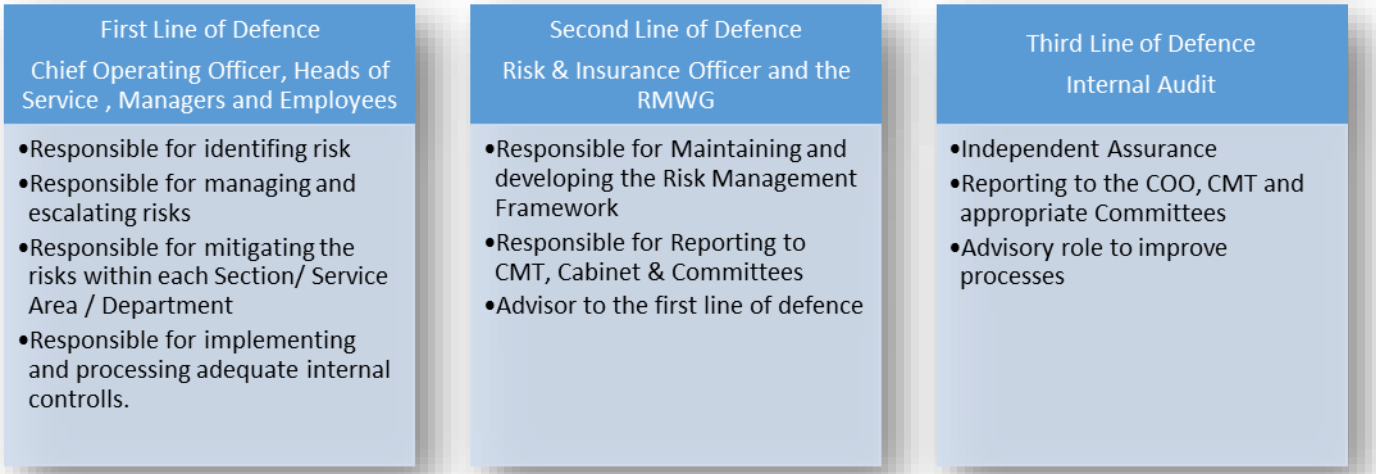
In addition to the three lines of defence there are then a further two functions:

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 is supported by appropriate policies, role definition and training.
- 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.



2.1.3 Risk management roles & responsibilities

Heads of Service

- Implement the risk management framework within their Service, including ensuring that up to date risk registers are maintained.
- Review service risk registers, as a minimum, on a quarterly basis to satisfy themselves that adequate controls for risks are in place, and that risks are added to and removed from risk registers when appropriate.
- Review the risk management framework to ensure that it is functioning effectively and that any further actions required are detailed in service action plans.
- Embed the importance of risk management within their Service and ensure that strategic risks are communicated to employees, and that day-to-day operational risks are communicated to senior management.
- Determine the nature and extent of the principal risks we are willing to take in achieving our strategic vision and priorities.
- Determine how significant risks should be managed or mitigated to reduce the likelihood of their incidence and / or their impact.
- Carry out service risk assessments as part of service action planning.
- Monitor the key risks and associated actions in their area of responsibility.
- Allocate sufficient resources to address significant risks.
- Nominate Risk Management Champions within their Service.
- Ensure risk is discussed at DMT meetings, as a minimum, on a quarterly basis.
- Discuss risk responsibilities during officers' annual performance reviews, and one to ones.

Corporate Management Team (CMT) & Members

- Annually review and approve the risk management policy & strategy, toolkit, and risk appetite of the Council.
- Review the key risks to the Council and the controls in place to manage those risks.
- Review the key risks across the Council, consider their importance against achieving our vision and priorities, and action further controls.
- Create an environment and culture where risk management is promoted, facilitated, and appropriately undertaken.
- Champion risk management activities and raise awareness of the benefits of managing risk effectively.

Senior Managers

- Manage risk effectively in their area of responsibility.
- Complete the risk management process as per the Council's framework.
- Complete, track and monitor the progress of risks, action plans and performance indicators.
- Discuss risk responsibilities during officers' annual performance reviews, and one to ones.

Employees

- Be familiar with, understand, accept, and implement the risk management framework.
- Report inefficient, unnecessary, or unworkable controls.
- Report loss events and near-miss incidents.
- Cooperate with management on incident investigations.
- Ensure that visitors and contractors comply with procedures.
- Monitor work on an ongoing basis to identify new and emerging risks and escalate as required.

Internal Audit

Evaluate risk management processes continuously to provide assurance to Members and senior management that significant risks are being managed appropriately and that the risk management and internal control framework is operating effectively.

Risk Management & Insurance Officer

- Coordinate the Council's risk management activity.
- Develop and maintain the risk management framework and tools.
- Highlight any significant new or worsening risks to the Corporate Management Team for review and action.
- Assist in the delivery of the risk management process across the organisation.
- Provide risk management guidance, training, and advice.
- Provide the link between risk management and other related disciplines.
- Promote and share best practice risk management across the organisation.
- Develop the risk management culture of the Council.

Risk Management Champions

- Attend meetings of the Risk Management Working Group (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 to engage staff in the management of risk.
- Communicate the benefits of risk management across operational areas.

Control Owner

Has accountability for ensuring that the control is in place and is operating effectively. The control owner does not necessarily perform the control activity, however, if not conducting the control, they should have a level of oversight of its performance.

Risk Management Working Group (RMWG)

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

Risk Owner (Officer "assigned to the risk")

- Has day to day responsibility for the risk and for updating the risk register.
- Along with the individual risk manager the risk owner is responsible for agreeing and delivering the action plan to control the risk and monitoring progress against it.
- Must update the risk on Pentana every quarter, as a minimum.

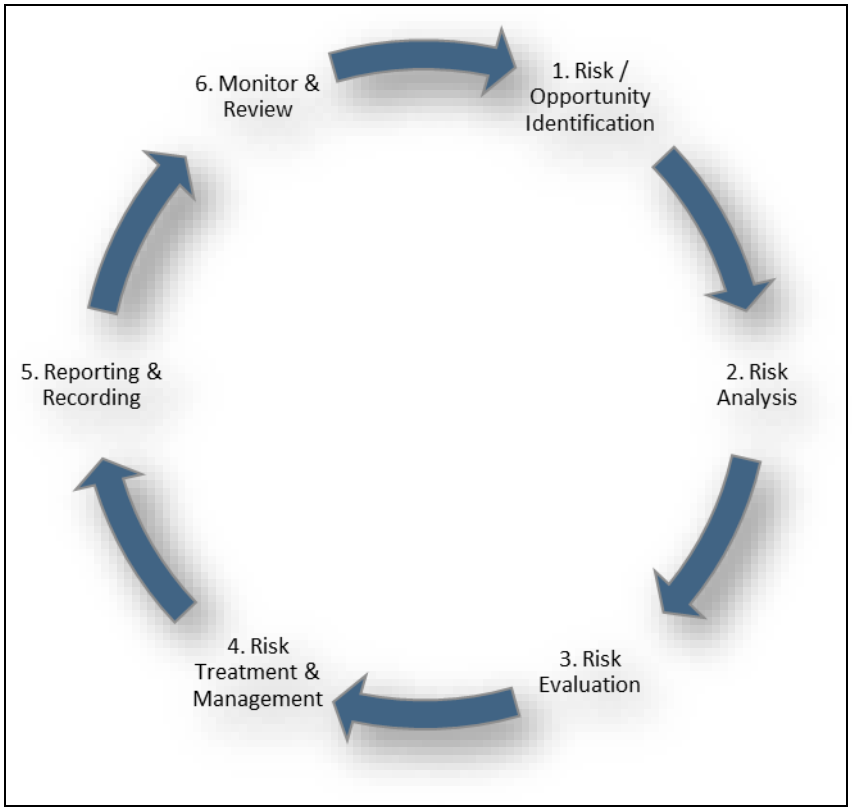
Risk Manager (Designated as manager "managed by")

- The designated member of staff (or management group) who carries the ultimate responsibility for ensuring that the risk is being effectively managed by the risk owner.
- Along with the risk owner is responsible for agreeing and delivering the action plan to control the risk and monitoring progress against it.

2.2 Risk management process

The Councils risk management process is a continuous process involving the identification of risks, prioritisation of these risks and the implementation of actions to further mitigate risks.

Our risk management processes has 6 key stages:



The risk management process outlined in this toolkit is broken down into the 6 steps in the diagram.

2.2.1 Step 1: risk/ opportunity identification

The purpose of risk identification is to generate a comprehensive inventory of risks based on events that might create, prevent, accelerate, or delay the achievement of our vision, priorities, and objectives. It is important that all risks are identified at each level of the Council e.g., CMT, services, departments, and teams.

The starting point for the identification of risks and opportunities should be to examine the Councils, directorate, service, or project's vision, priorities, 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 vision, priority, and outcomes where possible.

It is mandatory that risk management features on the agenda of quarterly DMT meetings and therefore senior 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 for them to report when the extent of the risk changes.

Officers assigned to risks i.e., risk owners should update Pentana with 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.

Risk Identification Techniques

There are a variety of techniques and methodologies that can be used to identify risks and it is essential the method selected works for your team. The important point to remember is that the technique(s) adopted should ensure a variety of officers can input to the process. This will ensure that all risks are identified.

Start the process by reviewing the existing risk registers and asking 3 questions:

1. Have any of the risks recorded changed significantly in terms of impact or likelihood?
2. Are any risks missing from the risk register?
3. Is anything planned over the next 12 months that will give rise to a significant risk?

This should not be limited to a review of existing risk registers; it must also include some fresh thinking on what new and emerging risks need to be considered. Techniques for this include:

- Analyse previous losses, events, incidents, or lessons learnt. All of these can be reviewed to identify the common causes which will allow related risks to be considered.
- Technical briefings, national reports, and networking. Access to relevant national reports, technical briefings, specialists (including internal experts) and guidance is a good way of disseminating and highlighting relevant risk issues.
- Checklists can be a good way of collecting a lot of risk information quickly.
- Experience
- Horizon scanning
- Inspections of premises
- Audits (internal audit, health & safety or external)
- Equality analysis
- Directorate / service / team meetings
- Workshops and brainstorming
- Internal control processes
- Day to day operations
- Local / national or social media
- Alterations to legislation
- Insurance claims / losses information

Risk Identification Techniques

- **SWOT analysis**: this represents Strengths, Weaknesses, Opportunities and Threats. A SWOT analysis is a strategic planning method for an organisation and its environment that focuses on identifying the strengths and weaknesses of the organisation (internal) as well as the opportunities and threats (external) to the organisation.

- **PESTLEC analysis**: this is a useful technique to understand the 'big picture' of the environment in which you are operating. It considers the organisation/ project from a Political, Economic, Sociological, Technological, Legal, Environmental and Cultural point of view.

- **Facilitated Workshop**: this is a useful technique to bring together a number of stakeholders who will all have differing perceptions of risk and the potential consequences if those risks were to materialise

Running a Risk Identification Workshop

There are many ways of designing and facilitating a risk workshop. One method is shown here – which is based on risk identification only.

Before the workshop be clear about:

- what the specific service / team / project priorities or objectives are that you will be considering
- the structure and content of the session, including what you will and will not be discussing
- the roles of the facilitator and participants
- who needs to attend
- any material which will be circulated in advance and who is responsible for circulating it.

During the Workshop

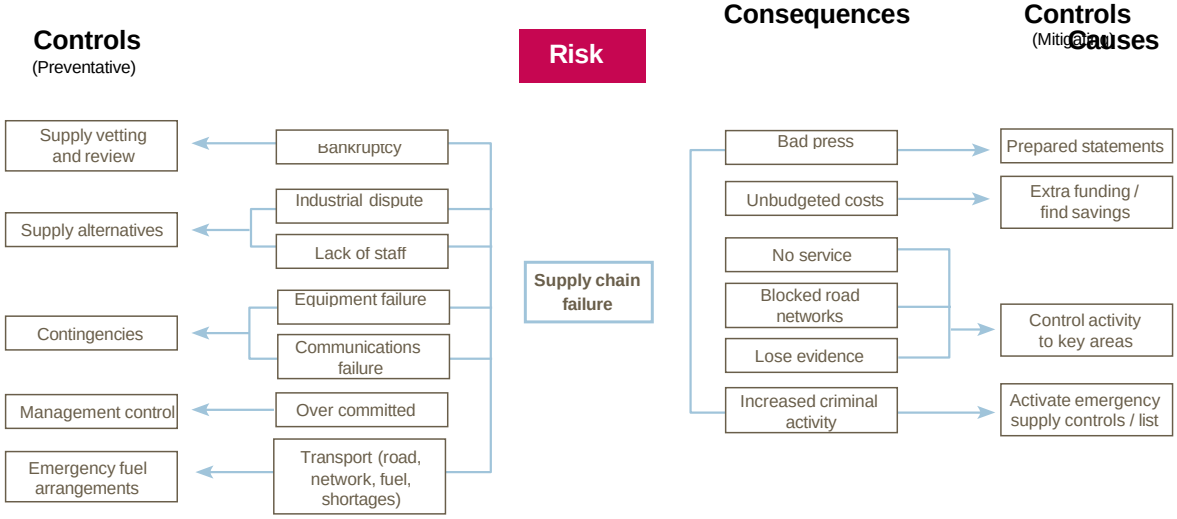
- Introduction / scene setting
  - agenda
  - the objectives or priorities that risks are being considered in relation to
  - details on how you will describe risks as well the different types of risk categories
  - for small groups (up to 6), you could use post-it notes to capture risks. The facilitator can then group them into risk categories before sharing them with the group.
  - for larger numbers you may wish to split the participants into syndicate groups (average 3-6 per group) get them to focus on one or two risk areas and use flipchart paper to write down the risks.

Output

- Your output report could cover
  - the aims and objectives of the workshop
  - the process used to identify the risks
  - a list of those who attended
  - the risks identified
- The report should be circulated to interested stakeholders requesting comments / feedback. A further workshop could be organised to complete the task of scoring and indicating new and existing controls etc.
- The risks should be entered onto Pentana.

- Bow tie analysis / illustration: a visual illustration of the identified risk, its causes, consequences, proactive controls, and reactive mitigation. The bow tie is easy to interpret and is a good way to engage officers at all levels in the risk identification process.

Example bow tie analysis



- These risk identification techniques are not mutually exclusive – use whichever one / combination works best for you.

The Risk & Insurance Officer is happy to facilitate any risk identification sessions so please consider inviting them along.

This following Risk Universe supports the risk identification stage of the risk management process. It can be used as a prompt as to the type of risks you should be considering during the risk identification process. The list that follows is provided as a guide and is not designed to be all encompassing but is useful as a starting point to identify risk(s). The risk identification stage should be repeated regularly to ensure that new risks arising are identified and brought into the risk profile as appropriate.

Cultural The cultural environment in which the Council is operating	• Cultural diversity of the local area and the Council's ability to ensure everyone is catered for. • Services are no longer in demand due to changing behaviours.
Environmental Environmental events as well as increased environmental awareness or regulation can all impact public service organisations	• Nature of environment • Waste disposal and recycling issues • Pollution issues, e.g., fly tipping, • Growing environmental, social and governance agenda • Severe weather or public health emergency increases demand on services • Flooding and other severe weather and the need for investment in counter measures
Financial risks Issues arising from the budgetary, financial planning and control framework	• Financial situations 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 • Changes in government priorities and fiscal policies that can influence the need for alternative revenue streams • Changing international economic relationships that can impact local businesses and the support they require • Push towards engaging partnering/ outsourcing to the private sector
Health & Safety Risks The need to provide a safe environment for staff, citizens, and all stakeholders	• 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
Legislative / Regulatory/ Compliance The legal and regulatory framework in which the Council exists	• Preparedness for new, and compliance with existing, legislation and regulations including European law / regulations • Exposure to regulators - e.g., auditors / inspectors • Changes to the litigation environment
Operational risks The need to effectively deliver services which meet the needs and expectations of customers and residents	• Why is service delivery not 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.
Partnership / Contractual Key strategic partners from public, private and third sectors, County strategic partnerships, joint ventures and outsourced services	• The delivery of services • Investment of time, money and expertise • Meeting organisational objectives • Fair procurement • Risk of financial and reputational risk.
People The need to be managerially and professionally competent and for staff to be satisfied	• Professional / managerial standing of key officers • Stability of officer structure - particularly at the top • Turnover, absence, stress levels, illness • Workforce planning • Equalities issues • Managing major changes

Physical risks to Systems & Assets Physical hazards associated with systems, property, vehicles, plant, and equipment.	• Nature and condition of assets e.g., buildings and other property owned, dilapidation of leased property • Testing of systems to ensure efficiency
Political Political decisions can impact on many areas in public service organisations.	• Central Government initiatives impacting on Local Government • Changes to devolution and powers of Councils • Political uncertainty and changing priorities of local and national groups • Pressure to become more commercial and provide support for local businesses
Sociological Changes in social trends can dramatically impact public service organisations, both on service demand and supply.	• An ageing population increases pressure on certain services • The impact of social media on patient or public activism is a potential opportunity as well as a threat • Changing expectations of the local community
Technological New technologies create new products and new processes that can impact service providers and end users.	• Impact on reputation and services of not implementing new technologies • Need to invest in provision of quality telecommunications to all communities • Effective communication is essential.

Categories of Risk

When identifying risks all categories of risk should be considered. The risk universe above provides examples of the types of risk that may occur across the Council, some of which are aligned to the risk categories. This can be used to guide the identification process, although it is not an exhaustive list of all the potential areas of risk and your may have to think beyond these risks to ensure the unique risk profile is captured. You may also wish to add more categories / amend some of the category titles to align better to your service/ team or project.

Articulation of Risk

It is important to ensure risk descriptions are brief but fully communicate the risk in question. The following wording groups are often used to begin the process of articulating risk:

Failure to …	Reduction of …
Loss of …	Disruption to …
Inability to …	Increase in …
Inappropriate …	Lack of …
Exploitation of …	Realisation that …
Enhancement of …	Empowerment of …

Example of a well worded risk

- Risk: failure to retain key employees.
- Cause: uncompetitive compensation packages, work overload of staff.
- Potential Effect: disruptions to services, increase in temporary staffing costs, increased pressure on recruitment team.

Opportunity risk management is discussed later. An example of a well worded opportunity is provided below:

- Risk: enhancement of the pricing terms with key contractors for labour / material.
- Cause: ongoing effects of the current economic climate are putting downward pressure on the price of labour and materials.
- Potential Effect: procurement savings, reduction in the cost of key projects.

Recording Risks

It is imperative that risks are recorded on the appropriate risk registers on the Pentana Risk System. 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, along with the risk manager, carries the ultimate responsibility for mitigating, controlling, and monitoring the risk.

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.

The Council's risk registers have several key elements to them, and officers are expected to record those elements detailed below on their service risk register. Whilst the following information summarises the steps that need to be taken, all officers using Pentana risk should watch the Pentana Risk Webinar available on the intranet before inputting any risks into Pentana

Officers should also consult the flowchart for permissions required to add a risk to service and key risk registers.

During the risk identification process you should aim to complete the following columns in the risk register:

- **Code:** unique risk number / letter that will follow the risk for the duration of the process to enable mentoring and reporting.
- **Risk title:** a brief articulation of the risk. This needs to be specific so as not to over complicate your risk register but also needs to fully articulate the risk in question to ensure it is clearly understood by the reader.
- **Risk Cause:** What the cause of the risk may be.

Notes Owners & Profile Tab

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 owner should be someone with knowledge of the risk area and be senior enough to insist mitigations are completed. The risk owner must carry out a quarterly review of the risk register. Managed by - The person ultimately responsible for managing the risk, agreeing, and delivering mitigations to control the risk. Risk Champion – Allocate to the Risk Management Champion for your area. A list of Risk Champions is available on the risk management page of the intranet.
Corporate Priority	Select the appropriate priority from the dropdown box.
Potential Effect	The consequence to the Council / service / team should the risk materialise. More than one consequence can be recorded for each risk.
Year Identified	The year that you first became aware of the risk.
Notes	Note any details that you wish to note in this section. Examples include: • Why a risk category was not scored • Reasons for changes in scoring • Detail briefly the current position of the risk e.g., has a report gone to Cabinet / Council, has a report been approved, is a periodic review about to take place, has a project manager been appointed, is the risk being audited.

2.2.2 Step 2: Risk Analysis

In the risk analysis phase, we analyse the size of risk based on the likelihood of the risk occurring and the impact that the risk may have if it did occur. The risks that have been identified need to be assessed so that we can prioritise mitigation actions towards better controlling those risk areas that are most likely to prevent or hinder the achievement of our vision, priorities, and outcomes.

We do this through the application of assessment criteria that evaluates risk from two perspectives; impact (severity) and likelihood (probability) and calculates a risk score. Risk impact refers to the impact to the Council should the risk materialise, whereas likelihood refers to the chance of that risk materialising.

The risk score is then calculated as follows

Impact Score x Likelihood Score = Risk Score

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

The likelihood and impact of the current risk is then assessed, this is an assessment of the risk with all current controls in place. 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.

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.

Risks must be assessed against each appropriate impact category.

The following table gives examples of how the **impact** score can be determined for each category. This impact chart will appear on Pentana when you are scoring your risk.

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 reduces service quality. Some minor staff dissatisfaction	Medium term low level / insufficient experienced staff to deliver quality service. Low staff morale.	Late delivery of key objective / service due to lack of experienced staff. Very low staff morale.	None delivery of key objective / service due to lack of experienced staff.
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 workdays 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 disruptions 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 noncritical 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.

Risk Type/ Category	Low	Medium	Significant	High
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 impact 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 impact categories will allow us to identify accumulations and interdependencies of risk.

Once the likelihood and impact for each appropriate category is scored on Pentana an overall risk score will be generated.

If for example you have a risk with a potential high environmental risk, but only a low financial impact this does not mean that Pentana 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

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 the risk to make judgements.

Record the following on Pentana

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.
Inherent Risk Matrix	This will be completed the first time you score a risk. Consider the Council's risk matrix and where the inherent risk sits in relation to likelihood and the impact of all categories.
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 the impact of all categories. The score should illustrate how the risk scored at the time of the review.
Target Risk Matrix	What can we do further to reduce the risk down to an acceptable level? Use the Council's risk assessment to calculate the likelihood and impact score.

2.2.3 Step 3: Risk Evaluation

The purpose of risk evaluation is to support decision making. Risk evaluation involves comparing the results of the risk analysis with the Council's risk appetite to determine where additional action is required. This can lead to a decision to:

- Do nothing further
- Consider risk treatment options
- Undertake further analysis to better understand the risk
- Maintain existing controls
- Reconsider priorities and objectives

The Council's full risk appetite statement is set out in the Risk Management Policy & Strategy 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

Risk Map

Producing a risk score not only allows you to easily prioritise the risks identified, it also enables their presentation on a risk map. This is a visual tool that illustrates the Council's risk profile.

The positioning of the risk on the risk map will guide the control response, for example a score in the red zone (critical zone) would be very severe and call for immediate action, whereas one in the green zone (comfortable) is likely to be relatively unimportant and viewed as manageable.

Once the inherent risk has been classified it is mapped onto the Council's corporate risk matrix. The colours are a “traffic light” system that denotes the risk appetite of the Council.

The mapping is repeated to record the current risk as this will show how controls in place have influenced the level of risk 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 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.

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? Evaluation of the risk will lead to decisions regarding the treatment of risk.

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.

		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**

2.2.4 Step 4: Risk Treatment & Management

The purpose of risk treatment is to select and implement options for addressing risk.

Risk treatment involves an iterative process of:

- Formulating and selecting risk treatment options
- Planning and implementing risk treatment and controls
- Assessing the effectiveness of that treatment / control
- Deciding whether the remaining risk is acceptable
- If not acceptable, taking further treatment

Controls are methods used by managers to assure them that they are achieving their 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 and needs to be balanced against the potential consequences if the event occurred. The cost of implementing and operating a control should not normally exceed the maximum potential benefit.

Risk action planning or risk treatment should only address those risks considered to be at an unacceptably high level, so requiring additional treatment.

Determining the nature of risk treatment

For those risks which require additional treatment, there are four primary responses; terminate, transfer, treat or tolerate:

1. ***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.

2. ***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.

3. ***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 the apportionment of liability and accountability between parties.

4. ***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 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.

Opportunities

If dealing with opportunities, opportunity responses will need to be considered e.g., exploit, share, enhance and accept.

When evaluating what treatment options to employ the following should be considered:

- existing best practices to treat the risk
- those critical few controls that will achieve the level of risk reduction required as part of the risk treatment / mitigation plan
- the costs associated with the different treatment options against the associated benefits
- how other organisations mitigate the risk.

Control Effectiveness

Scale		Description	Control type
1	Fully effective	Full compliance with statutory requirements; comprehensive procedures in place; no other controls considered necessary; ongoing monitoring only	Control is likely to be of a preventative nature (e.g., prevents the risk from occurring) and be system or automatic (e.g. password protection, electronic banking authorisation process)
2	Partially effective	Reasonable compliance with statutory requirements; reasonable standards established; some preventative measures in place; controls can be improved	Control is likely to be either reactive (e.g. Business Continuity Plan) or of a deterrent nature (e.g. corporate policy, training) and as such would not be considered as effective as a purely preventative control
3	Not effective	Insufficient controls; weak procedures; limited attempt made to implement preventative measures	Control is either not in place or not working as intended

Action Plans

The risk owner then may wish to develop an action plan in collaboration with relevant stakeholders. Action plans can be used as a tool for assigning and monitoring additional actions that have been identified to mitigate the risk further. These are not internal controls that have already been put in place but are further actions that could be put in place to mitigate the risk further e.g., if the risk was not having a fit for purpose risk management framework, internal controls already in place may be all staff have been trained in risk management. An action may be a 3-year programme of work to develop risk management with milestones such as develop a commercial risk appetite, draft guidance on project risk management etc. Action Plans can be detailed on Pentana with milestones and associated performance indicators. The remainder of the Pentana screens should be completed at this point.

Internal Controls Tab

Internal Controls	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, i.e., the control owner. Record the further controls that are required to reach the target risk and detail who the controls will be assigned to. Controls must be allocated to a control owner to enable us to identity the responsibility for a control. Individual controls should be scored as not effective, partially effective, or fully effective. (Guidance above) The control should state whether is reduces the impact and / or likelihood of the risk. 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. If appropriate 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. Once internal controls are entered summarise them in the summary section and tick the "internal controls ok" box if you believe that adequate controls are in place.

Related To Tab

Actions	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. Is appropriate action plans and risks should be linked on the Pentana system, and it is recommended that where appropriate, or where the risk is a key risk that it is linked to an action and vice versa. Key risks should include the risks that will stop the achievement of the Council vision, priorities and outcomes.
Performance Indicators	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.
Risks	Link to any other appropriate risks
Assignment of a risk to a risk category	Key Risks should be allocated to the key risk register by assigning them to category "KR Key Risks". You should discuss the risk with your Head of Service to ensure that they agree with allocating the risk to the Key Risk Register. 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

More Tab

Management	Select how controlled the risk is • **Uncontrolled** - no controls in place that reduce the impact or likelihood of the risk occurring • **Control Pending** - controls considered but action not yet taken to implement them • **Controlled** – controls in place are reducing the impact and/ or likelihood of the risk occurring. • **Over Controlled** – the controls in place are disproportionate to the level of risk.
Approach	For risks requiring additional treatment, there are four primary responses, these are known as the 4T's Select one of the 4Ts of risk management: tolerate, terminate, treat, and transfer.
External Assurance	If external assurance has been received that the controls are effective then tick the "External Assurance Given" box and in the External Assurance comments box explain what the external assurance is e.g., an external review of health & safety procedures, an external audit of council procedures.

2.2.5 Step 5: Reporting & Recording

The Council has in place a risk reporting process.

- The risk management framework is reported to Audit & Governance, Executive Overview & Scrutiny Committee, and Cabinet on an annual basis.
- Key risks are reported to CMT on a quarterly basis
- Key risks are reported to Executive Overview & Scrutiny Committee, and Cabinet on a 6 monthly basis
- Critical risks are reported to CMT on a quarterly basis.

The risk tab on your portal on Pentana will display all your service risks in addition to the risks that have been determined key risks to the Council.

Key risks are also reported on the Corporate Reporting tab on your home portal.

Risk reporting is necessary

- for decision making and to provide assurance
- to compare risk levels with risk appetite
- to enable a thorough review of key, service, and project risk registers

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 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.

The Reporting of Key Risks

Our Key Risks are those risks which if they occur would have the greatest impact on the Council, the achievement of its the achievement of its vision, priorities, and activities. They are strategic high-level Council risks.

If you are assigned to a risk that has been assessed as a key risk, it will appear on your home portal as a key risk. It will also appear on the corporate reporting tab of your home portal. It will be assigned to the key risk code "KR Key Risks" and will have the word KEY in the title.

If your risk is a **key risk** then you will also have to complete the reporting information section on the Notes, Owner & Profile Tab of Pentana. This reporting information contains the Internal Controls Summary and Notes Summary that will used to update Members on the progress of the risk. The reporting information section only needs to be completed for key risks.

2.2.6 Step 6: Monitor & Review

The purpose of monitoring and review is to assure and improve the quality and effectiveness of the risk management process design, implementation, and outcomes. Ongoing monitoring and periodic review of the risk management process and its outcomes takes place, and the results are incorporated in our performance management, measurement, and reporting activities.

Few risks and risk action plans remain static; risks change, priorities change, actions get completed, risk responses that were once effective may become irrelevant, etc. Therefore, there are two elements to monitoring that need to be addressed:

- monitoring risk response effectiveness
- monitoring the risk profile.

Monitoring risk response effectiveness

As the Council will be constantly changing, we need to constantly determine whether risk controls are still effective and adapt them as required.

In addition, monitoring and review should take place in all individual stages of the process. 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 vision, priorities and objectives is maximised, and losses are minimised.

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

Reviews of risk registers to ensure they remain up-to-date and relevant should also be carried out as;

- Few risks and risk action plans remain static; risks change, priorities change, actions are completed, risk responses that were once effective may become irrelevant.
- 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.

Monitoring risk profile

The risk profile of the Council will constantly change in line with the organisation, strategy, government decisions, service models, new initiatives, and projects. To ensure senior management is effectively managing this changing risk profile it is important to ensure the management of risk process is continuous.

Any significant changes to the risk profile noted during the formal risk management process should be recorded in the relevant risk register and reported as required.

Metrics

Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) can be developed to assist the monitoring process.

Key Performance Indicators (KPIs) measure the effectiveness of functions and processes.

Key Risk Indicators (KRIs) measure how much risk the organisation faces and which risk treatments to apply.

KRIs can be used as early warning indicators to monitor the risk causes to ensure that the monitoring of risks is proactive rather than reactive. They can be an indicator of change in the likelihood or impact of a risk and assist in the decision-making process for risk mitigation.

Examples of KRIs include:

- complaints
- service user numbers
- employee turnover rates
- budget over or under spend
- public liability claims
- incidents of vandalism
- helpdesk responsiveness.

Risk at DMT Meetings

It is a mandatory requirement that risks are discussed at least quarterly at DMT meetings. Although the exact process used will differ between management teams, the following questions can be used as a guide to promote discussion.

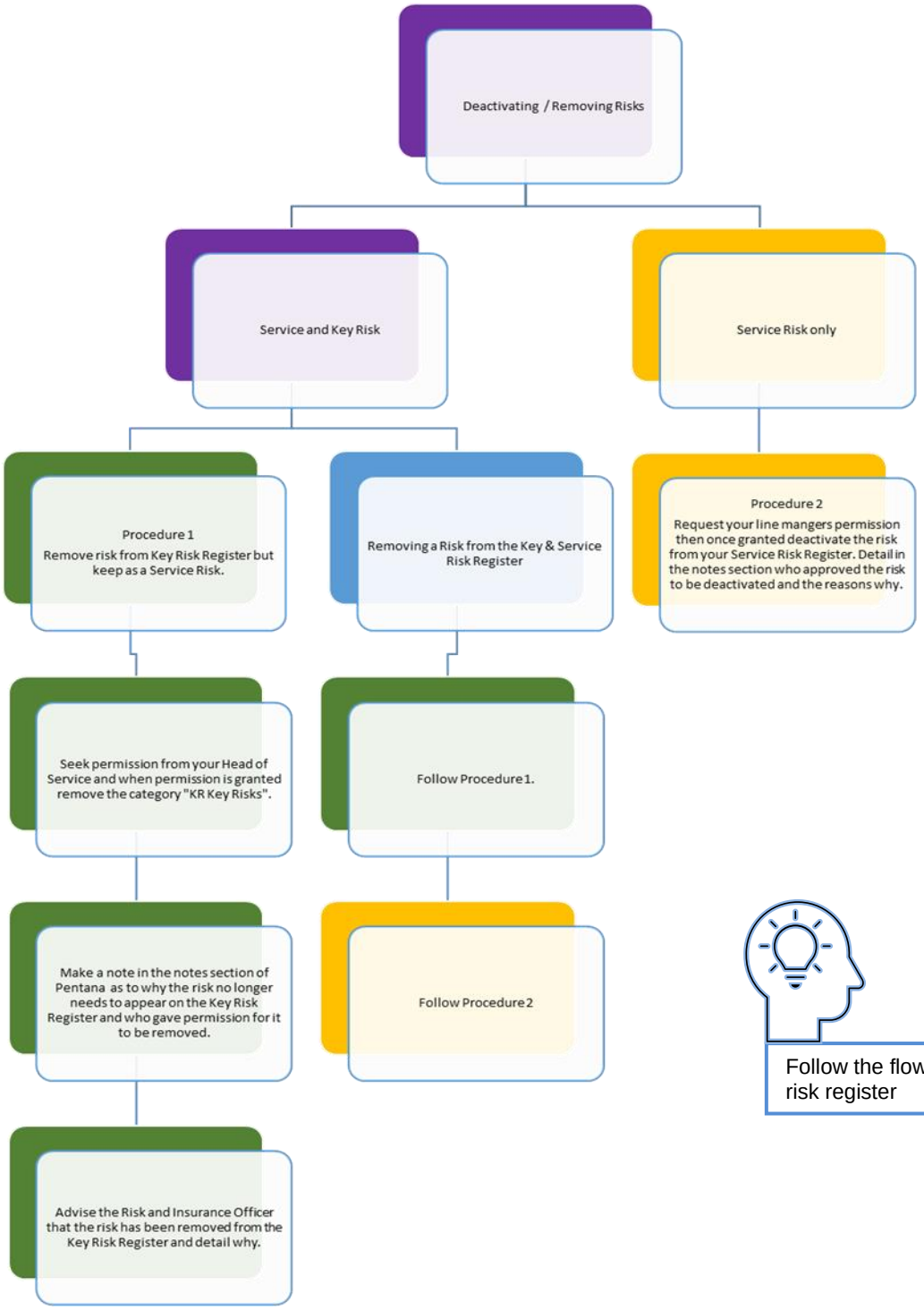
1. Are there any risks missing from the risk register that should be included?
2. Have we included all the risks that may hinder the achievement of the Council's vision and priorities?
3. Have any of the risks in the risk register changed significantly in terms of impact and/ or likelihood and require additional mitigation efforts?
4. Do any of the risks now require escalation?
5. Are controls, any related action plans, and performance indicators still appropriate for the risks?
6. Is there anything planned in the next 12 months that may give rise to service or key risks?
7. Can any risks be removed from the register?
8. How might the risks on the key risk register impact the service?

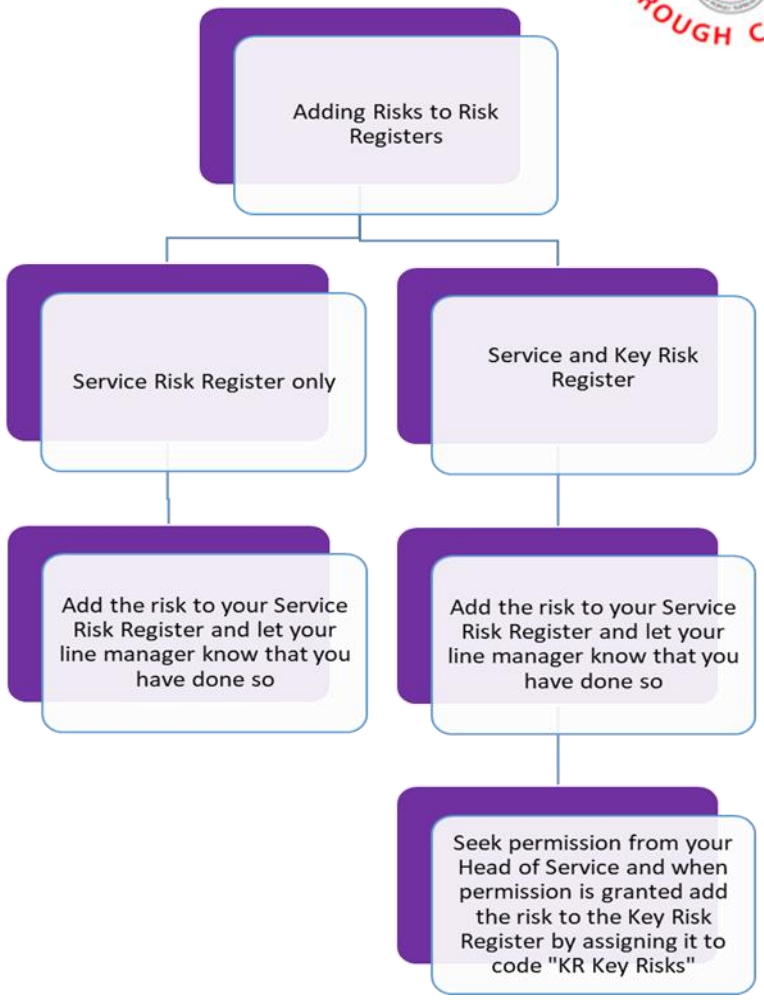
Deactivating and adding risks to service and key risk registers.

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 key 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 and Committees. 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.





Follow the flowcharts when adding or removing a risk from service or the key risk register

2.3 Integration of risk management

2.3.1 Integration with projects and programmes

Projects and programmes form a large part of the operations of the Council. Risk is present in all projects and programmes and therefore these risks require recording, managing, and monitoring through the Council's process. Some of the benefits of project / programme risk management include:

- improved stakeholder relations
- on time, on quality and on budget programme / project completion
- early allocation of risk and risk mitigation responsibility to the most appropriate owner
- risk mitigation is focused on the biggest risks to achieving the project / programme objectives
- greater certainty around decisions
- demonstration to stakeholders that the project / programme is being managed effectively.

When dealing with the management of risk across projects and programmes the risk management process outlined in Section 2.2 of this toolkit should be applied.

The basic process will remain the same but there are some additional considerations:

- Risk identification:
  - should focus on the risks that may impact the achievement of the project or programme objectives
  - should be completed by key project / programme team members
- Prioritisation:
  - risk assessment scales can be developed based on the parameters of the project / programme e.g. the likelihood scale should be aligned to the duration of the programme / project.
- Controls:
  - the cost / benefit of proposed additional controls should be considered within the parameters of the project
  - risk ownership should be allocated across the project / programme team.
- Monitoring and reporting
  - risk reporting should be integrated with established project / programme reporting lines
  - risks should be monitored at the beginning of each stage of the project.

- Ask the Council's risk function to be involved at the very beginning of the project.

The golden rules of project risk management

1. Make risk management part of the project
2. Identify risks early
3. Communicate about risks
4. Consider both threats and opportunities
5. Clarify ownership issues
6. Prioritise risks
7. Analyse risks
8. Plan and implement risk responses
9. Register project risks
10. Track risks, associated actions, and performance indicators.

2.3.2 Partnerships and third parties

Reduced public service funding is leading to more public services and community projects being delivered through different forms of partnership, involving the public, private and third sectors. These partnerships range from small, local initiatives to much larger agendas, such as issues of obesity and ill-health in the community, or anti-social behaviour.

Examples of partnership risks:

Ask to view partners risk policies and ask them to demonstrate the approach that they have to risk management as part of any procurement process.

To ensure a successful outcome, all the risks need to be evaluated, including those relating to the partner organisations themselves, and their relationships with one another. It is also important to ensure a common risk language is agreed between the parties and an understanding reached on the risk appetite of each partner organisation, at the outset.

In this toolkit Partners are defined as:

Organisations with which a department works to deliver their objectives, with a formal agreement of roles, contract, funding agreement, Service Level Agreement, etc.

The risk management process for partnerships is similar to that outlined in Section 2.2, with the following considerations:

Risk identification

- Focus on risks that may impact achieving partnership objectives.
- Involve all key partners.
- Use a partnership risk register to record this information. Pentana may be used for this and to generate risk reports to share with partners.

Prioritisation

- Develop risk assessment criteria based on the parameters of the partnership. For example, the likelihood scale should reflect the partnership timeframe.

Controls

- Allocate risk ownership and responsibility for actioning controls to an individual partner within the partnership.
- Agree risk mitigation that requires input from multiple partners with the partnership.

Monitoring and reporting

- The process for ongoing monitoring of the risk profile and progress of the action plan should be agreed by the partnership.
- The frequency and content of risk reports should be agreed by the partnership, with allocated responsibility all key partners should be involved

2.4 Risk management culture

Assimilation of risk management into the culture of the Council is central in contributing to its long-term success. Risk management culture refers to people embracing the risk management policy, strategy and process as well as creating a culture that is willing to talk about mistakes and lessons learned without consequence.

Training and communication are two factors that positively influence risk management culture; each is outlined below.

2.4.1 Training

The Council acknowledges that risk management training for staff and Members 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 a mandatory part of the induction process. Two presentations are available, one for Senior Management and Risk Champions 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.

A risk management toolbox talk should be given to those members of staff who do not have intranet access.

Additional refresher training for Officers is arranged and provided annually by the Council's Risk and Insurance Officer. Outsourced training will also be provided periodically.

Training for Members will be arranged and provided annually by the Council's Risk and Insurance Officer. In addition, a risk management webinar is available and forms part of Members essential induction training. This webinar can also be viewed as refresher training.

Frequent "lunch and learn" sessions are run on a variety of risk management topics. These are recorded and are made available on the risk management page of the intranet for all officers to view.

The quarterly risk newsletter "The Risk Round Up" is a good source of risk information and is circulate to all staff and Members. It highlights training sessions that are available, digests risk disasters and lessons that can be learnt from other organisations, and covers appropriate risk management topics.

The Risk & Insurance Officer welcomes she opportunity to attend DMT and service meetings to discuss risk and to act as a critical friend in reviewing the service risk register.

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

2.4.2 Communication

Effective risk management requires engagement from staff across the organisation. Communication on the risk management strategy, policy and processes is essential to ensure a consistent approach to risk management. Managers need to ensure that there is a risk escalation procedure in place so that officers can report any risks that they encounter or when the profile of a risk changes. Officers also have a duty to communicate any risks that they encounter in their role. The reporting of risk is in job descriptions of officers.

Concerns about risks can also be reported to Heads of Service, any CMT member or the Risk & Insurance Officer.

The Council also wishes to learn lessons from failings of near misses, so an open and honest culture needs to be developed within teams. Losses and near misses need to be reported and lessons learnt to ensure that future risks are mitigated.

Appendices

A: Risk Management Work Cycle

	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			Annual Risk Management refresher training for Officers.	
May								
June			Service Registers reviewed					RMWG Meeting
July				Risk Reporting to CMT (approval prior to Cabinet & Exec O&S)			Annual Training for Members	
August								
September			Service Registers reviewed		Key Risk Register reported to Cabinet	Key Risk Register reported to Executive O&S		
October	Reviewed and updated if required. Endorsed by CMT			Risk Reporting to CMT				
November		SAP guidance issued						
December			Service Registers reviewed					RMWG Meeting
January	Reported to Audit & Governance and Executive Overview & Scrutiny			Risk Reporting to CMT (approval prior to Cabinet & Exec O&S)				
February						Key Risk Register reported to Executive O&S		
March	Approval by Cabinet	Proposed SAPs finalised	Service Registers reviewed		Key Risk Register reported to Cabinet		Review & Update On Line Training Sessions	