LANCASTER CITY COUNCIL

Promoting City, Coast & Countryside

Risk Management Policy

November 2025

DRAFT

Contents

Version control

	Description	Date
V0.1	Draft submitted to Executive Team for comments	13 November 2019
V0.2	Draft submitted to Audit Committee	27 November 2019
V1.0	Approved by Audit Committee	27 November 2019
V1.1	Draft submitted to Audit Committee	24 March 2021
V1.2	Revisions submitted to the Senior Leadership Team for comments	18 January 2023
V1.2	Draft submitted to Audit Committee	March 2023
V1.2	Approved by Audit Committee	22 March 2023
V1.3	Revisions to reflect new structure of Council, updated risk categories and risk appetite and clarity on roles and responsibilities.	15 December 2023
V1.4	Minor revisions made to roles and responsibilities	23 February 2024
V2.0	Approved and adopted by Audit Committee	20 March 2024
V2.1	Review by MIAA	April 2025
V3.0	Approved and adopted by Audit Committee	

Due for review every 2 years.

1 Policy Statement

Lancaster City Council is committed to having a risk management culture that underpins and supports its services and intends to demonstrate an ongoing commitment to improving the management of risk throughout the organisation.

The identification and recognition of risks, management of them via mitigation, elimination or acceptance (as appropriate), is essential for the efficient and effective delivery of safe and high-quality services. The priority is to reduce those risks that could impact on the safety of individuals, whilst reducing our financial, operational and reputational risks to acceptable levels.

All staff should have an awareness and understanding of the risks that relate to their role and are encouraged to identify and escalate new risks.

In developing, improving and embedding its risk management system, the Council will take account of the appropriate statutory requirements, national guidance and the requirements of its regulators.

1.1 Key Objectives of the Policy

This policy will ensure that:

a. The management of risk contributes towards ensuring effective service delivery and the achievement of the Council's strategic objectives.
b. All Councillors and staff acknowledge and understand the importance of risk management as a good governance process, by which key risks and opportunities are identified, evaluated and managed.
c. Ownership and accountability are clearly assigned for the management of risks throughout the Council.
d. There is a commitment to embedding risk management into the Council's culture and organisational processes, at all levels, including strategic, programme, project and operational.
e. Effective monitoring and reporting mechanisms are in place to continuously review the Council's exposure to, and management of, risks and opportunities.
f. Best practice systems for managing risk are used throughout the Council, including mechanisms for monitoring and reviewing effectiveness against agreed standards and targets.
g. Accountability to stakeholders is demonstrated through periodic progress reports and an annual statement on the effectiveness of and the added value (benefits) from the Council's risk management strategy, framework and processes.
h. Where possible the Council's approach is regularly assessed by an external, independent body against other public sector organisations, national standards and Best Practice.
i. The Risk Management Policy is reviewed and updated biennially in line with the Council's developing needs and requirements.

1.2 Scope of the Policy

This policy applies to all staff, Councillors, functions, working groups and partnerships. The responsibilities of these groups and the individuals within them, for the implementation and the effective management of risk is contained within this policy.

2. What Is Risk Management?

Risk is unavoidable and is part of all our lives. Risk management is a systematic and cyclical process, in which potential risks are identified, assessed, managed, monitored and reviewed. It is applicable at all levels – Leadership Team, service, team and individual.

Risk management is a proactive approach which:

- Identifies the various activities of the organisation
- Identifies the hazards that exist within those activities and the risks associated with those hazards
- Assesses those risks for likelihood and potential severity (impact)
- Eliminates the risks that can be eliminated
- Reduces the effect of those risks that cannot be eliminated
- Acknowledges those risks that can be accepted
- Seeks to engage with colleagues to understand risks and explain tolerated risks
- Regularly monitors and reviews all risks.

This policy explains Lancaster City Council's approach to **all** risk management activities within the Council and describes the framework that will operate to establish and drive effective, integrated risk management across the totality of Council activities. The diagram below identifies the core categories of risk management activities referenced in this Policy.

2.1 Risk Management Framework

By managing the Council's risk process effectively, we will be in a better position to safeguard against potential threats and exploit potential opportunities to improve services and provide better value for money.

A Risk Framework is made up of several interconnected and dependent processes and is shown in the diagram below.

2.2 Identification of Risk

Everyone needs to be aware of the potential for risks to emerge which may affect the Councils services or business. All colleagues should be prepared to identify and report risks as appropriate. The Council will be open in its approach to managing risks and will seek to avoid a blame culture. Discussion on risk in any context will be conducted in an open and honest manner.

- A **risk** is a future uncertain event or set of events that, should it occur, will have an effect on the achievement of the Council, a project management failure, or a failure of governance arrangements. Risks facing the Council will be identified from several sources:

  i. Risks arising out of the delivery of work-related tasks or activities.
  ii. The review of strategic or operational objectives.
  iii. A result of incidents and the outcomes of investigations.
  iv. Complains, claims, staff and customer feedback, health and safety inspections, audit reports, external reviews or ad hoc assessments.

- An **issue** can be defined as an event that has already happened, was not planned and requires management action. Issues should be captured on an issue log and managed in a timely manner.

2.3 Types of Risk

Risks can be classed as internal or external facing and can be associated with an opportunity:

- **Internal Risks** – are those faced from within the organisation, that arise from routine day to day activities such as managing staff, safeguarding, health and safety, financial challenges or operating IT systems etc.

- **External Risks** – are those that from outside the Council but may still have an adverse impact on its activities, for example, a major cyber-attack or extreme weather conditions. External risks are hard to manage as we have less control over whether they occur.

- **Opportunity Risks** – are those risks associated with plans that aim to benefit the area the Council services, for example from an investment. These risks can be acceptable provided they are well thought out and properly managed.

2.4 Risk Management Across the Council

Risk management is applied at all levels of service delivery across the Council. Some areas require their own risk management policy, with the Risk Management Policy forming an umbrella policy over these.

- **Strategic Risk -** are comprised of internal and external risks, the careful management of these risks is critical to the success and continuation of the Council. Strategic risks may emerge following the inability to manage/mitigate/element risks initially reported in other risk categories, through escalation scoring. All strategic risks should be assigned to at least one Chief Officer. These risks are reviewed on a quarterly basis and reported to various Council committees.

- **Health & Safety Risk -** Health and Safety is a complex area of legislation one requirement of which is for the organisation to have a Health and Safety Policy and which should incorporate effective risk management and align. The Council's Health and Safety Risk Register is held within the My Compliance system with the overarching risks being repeated within the Grace system for escalation purposes. The risk assessment policy can be accessed via this link: SG02 Risk Assessment Policy.

- **Information (including Information Governance, IT Security and Systems Management) Risk -** is an integral element of good data security and protection. It includes use of IT systems, management of paper records, cyber security and physical security of our facilities. The Council has a number of policies in place to manage risks in this area. Key risks in these areas are included within the Grace system as the central repository.

- **Business Continuity Risk -** are those which threaten the organisation's ability to deliver its key services. These generally fall into three categories:

    i. access to premises
    ii. access to resources (e.g. IT systems)
    iii. and access to staff

  They can originate from a number of different sources e.g. severe weather, fuel shortage, availability of trained professionals, and usually, but not always, originating outside of the Council. Key risks in these areas are included within the Grace system as the central repository.

2.5 Risk Management Categories

When logging risks in the Grace risk management system, the Council separates risk into the following categories. Risk owners are asked to choose one, or at the most two, risk categories for each risk and refer to the risk appetite guidance in appendix 3.

- Strategy
- Governance
- Operations
- Legal
- Property
- Financial
- Commercial
- People
- Technology
- Data Information and Management
- Security
- Project and Programme

2.6 Describing Risks

Risks need to be described in clear terms that can easily be understood and must specify what is the tangible threat or opportunity. The description should help determine how the risk will be managed and treated.

Risk descriptors are often prefaced with:

- 'Lack of…'
- 'Loss of…'
- 'Failure to…'
- 'Inability to ….'
- 'Reduction of….'
- 'Disruption to…'
- 'Inappropriate…'

Risks should generally be described in a couple of sentences, explaining the risk, cause and effect.

> *For Example:*
>
> *"Failure to deliver major change project on time and in budget (risk) due to a lack of project management and appropriate resources and conflicting priorities (cause) which will result in detrimental impact to deliver the next stage of the programme and will increase temporary staffing costs (effect)."*

2.7 Reporting Risks

All risks should be recorded once identified. The Council uses the Grace Risk Management System for operational (service), strategic and project risks. Any H&S risks should be logged in the My Compliance system.

Training on the use of the Grace risk management system is available to all Chief Officers and risk owners. The Projects and Performance Team (projects@lancaster.gov.uk) can provide further guidance and assistance on this. Colleagues who don't have access to the Grace system should report a risk to their line manager. If they are unable to report and record a risk this way, there is an MS Form which can be accessed from the risk management pages of the intranet that can be used to report a risk. The Projects and Performance team will then progress the recording of this risk with the correct colleagues.

2.8 Risk Scoring - Assessing, Analysing and Evaluating Risks

Scoring A Risk

The purpose of assessing and scoring a risk (which is undertaken as an integral task of reporting a risk) is to estimate the level of exposure to it the Council has, which will then help to inform where responses to reduce or otherwise manage a risk can be taken.

To analyse and evaluate risks, a thorough risk assessment should be undertaken. That is, a detailed analysis of the potential threats faced by the Council which may prevent achievement of its objectives. Through consideration of the sources of the risk, possible consequences, and the likelihood of those consequences occurring, it helps make decisions about the significance of risks and whether they should be accepted or treated.

The Council has adopted the 5 x 5 scoring matrix to ensure that a consistent scoring mechanism is in place across the Council, risks are assessed using the agreed criteria for likelihood and impact detailed in Appendix 1.

When assessing the risk, the highest measure identified in each table is the score taken to plot the risk level on the risk matrix. Where the likelihood and impact cross, determines the risk level:

A "traffic light" approach is used to show high (red), moderate (amber), low (yellow) and very low (green) risks.

For example, a Likelihood of 3 (possible) and a Major impact of 4 would result in a risk level of 12 (Moderate). This score is identified as the **inherent** risk score and would be recorded as such on the Grace risk management system.

Impact	Catastrophic 5	5 Low	10 Moderate	15 High	20 High	25 High
	Major 4	4 Low	8 Moderate	12 Moderate	16 High	20 High
	Moderate 3	3 Very Low	6 Low	9 Moderate	12 Moderate	15 High
	Minor 2	2 Very Low	4 Low	6 Low	8 Moderate	10 Moderate
	Insignificant 1	1 Very low	2 Very Low	3 Very Low	4 Low	5 Low
		Remote 1	Unlikely 2	Possible 3	Highly Likely 4	Almost Certain 5
		Likelihood				

Risk Scoring – types

Initial or First Risk Score – Inherent (or Gross) Risk Score
Following identification of the risk, a score for the gross likelihood and gross impact will be given to the risk as it currently stands, to ascertain the inherent (gross) risk score. The inherent risk score is the score given before any controls or actions are taken to alter the risk's impact or likelihood.

Second Risk Score – Residual (or Risk Response) Score
Risks are then re-scored by the risk owner to ascertain the residual risk score. This is the score given when taking into consideration all controls and treatments in place and/or any existing actions that are not operating effectively. The residual risk score will be the same or lower than the inherent risk score but can never be higher.

Comparing the residual risk score to the guidance on risk appetite for the respective risk category should be the deciding factor as to whether further action is required (see the guidance on risk appetite in Appendix 3). For example, if the inherent risk score is 20, actions are put in place / or can be put in place which will result in the residual risk scoring 8, if this score is within the range of the Council's risk appetite guidance for the respective risk type then this residual risk score should be recorded as such on the risk register. See appendix 2 for further information on risk response categories.

If the residual risk score is either red or amber, the risk owner should escalate this to their manager for information and further review.

Third Risk Score – Target Risk (or Retained Risk) Score
If a residual risk score, after comparison to the Council's risk appetite guidance, requires further mitigating action to reduce the risk score to within the recommended risk appetite of the Council, the risk owner needs to develop an action plan to reduce the risk to within the Councils risk appetite matrix score. For some risks, a Council-wide risk response will be needed.

The amount of time and effort put into reducing a risk should always be aligned with the severity of the risk and should take into account what is practical and achievable. For example, if a risk receives the highest awardable score of 25 then far more time and effort would be put into mitigating it than if it received a far lower score of 6.

It is unusual, but not impossible to be able to reduce a risk down to the very lowest risk score of 1.

2.9 Treatment and Action Planning

Actions, which form part of an action plan to address a risk, will help to minimise or eliminate the likelihood and / or impact of a risk occurring, are identified where the gross (inherent) risk score needs to be reduced. This is either to determine the residual risk score or if the risk score needs further reduction in line with the Councils risk appetite.

Risk may be managed in one, or a combination of, the following ways:

Accept	A decision is taken to accept the risk.
Avoid	A decision is made not to take a risk.
Fallback	Put in place a fallback plan for the actions that will be taken to reduce the impact of the threat should the risk occur.
Reduce	Further additional actions are implemented to reduce the risk.
Transfer	All or part of the risk is transferred through insurance or to a third party.
Share	Share the risk with others on pain/gain basis.
Enhance	Proactive actions taken to enhance the likelihood of the event occurring or enhance the impact of the event should it occur.
Exploit	Whilst taking action to mitigate risks, a decision is made to exploit a resulting opportunity.
Reject	A deliberate decision is taken not to exploit or enhance the opportunity.

These are described in more detail in Appendix 2. The managed approach to risk should always be documented in the risk register, for example, after assessment of the risk, a decision may be made to transfer the risk, therefore no further mitigating controls are required.

2.10 Risk Appetite

The Council's risk appetite refers to the amount and type of risk that it is prepared to pursue, retain or take in pursuit of our objectives before action is deemed necessary to reduce the risk.

Risk appetite is not a single fixed concept; there are a range of appetites for different risks which the Council need to be aligned and regularly reviewed as this will change/vary over time. The Council recognises that it may be necessary to deviate from the adopted risk appetite for individual decisions when there is a good reason to do so.

Our risk appetite varies depending on the risk category assigned. Generally, the Council's appetite for risk can be described as "Cautious". However, there are some exceptions to this. For Operation, Property, Commercial, Technology and Project/ Programme risks our risk appetite is "Open" which means we are willing to accept a slightly higher level of risk to maximise potential benefits.

The order our risk categories appear in, from most risk averse to least risk averse is:

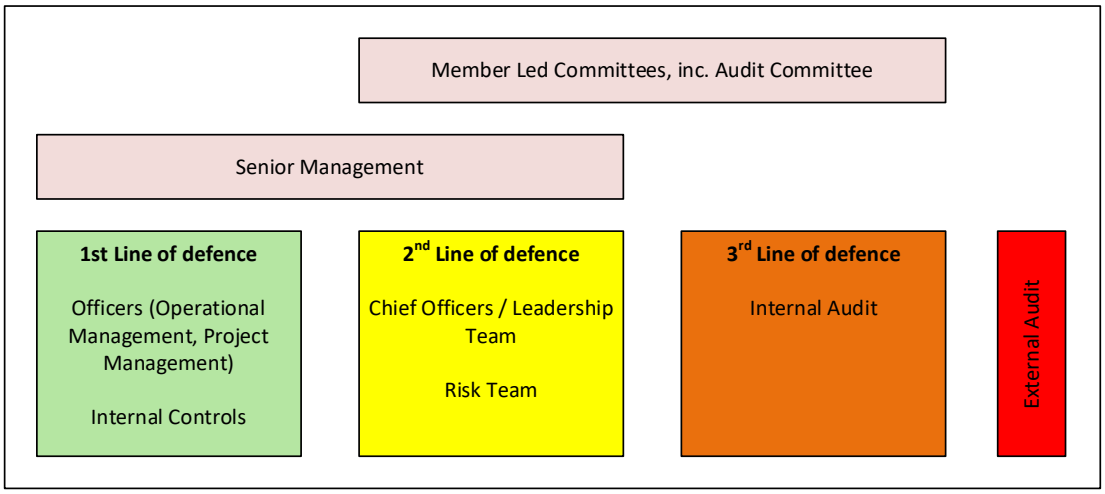
1. Averse
2. Minimal
3. Cautious
4. Open
5. Eager

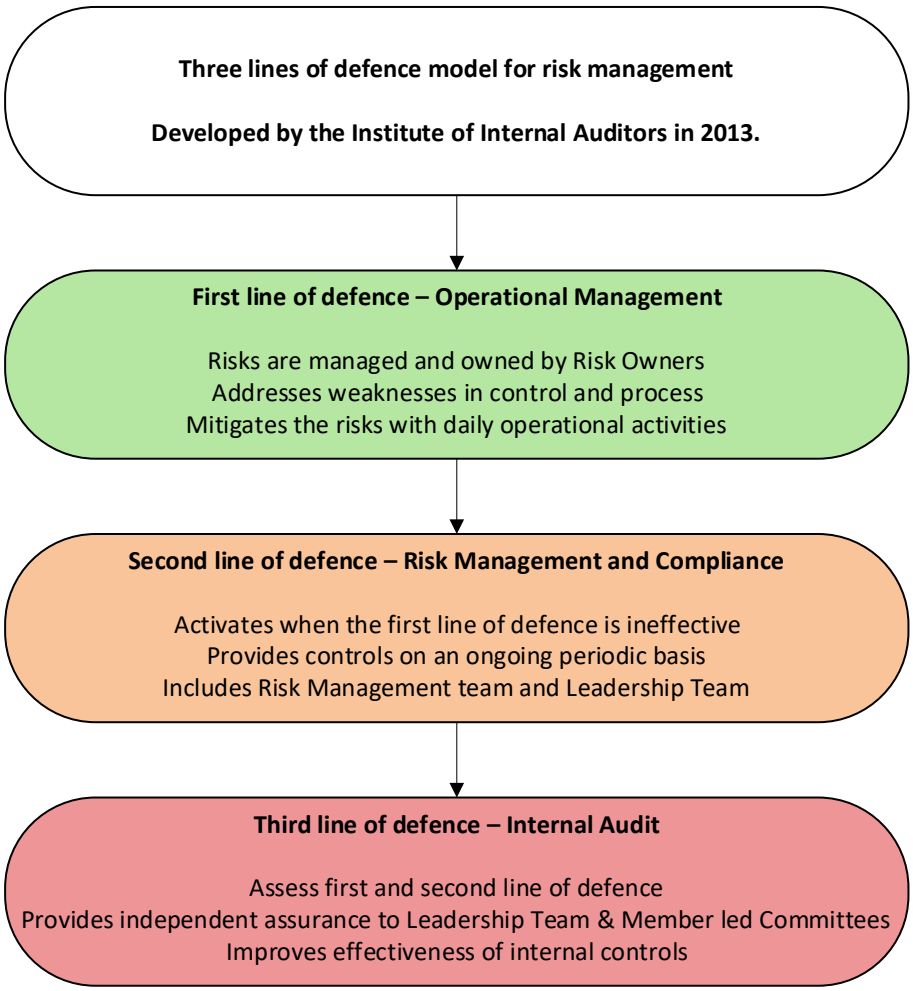
A table showing the Council's risk appetite can be found as Appendix 3.

3 Three Lines of Defence

The Risk Management Policy is predicated on the need to ensure the Council is aware of any significant risk to its ability to deliver its strategic objectives. To do this a process needs to be in place which allows the recording, management and mitigation actions to take place by the right people, in the right place at the right time.

To achieve this, we use the '3 Line Defence Model', shown in the visuals below.





Colleagues within the Projects and Performance Team (People and Policy Service) oversee administration of strategic, operational and project risk registers within the Grace risk management system. Identified risk owners are ultimately responsible for monitoring and updating their risk scores and actions plans.

The Grace system will automatically send risk owners a weekly email reminder of any overdue risk reviews and overdue actions. The Projects and Performance team will monitor overdue risks and action on a periodic basis to ensure that risk owners are updating records as and when required.

Managers are encouraged to amend risk scores or descriptions with the intention of maintaining a culture of openness. The Projects and Performance Team will spot check a selection of amendments to ensure that actions taken such as increased or improved control, or another viable explanation such as the activity ceases altogether, has been recorded within the system to support the change.

4 Management, Escalation and Reporting Framework

Risk management should be thought of as an ongoing process and as such risks need to be reviewed regularly to ensure that prompt and appropriate action is taken to reduce their likelihood and/or impact.

Regular reporting enables Leadership Team and Councillors to have greater awareness of the extent of the risks and progression being made to manage them.

Risk reporting and scoring needs to be simple and transparent and ensure all reported risks are visible and reviewed by the respective oversight.

This will mean that all risks should have clearly identified:

a. Risk Owner
b. Risk Actionee (where further actions are needed)
c. Chief Officer
d. Responsible Governance body – meeting/function and / or specialist (H&S, ICT, Project Board etc)
e. Escalation Route

All risks that fall within the categories of Health & Safety, ICT and Business Continuity should be subject to scrutiny and sign-off (scoring and mitigating actions) and cross-referenced as appropriate on the Grace risk management system.

4.1 Escalation of Risks

All risks originate in the respective operational risk register. The gross (inherent) risk score identified should determine the Responsible Governance Body and the likely escalation route should that be needed.

The decision to escalate or de-escalate a risk score needs to be made within the thresholds identified in this Policy.

The thresholds are defined below:

Risk Rating	Management/Oversight
Very Low **between 1 and 3**	Managed at service level by the risk owner. Updates via Grace. Assurance will be provided on the management of this risk with regular reviews run at least every 12 months.
Low **between 4 and 6**	Managed at a service level by the risk owner with an appropriate manager designated as risk owner who will monitor the delivery of any actions. Reviewed at least every 6 months.
Moderate **between 8 and 12**	The risk owner will make their manager aware of a moderate risk as soon as it is logged. Reports run from the Grace system every month and sent to the Leadership Team for discussion and further action. Amber risks will be reviewed by the risk owner and other interested parties at least every 3 months.
High **between 15 and 25 (strategically significant risks)**	New risks at this level should be reported immediately to the Chief Officer and then raised at the next available Leadership Team meeting. These risks will also be captured in the monthly reporting sent to the Leadership Team for discussion and further action. High risks will be owned by a Chief Officer, regardless of who initially raised the risk. The risks should be reviewed monthly.

Risks should be escalated up the hierarchy of risk registers, from operational (departmental) to strategic etc. when any of the following criteria apply:

a. The current risk score remains very high with a score of 15 or higher, even after control measures and mitigating actions have been fully implemented.
b. The current risk score exceeds the appetite boundaries set for the risk, even after control measures and mitigating actions have been fully implemented.
c. The risk becomes unmanageable by responsible officers at the current level.
d. The risk would impact beyond the current service/directorate/project as appropriate for the current tier of risk register.

Risks should be de-escalated to a lower tier of risk register when the criteria listed above no longer apply.

Escalation to the Strategic Risk Register, should be reviewed and agreed by the respective Chief Officer.

4.2 Recording Incidents

When a risk occurs, it is often known as an issue or incident. It could be beneficial to record an incident when it occurs, so records exist of how often it occurs and the severity of the consequence. Near misses can be recorded in the same way. There is provision within the Grace risk management system to record incidents, using the drop-down fields to note if it was a near miss or an incident and how severe the consequence of this occurring was.

Depending on the risk and what occurred, you may wish to escalate this or involve another professional, such as the Health and Safety team. You may also wish to re-evaluate your risk scoring after an incident occurs, remembering to run a risk review at the end.

Recording an occurrence or near miss allows the Council to review the information collected and learn from these events.

4.3 Grace Risk Management System

The Grace risk management system will encourage risk owners to monitor and update identified risks on a regular basis. In line with our policy, the Grace risk system will issue risk review reminders as follows:

- Red risks – every month
- Amber – every 3 months
- Yellow risks – every 6 months
- Green risks – every 12 months

Risk owners are encouraged to review and update their risks more frequently than this if events occur which means an earlier review is beneficial.

Updates from the strategic risk register will be reported to the Audit Committee at each of their meetings. Strategic risks will also be seen by Cabinet and Budget and Performance Panel for noting.

5 Roles and Responsibilities

To ensure risk management is effectively implemented, all staff and Councillors should have a level of understanding of the Council's risk management approach and regard risk management as part of their responsibilities:

All Colleagues

- Report risk management concerns to their line managers, or in cases where this is not possible, use the online risk reporting form.
- Manage day-to-day risks and opportunities effectively.
- Participate fully in risk workshops and action planning as appropriate.
- Attend training and awareness sessions as requested.

Risk Owners (including project managers)

- Manage day-to-day risks and opportunities effectively and report risk management concerns to their line managers, including escalating any risks with a residual score of amber or red (scoring 8 or above), or risks which are above the Councils risk appetite.
- Promptly escalate high (red) risks to the appropriate Chief Officer.
- Take ownership of the risks they are responsible for by confirming control measures and/or implementing new actions.
- Provide assurance about the management of those risks.
- Update the Grace system as new risks occur, when changes happen to existing risks and when prompted to run a risk review.

Note: The above also applies to colleagues within the shared service (Preston City Council). The Preston risk scoring matrix (3x3) and has been mapped to the Lancaster City Council risk scoring matrix so the risks can be managed and reported on effectively.

Risk Actionees (colleague who have been assigned a risk action)

- Carry out the actions to manage the risk within the agreed timeframe, update the Grace system as needed, including once the action is complete.

Owners of secondary risk registers, such as H&S and Business Continuity

- Review the risk registers they own, updating the central risk register (Grace risk management system) as needed.
- Assist other colleagues in their knowledge and understanding of risk and risk management processes.

Leadership Team / Chief Officers

- Champion an effective Council-wide risk management culture.
- Manage risk in their services by ensuring colleagues are updating their risk registers as required.
- Encourage staff to be open and honest in identifying risks and opportunities.
- In conjunction with the appropriate risk owner, maintain the relevant risk registers ensuring all key risks are identified, managed and reviewed in line with the corporate risk management approach.
- Constructively review and challenge the risks involved in decision making.
- Ensure Councillors receive relevant risk information including discussing significant service risks with the relevant Portfolio Holders.
- Responsible for owning and managing strategic risks, which will be reviewed quarterly or more often when needed.
- Promptly escalate risks, including adding additional strategic risks where a service risk requires escalation.
- Ensure risk management process is an explicit part of all projects.
- Ensure that appropriate resources and importance are allocated to the risk management process.
- Provide assurance that the risks for which they are the risk owner are being effectively managed. This will be completed as part of the Annual Governance review process.
- Ensure that the Council's risk management policy is implemented and followed.

All Councillors

- Support and promote an effective risk management culture.
- Constructively review and scrutinise the risks involved in delivering the Council's core purpose, priorities and outcomes.

Cabinet / Portfolio Holder

- Take a strategic view of risks in the organisation, specifically to:
  - Determine and continuously assess the Councils risk appetite.
  - Review how management is responding to the strategic risks.
  - Consider and challenge the risks involved when making any key decisions.
  - Review operational and projects risks supplied to them in their capacity as portfolio holder.

Audit Committee

- Monitor the effective development and operation of risk management in the Council and monitor progress in addressing risk-related issues reported to the committee.
- Consider the Councils framework of assurance and ensure that it adequately addresses the risks and priorities of the Council.
- Approve the Council's risk management policy statement and strategy, reviewing their effectiveness, to help ensure that risk is appropriately managed.
- Review and challenge the content of the strategic risk register.

Budget and Performance Panel

- Consider risk management issues in reviewing and scrutinising performance (as stated in the panels terms of Reference).

Partners

- Where appropriate, participate in the development of a joint partnership risk register.
- Ensure ownership of each risk is clear.
- Actively manage risk within the partnership, setting a timetable for reviewing risks when the partnership is formed.
- Report on risk management issues to partnership boards or equivalent. It may be necessary to adopt a dual scoring approach, to identify and score risks from more than one perspective.
- Where possible, map your chosen method for managing risks back to the Council's method
- Seek advice from the Lancaster City Council Projects and Performance Team (projects@lancaster.gov.uk) if unclear on risk management and reporting risks.

Projects and Performance Team

- Design and facilitate the implementation of a risk management framework ensuring it meets the needs of the organisation.
- Act as a centre of expertise, providing support, training and guidance as required.
- Act as systems administrators for the Grace risk management system and check that risk owners are updating their assigned risks in accordance with the schedule. Escalating to senior management as required.
- Collate risk information and prepare reports as necessary for Leadership Team and Councillor led committees.

Internal Audit

- Ensure the Internal Audit work plan is focused on the key risks facing the Council.
- During all relevant audits, challenge the content of risk registers to provide assurance that risks are being effectively managed.
- Periodically arrange for the independent review of the Council's risk management process and provide an independent objective opinion on its operation and effectiveness.

6 Embedding Risk Management

For risk management to be effective and a meaningful management tool, it needs to be an integral part of key management processes and day-to-day working. As such, risks and the monitoring of associated actions should be considered as part of the Council's significant business processes, including:

- **Corporate Decision Making** – significant risks, which are associated with policy or action to be taken when making key decisions, are included in appropriate committee reports.

- **Business / budget planning** – this annual process includes updating the relevant risk registers to reflect current aims / outcomes.

- **Project Management** – all significant projects should formally consider the risks to delivering the project outcomes before and throughout the project. This includes risks that could influence service delivery, benefits realisation and engagement with key stakeholders (service users, third parties, partners etc.).

- **Partnership Working** – partnerships should establish procedures to record and monitor risks and opportunities that may impact the Council and/or the partnership's aims and objectives.

- **Procurement** – all risks and actions associated with a purchase need to be identified and assessed, kept under review and amended as necessary during the procurement process.

- **Contract Management** – significant risks associated with all stages of contract management are identified and kept under review

- **Insurance** – the Council's Insurance Officer manages insurable risks and self-insurance arrangements.

- **Health and Safety** – the Council has specific policies and procedures to be followed in relation to health and safety risks. For more information on H&S, please contact: healthandsafety@lancaster.gov.uk.

Appendix 1 – Measures of Likelihood and Impact

Likelihood: Can be measured using Frequency of Probability

Score	Description	Frequency or Probability
5	Almost Certain	Almost certain occurrence /The event is expected to occur in most circumstances / There is a history of very frequent occurrence at the Council or similar organisations **OR** > 80% probability
4	Highly Likely	There is a strong possibility that the event will occur / There is a history of frequent occurrence at the Council or similar organisations **OR** 50-80% probability
3	Possible	The event might occur / There is a history of occurrence at the Council or similar organisations **OR** 20-50% probability
2	Unlikely	Not expected / but there is a moderate possibility it may occur **OR** 5-20% probability
1	Remote	Highly unlikely, but it may occur in exceptional circumstances / It could happen but it is very unlikely **OR** <5% probability

DRAFT

Impact Measures:

Example	Insignificant – 1	Minor – 2	Moderate – 3	Major – 4	Catastrophic – 5
People / Duty of Care	Minor injury	Temporary disability or illness	Permanent disability or major injury	Fatality, multiple serious injuries	Multiple fatalities
Financial Impact	The lesser of <5% or < £10,000 over budget.	The lesser of 5-10% or £10,000 to £50,000 over budget.	The lesser of 11-15% or £50,000 to £250,000 over budget.	The lesser of 16-25% or £250,000 to £1,000,000 over budget.	The lesser of >25% or > £1,000,000 over budget.
Legal and Compliance Impact	No legal proceedings brought against the Council	Minor civil litigation	Low Civil litigation numbers and/or local public enquiry	Significant civil litigation and/or national public enquiry	High significant legal action certain Section 151 or government intervention or criminal charges
Service Impact	No impact on service delivery as temporary capacity / work around in place	Short term service disruption	Noticeable service disruption affecting customers	Significant service failure but not directly affecting vulnerable groups	Serious service failure affecting all customer, including vulnerable groups
Project Delivery	Minor delay to project. Very limited impact on cost or savings. Scope / deliverables of project unaffected.	Minor delay to project, limited impact on cost or savings. Scope / deliverables of project broadly unaffected.	Significant delay to project, significant impact on cost or savings. Scope / deliverables of project affected.	Major delay to project, major impact to cost or savings. Many of the deliverables of the project are not possible.	Project spends allocated funding but fails to deliver any objectives or benefits.
Intervention Required	Limited intervention by Service Manager or Project Manager required	Major intervention by Service Manager or Project Manager	Intervention by Chief Officer	Intervention by the Leadership Team, Chief Exec or Project Board	Intervention by Council, Project Board or external authority / governing body.
Reputation Impact	Little or no media attention	Minor negative local media attention	Significant negative local media attention	Sustained negative local media attention and/or significant regional media attention	Sustained negative national media attention

Appendix 2 - Risk Response Categories

Category	Opportunity or Threat	Description
Accept	Threat	A decision is taken to accept the risk. Management and/or the risk owner make an informed decision to accept that existing actions sufficiently reduce the likelihood and impact of a risk and there is no added value in doing more.
Avoid	Threat	A decision is made not to take a risk. Where the risks outweigh the possible benefits, avoid the risk by doing things differently e.g. revise strategy, revisit objectives or stop the activity.
Fallback	Threat	Put in place a fallback plan for the actions that will be taken to reduce the impact of the threat should the risk occur. This is a reactive form of the 'reduce' response which has no impact on likelihood.
Reduce	Threat	Implement further additional action(s) to reduce the risk by: • minimising the likelihood of an event occurring (e.g. preventative action) and/or • reducing the potential impact should the risk occur (e.g. business continuity plans) Further actions are recorded in the risk register and regularly monitored.
Transfer	Threat	Transfer all or part of the risk through insurance or to a third party e.g. contractor or partner, who is better able to manage the risk. Although responsibility can be transferred, in most cases accountability remains with the Council, so this still needs to be monitored.
Share	Threat or Opportunity	Share is different from the transfer response. It seeks multiple parties, typically within the supply chain, to share the risk on pain/gain share basis.
Enhance	Opportunity	Proactive actions taken to: • Enhance the probability of the event occurring. • Enhance the impact of the event should it occur.
Exploit	Opportunity	Whilst taking action to mitigate risks, a decision is made to exploit a resulting opportunity.
Reject	Opportunity	A conscious and deliberate decision is taken not to exploit or enhance the opportunity, having discerned that it is more economical not to attempt an opportunity response action. The opportunity should continue to be monitored.

Appendix 3 – Risk Appetite

The boxes shaded in yellow, indicate the Council's current risk appetite for each category. The score is the impact x likelihood score as generated at the residual risk stage of the risk management process.

	Risk Appetite				
Risk Category	**Averse Score 1-3**	**Minimal Score 4-6**	**Cautious Score 8-9**	**Open Score 10-12**	**Eager Score 15-25**
Strategy (Cautious, Score 8-9) Risks arising from identifying and pursuing a strategy, which is poorly defined, is based on flawed or inaccurate data or fails to support the delivery of commitments, plans or objectives due to a changing macro-environment (e.g. political, economic, social, technological, environment and legislative change).	Guiding principles or rules in place that limit risk in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 5+ year intervals	Guiding principles or rules in place that minimise risk in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 4-5 year intervals	Guiding principles or rules in place that allow considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 3-4 year intervals	Guiding principles or rules in place that are receptive to considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 2-3 year intervals	Guiding principles or rules in place that welcome considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 1-2 year intervals
Governance (Cautious, Score 8-9) Risks arising from unclear plans, priorities, authorities and accountabilities, and/or ineffective or disproportionate oversight of decision-making and/or performance.	Avoid actions with associated risk. No decisions are taken outside of processes and oversight / monitoring arrangements. Organisational controls minimise risk of fraud, with significant levels of resource focused on detection and prevention.	Willing to consider low risk actions which support delivery of priorities and objectives. Processes, and oversight / monitoring arrangements enable limited risk taking. Organisational controls maximise fraud prevention, detection and deterrence through robust controls and sanctions.	Willing to consider actions where benefits outweigh risks. Processes, and oversight / monitoring arrangements enable cautious risk taking. Controls enable fraud prevention, detection and deterrence by maintaining appropriate controls and sanctions.	Receptive to taking difficult decisions when benefits outweigh risks. Processes, and oversight / monitoring arrangements enable considered risk taking. Levels of fraud controls are varied to reflect scale of risks with costs.	Ready to take difficult decisions when benefits outweigh risks. Processes, and oversight / monitoring arrangements support informed risk taking. Levels of fraud controls are varied to reflect scale of risk with costs.
Operations (Open, Score 10-12) Risks arising from inadequate, poorly designed or ineffective/ inefficient internal processes resulting in fraud, error, impaired customer service (quality and/or quantity of service), non-compliance and/or poor value for money.	Defensive approach to operational delivery - aim to maintain/protect, rather than create or innovate. Priority for close management controls and oversight with limited devolved authority.	Innovations largely avoided unless essential. Decision making authority held by senior management.	Tendency to stick to the status quo, innovations generally avoided unless necessary. Decision making authority generally held by senior management. Management through leading indicators.	Innovation supported, with clear demonstration of benefit / improvement in management control. Responsibility for non-critical decisions may be devolved.	Innovation pursued – desire to 'break the mould' and challenge current working practices. High levels of devolved authority – management by trust / lagging indicators rather than close control.
Legal (Cautious, Score 8-9) Risks arising from a defective transaction, a claim being made (including a defence to a claim or a counterclaim) or some other legal event occurring that results in a liability or other loss, or a failure to take appropriate measures to meet legal or regulatory requirements or to protect assets (for example, intellectual property).	Play safe and avoid anything which could be challenged, even unsuccessfully.	Want to be very sure we would win any challenge.	Want to be reasonably sure we would win any challenge.	Challenge will be problematic; we are likely to win, and the gain will outweigh the adverse impact.	Chances of losing are high but exceptional benefits could be realised.
Property (Open, Score 10-12) Risks arising from property deficiencies or poorly designed or ineffective/ inefficient safety management resulting in non-compliance and/or harm and suffering to employees, contractors, service users or the public.	Obligation to comply with strict policies for purchase, rental, disposal, construction, and refurbishment that ensures producing good value for money	Recommendation to follow strict policies for purchase, rental, disposal, construction, and refurbishment that ensures producing good value for money.	Requirement to adopt arrange of agreed solutions for purchase, rental, disposal, construction, and refurbishment that ensures producing good value for money.	Consider benefits of agreed solutions for purchase, rental, disposal, construction, and refurbishment that meeting organisational requirements.	Application of dynamic solutions for purchase, rental, disposal, construction, and refurbishment that ensures meeting organisational requirements.
Financial (Cautious, Score 8-9) Risks arising from not managing finances in accordance with requirements and financial constraints resulting in poor returns from	Avoidance of any financial impact or loss, is a key objective.	Only prepared to accept the possibility of very limited financial impact if essential to delivery.	Seek safe delivery options with little residual financial loss only if it could yield upside opportunities.	Prepared to invest for benefit and to minimise the possibility of financial loss by managing the risks to tolerable levels.	Prepared to invest for best possible benefit and accept possibility of financial loss (controls must be in place).

DRAFT

investments, failure to manage assets/liabilities or to obtain value for money from the resources deployed, and/or non-compliant financial reporting.					
Commercial (Open, Score 10-12) Risks arising from weaknesses in the management of commercial partnerships, supply chains and contractual requirements, resulting in poor performance, inefficiency, poor value for money, fraud, and/or failure to meet business requirements/objectives.	Zero appetite for untested commercial agreements. Priority for close management controls and oversight with limited devolved authority.	Appetite for risk taking limited to low scale procurement activity. Decision making authority held by senior management.	Tendency to stick to the status quo, innovations generally avoided unless necessary. Decision making authority generally held by senior management. Management through leading indicators.	Innovation supported, with demonstration of benefit / improvement in service delivery. Responsibility for non-critical decisions may be devolved.	Innovation pursued – desire to 'break the mould' and challenge current working practices. High levels of devolved authority – management by trust / lagging indicators rather than close control.
People (Cautious, Score 8-9) Risks arising from ineffective leadership and engagement, suboptimal culture, inappropriate behaviours, the unavailability of sufficient capacity and capability, industrial action and/or non-compliance with relevant employment legislation/HR policies resulting in negative impact on performance.	Priority to maintain close management control & oversight. Limited devolved authority. Limited flexibility in relation to working practices. Development investment in standard practices only	Decision making authority held by senior management. Development investment generally in standard practices.	Seek safe and standard people policy. Decision making authority generally held by senior management.	Prepared to invest in our people to create innovative mix of skills environment. Responsibility for noncritical decisions may be devolved.	Innovation pursued – desire to 'break the mould' and challenge current working practices. High levels of devolved authority – management by trust rather than close control.
Technology (Open, Score 10-12) Risks arising from technology not delivering the expected services due to inadequate or deficient system/ process development and performance or inadequate resilience.	General avoidance of systems / technology developments.	Only essential systems / technology developments to protect current operations.	Consideration given to adoption of established / mature systems and technology improvements. Agile principles are considered.	Systems / technology developments considered to enable improved delivery. Agile principles may be followed.	New technologies viewed as a key enabler of operational delivery. Agile principles are embraced.
Data Info and Management (Cautious, Score 8-9) Risks arising from a failure to produce robust, suitable and appropriate data/ information and to exploit data/information to its full potential.	Lock down data & information. Access tightly controlled, high levels of monitoring.	Minimise level of risk due to potential damage from disclosure.	Accept need for operational effectiveness with risk mitigated through careful management limiting distribution.	Accept need for operational effectiveness in distribution and information sharing.	Level of controls minimised with data and information openly shared.

Security (Cautious, Score 8-9) Risks arising from a failure to prevent unauthorised and/or inappropriate access to the estate and information, including cyber security and non-compliance with General Data Protection Regulation requirements.	No tolerance for security risks causing loss or damage to HMG property, assets, information or people. Stringent measures in place, including: • Adherence to FCDO travel restrictions • Staff vetting maintained at highest appropriate level • Controls limiting staff and visitor access to information, assets and estate • Access to staff personal devices restricted in official sites * FCDO = Foreign, Commonwealth and Development Office	Risk of loss or damage to HMG property, assets, information or people minimised through stringent security measures, including: • Adherence to FCDO travel restrictions • All staff vetted levels defined by role requirements. • Controls limiting staff and visitor access to information, assets and estate • Staff personal devices permitted, but may not be used for official tasks	Limited security risks accepted to support business need, with appropriate checks and balances in place: • Adherence to FCDO travel restrictions • Vetting levels may flex within teams, as required • Controls managing staff and limiting visitor access to information, assets and estate • Staff personal devices may be used for limited official tasks with appropriate permissions.	Considered security risk accepted to support business need, with appropriate checks and balances in place: • New starters may commence employment at risk, following partial completion of vetting processes • Permission may be sought for travel within FCDO restricted areas. • Controls limiting visitor access to information, assets and estate. • Staff personal devices may be used for official tasks with appropriate permissions.	Organisational willing to accept security risk to support business need, with appropriate checks and balances in place: • New starters may commence employment at risk, following partial completion of vetting processes • Travel permitted within FCDO restricted areas. • Controls limiting visitor access to information, assets and estate. • Staff personal devices permitted for official tasks.
Project / Programme (Open, Score 10-12) Risks that change programmes and projects are not aligned with strategic priorities and do not successfully and safely deliver requirements and intended benefits to time, cost and quality.	Defensive approach to transformational activity - aim to maintain/protect, rather than create or innovate. Priority for close management controls and oversight with limited devolved authority. Benefits led plans fully aligned with strategic priorities, functional standards.	Innovations avoided unless essential. Decision making authority held by senior management. Benefits led plans aligned with strategic priorities, functional standards.	Tendency to stick to the status quo, innovations generally avoided unless necessary. Decision making authority generally held by senior management. Plans aligned with strategic priorities, functional standards.	Innovation supported, with demonstration of commensurate improvements in management control. Responsibility for noncritical decisions may be devolved. Plans aligned with functional standards and organisational governance.	Innovation pursued – desire to 'break the mould' and challenge current working practices. High levels of devolved authority – management by trust rather than close control. Plans aligned with organisational governance.