LANCASTER CITY COUNCIL

Promoting City, Coast & Countryside

Risk Management Policy and Procedure

March 2024

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

Due for review every 2 years.

1.0 Introduction

1.1 Risk is unavoidable and is part of all our lives. As an organisation, we need to take risks to grow and develop. Risk management involves understanding, analysing and addressing risks to make sure the organisation achieves its objectives. Successful risk management can make a council more flexible and responsive to new pressures and external demands. It allows an organisation to deliver services better and to meet the needs and expectations of its community in what is a fast changing and dynamic environment. The benefits of successful risk management include improved service delivery, financial performance and corporate governance.

1.2 This policy explains Lancaster City Council's approach to risk management and the framework that will operate to establish and drive an effective system not only to minimise risk but also to enable continuous improvement at every level of the organisation.

2.0 Scope

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

2.2 This policy will be reviewed every two years to take account of changing legislation, government initiatives, best practice and experience gained within the council.

3.0 Risk Management Objectives

3.1 The council has identified a number of key risk management objectives that need to be met to ensure a robust risk management framework is embedded across the council, namely:

- Adopt a strategic approach to risk management to make better informed decisions which is vital to successful transformational change.
- Set the 'tone from the top' on the level of risk we are prepared to accept on our different service delivery activities and ambitions.
- Acknowledge that even with good risk management and our best endeavours, things can go wrong. Where this happens, we use the lessons learned to try to prevent it from happening again.
- Develop leadership capacity and skills in identifying, understanding and managing the risks facing the council.
- Integrate risk management into how we run council business/services. Robust risk management processes help us to achieve our core purpose, ambitions and outcomes.
- Support a culture of well-measured risk taking throughout the council's business. This includes setting risk ownership and accountabilities and responding to risk in a balanced way, considering the level of risk, reward, impact and cost of control measures.
- Ensure that the council continues to meet all statutory and best practice requirements in relation to risk management.

- Ensure risk management continues to be a key and effective element of our Corporate Governance arrangements.

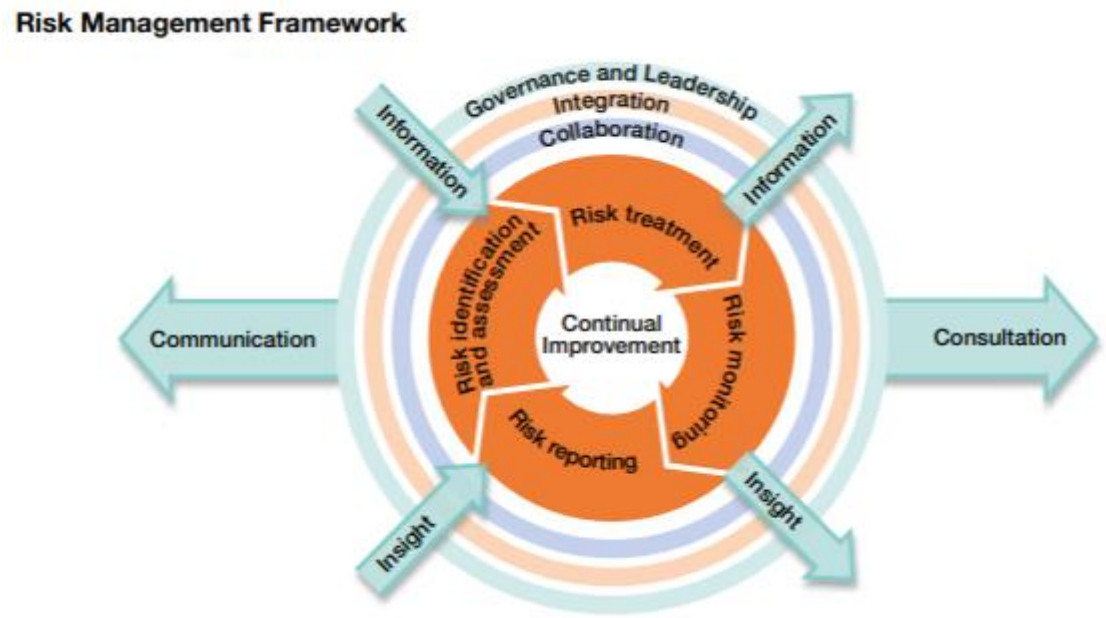


Figure 1 - Taken from HMT The Orange Book, Management of Risk - Principles and Concepts

Figure 1 shows a risk management framework. Working from the outer rings inwards it shows:

- Green ring – Risk management is an essential part of governance and leadership.
- Peach ring – Risk management is an integral part of all organisational activities to support decision-making in achieving objectives.
- Blue ring – Risk management is collaborative and informed by the best available information and expertise.
- Orange ring – process are in place to include:
    - Risk identification and assessment to determine and prioritise how the risks should be managed.
    - Selection, design and implementation of risk treatment options that support achievement of intended outcomes and manage risks to an acceptable level.
    - Design and operation of integrated, insightful and informative risk monitoring.
    - Timely, accurate and useful risk reporting to enhance the quality of decision-making and to support management and oversight bodies in meeting their responsibilities.
- General principle - Risk management will be continually improved through learning and experience.

4.0 Benefits

4.1 In addition to supporting strategic and operational business planning, if risk management is thoroughly embedded and practices are consistently applied it can bring a number of other key benefits to the organisation, namely:

- Improved service delivery and financial performance, supporting the effective use of the council's resources.
- Improved decision making and budgeting.
- Continuous service improvement.
- Enhanced communication between staff, Councillors, and partners.

5.0 Definitions

5.1 Risk can be defined as:

> *"An uncertain event that, should it occur, will have an effect on the council's objectives and/or reputation. It is the combination of the probability of an event (likelihood) and its effect (impact)."*

Risk management can be defined as:

> *"The systematic application of principles, approach and processes to the identification, assessment and management of risks."*

5.2 By managing our 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.

5.3 Risk management is applied at all levels of service delivery across the council. The council separates risk into three categories:

Corporate Strategic Risks – Risks that could influence the successful achievement of our long-term core purpose, priorities and outcomes. These are risks that could potentially have a council-wide impact and/or risks that cannot be managed solely at a service level because higher level support/intervention is needed.

Operational / Service Risks – Risks that could influence the successful achievement of the service or business outcomes / objectives. Potentially these risks could have a significant financial, reputational and/or service delivery impact on the business unit as a whole.

Project Risks – For strategic projects these registers will include risks relating to the completion of the project. These will be included within Grace once the project has been agreed and any external funding accepted. For smaller projects the risk may be included in the services risk register with the project risk type recorded against the risk. However, for projects managed by an external organisation it is accepted that risks registers may need to be held outside of the Grace system, ensuring that alternative monitoring arrangements are in place.

6.0 Risk Management Standards

6.1 Several standards have been developed worldwide to help organisations implement risk management systematically and effectively. These standards seek to establish a common view on frameworks, processes and practice, and are generally set by recognised international standards bodies or by industry groups.

6.2 Despite the publication of the global risk management standard in 2009; ISO 31000, the Institute of Risk Management (IRM) has decided to retain its support for the original 'Risk Management Standard' that was published in 2002 because it is a simple guide that outlines a practical and systematic approach to the management of risk. The standard is not prescriptive i.e. a box ticking exercise or a certifiable process. Instead, the standard represents best practice against which organisations can measure themselves. The council has reviewed this policy against this standard.

6.3 The HM Treasury Orange Book standard for risk categories and risk appetite has been adopted by the council as best practice. It sets out the council's risk appetite across a number of different risk categories. Further information on this can be found in "Section 8 – Risk Management" of this policy.

7.0 Risk Management Approach

7.1 The purpose of the risk management approach outlined in this policy is to:

- Provide standard definitions and language to underpin the risk management process.
- Ensure risks are identified and assessed consistently throughout the organisation through the clarification of key concepts.
- Clarify roles and responsibilities for managing risk.
- Implement an approach that meets current legislative requirements and follows best practice and relevant standards.

7.2 Before we can identify our risks, we need to establish the context by looking at what we are trying to achieve and what our proposed outcomes are. Depending on the area under review, the relevant objectives and outcomes will usually be detailed in existing documents, e.g., council plan, individual services plans, project briefs, partnership agreements etc.

To ensure consistency, the following four steps should be followed when identifying, evaluating, treating / mitigating and reviewing risks:

Step 1 – Identifying risks

Risk identification should be approached in a methodical way to ensure that all significant activities within the organisation have been identified and all risks flowing from these activities have been defined. Many risks will be identified as part of the routine service planning stages where barriers to specific business objectives can easily be recognised. All staff have a duty to report emerging risks to their Chief Officer / Manager as and when they are identified. Risks can arise and be identified when the following events occur:

- the change of internal or external processes
- staff/councillors leave and/or restructuring takes place
- through procurement of a new supplier or asset
- partners change or are re-structured
- legislation is revised or introduced
- the social and or economic climate alters
- new projects are undertaken
- an incident occurs

To help in the risk identification process some common risk assessment techniques/methods can be used, for example, questionnaires, checklists, workshops, brainstorming sessions, audits and inspection reports or flowcharts.

Each identified risk will sit within one primary risk category. Our categories are taken from the HM Treasury "Orange Book Risk Appetite Guidance Note". The categories are listed in the table below. Full details and definitions can be found in Appendix 3 - Risk Appetite.

Strategy	Property	Technology
Governance	Financial	Data Info and Management
Operations	Commercial	Security
Legal	People	Project / Programme

When describing risks, it helps to display the identified risk in a structured format to ensure a comprehensive risk identification, description and assessment process takes place. The Grace system prompts the risk owner to do this.

Once identified, all risks are recorded in the appropriate 'Risk Register' on the Grace risk management system. Risks recorded in the register should be given a unique identifier. A risk owner must be allocated and recorded against each risk on the risk register. Such accountability helps to ensure 'ownership' of the risk is documented and recognised. A risk owner is defined as a person with the accountability and authority to effectively manage the risk. At this stage there may well be a long list of possible risks. The next step will help to prioritise these in order of importance.

Step 2 – Analysing and Evaluating risk

To analyse and evaluate risks, a thorough risk assessment needs to 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.

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 (Table 1). Where the likelihood and impact cross, determines the risk level.

For example, a Likelihood of 2 (possible) and a Very High Impact of 4 would result in a risk level of 8.

Table 1

Impact	Unlikely - 1	Possible - 2	Likely - 3	Very Likely - 4
Very High - 4	4	8	12	16
High - 3	3	6	9	12
Medium - 2	2	4	6	8
Low - 1	1	2	3	4

Likelihood

A "traffic light" approach is used to show high (red), medium (amber) and low (green) risks. It is important to note that different businesses use different models, therefore it is not always possible to compare our risks directly with those of other councils or businesses.

First Risk Score – Inherent (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 Risk Score

Risks are then re-scored 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.

Comparing the residual risk score to the guidance on risk appetite for the appropriate risk category will be the deciding factor as to whether further action is required (see the guidance on risk appetite in appendix 3). It is at this point that a risk response category is assigned by the risk owner to determine what, if any, action is to be taken e.g. reduce or accept the level of risk. (See appendix 2 for further information on risk response categories).

Third Risk Score – Target Risk (Retained Risk) Score

If a risk requires further mitigating action to reduce the risk score to within the recommended risk appetite, the risk owner needs to set a realistic target score and develop an action plan which when implemented will reduce the risk to within the target risk score. It is important to note, that for many risks a target score of 1, will be too low, due to budget, time or resource restrictions.

Step 3 – Treatment and Action Planning

Actions, which will help to minimise the likelihood and / or impact of the risk occurring, are identified where the risk score needs to be reduced further. One or more action plan owners should be identified for each action.

Net risks are prioritised by applying the same criteria and matrix used for assessing the gross risk level (Step 2). It is the risk owner's responsibility to ensure that the agreed net risk level for each risk is an accurate reflection of the likelihood and impact measures detailed in Appendix 1.

Not all risks can be managed all of the time, so having assessed and prioritised the identified risks, cost effective action needs to be taken to manage those that pose the most significant threat.

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.

Step 4 – Management and Reporting

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 senior managers and Councillors to have greater awareness of the extent of the risks and progression being made to manage them. 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 3 months
- Amber 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 mean an earlier review is beneficial.

In addition, quarterly reminders will be sent to Chief Officers / Managers asking them to consider / add newly identified risks to the system throughout the course of the year.

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.

8.0 Risk Appetite

8.1 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.

8.2 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.

9.0 Risk Registers

9.1 To ensure that the risk registers are comprehensive and accurately reflect the levels of risk within the council, all relevant and available sources of information will be used in their compilation and review, namely:

- The council's Annual Governance Statement
- Internal audit reports
- External audit reports
- Committee reports / portfolio holder / officer delegation reports
- Risk Assessments
- Incident / accident reports
- Insurance claims and advice from the council's Insurers
- Complaints
- Any relevant articles from risk management publications

9.2 Colleagues within the Policy and Performance Team (People and Policy Service) will oversee administration of both strategic and operational risk registers within the Grace Risk Management system. Identified risk owners will ultimately be responsible for monitoring and updating their risk scores and actions plans.

9.3 The Grace system will automatically send risk owners a weekly email reminder of any overdue risk reviews and overdue actions, and the Policy and Performance team will monitor risk movements 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 Policy 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.

10.0 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 Employees

- Manage day to day risks and opportunities effectively and report risk management concerns to their line managers.
- Participate fully in risk workshops and action planning as appropriate.
- Attend training and awareness sessions as appropriate.

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

- Take a strategic view of risks in the organisation, specifically to:
    - Determine and continuously assess the risk appetite.
    - Review how management is responding to the principal risks.
    - Consider and challenge the risks involved in making any 'key decisions'.

Audit Committee

- Provide independent assurance to the council on the overall adequacy of the risk management framework, including review of proposed amendments to the Risk Management Policy prior to its presentation to Cabinet.
- Consider the Councils framework of assurance and ensure that it adequately addresses the risks and priorities of the Council.
- Monitor the effective development and operation of risk management in the council and monitor progress in addressing risk-related issues reported to the committee.
- Review and challenge the content of the strategic risk register.
- Approve and review recommendations and amendments to the Risk Management Policy.

Budget and Performance Panel

- Consider risk management issues in reviewing and scrutinising performance.

Leadership Team / Chief Officers

- Champion an effective council-wide risk management culture.
- Risk manage their services in delivering the council's core purpose, priorities and outcomes. Ensuring colleagues are updating their risk registers as required.
- 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 appropriately, including adding additional strategic risks where a service risk requires escalation.
- Encourage staff to be open and honest in identifying risks and opportunities.
- Ensure risk management process is an explicit part of transformation and all significant 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.

Risk Owners

- Take ownership of the risks they are responsible for by confirming control measures and/or implementing new actions.
- Promptly escalate risks to the appropriate Chief Officer.

Partners

- Where appropriate, participate in the development of a joint partnership risk register.
- Actively manage risk within the partnership.
- Report on risk management issues to partnership boards or equivalent.

Project Managers

- Ensure that the risks associated with their projects are identified, recorded and regularly reviewed as part of the project management process.
- Provide assurance about the management of those risks.

- Promptly escalate risks in an appropriate way.

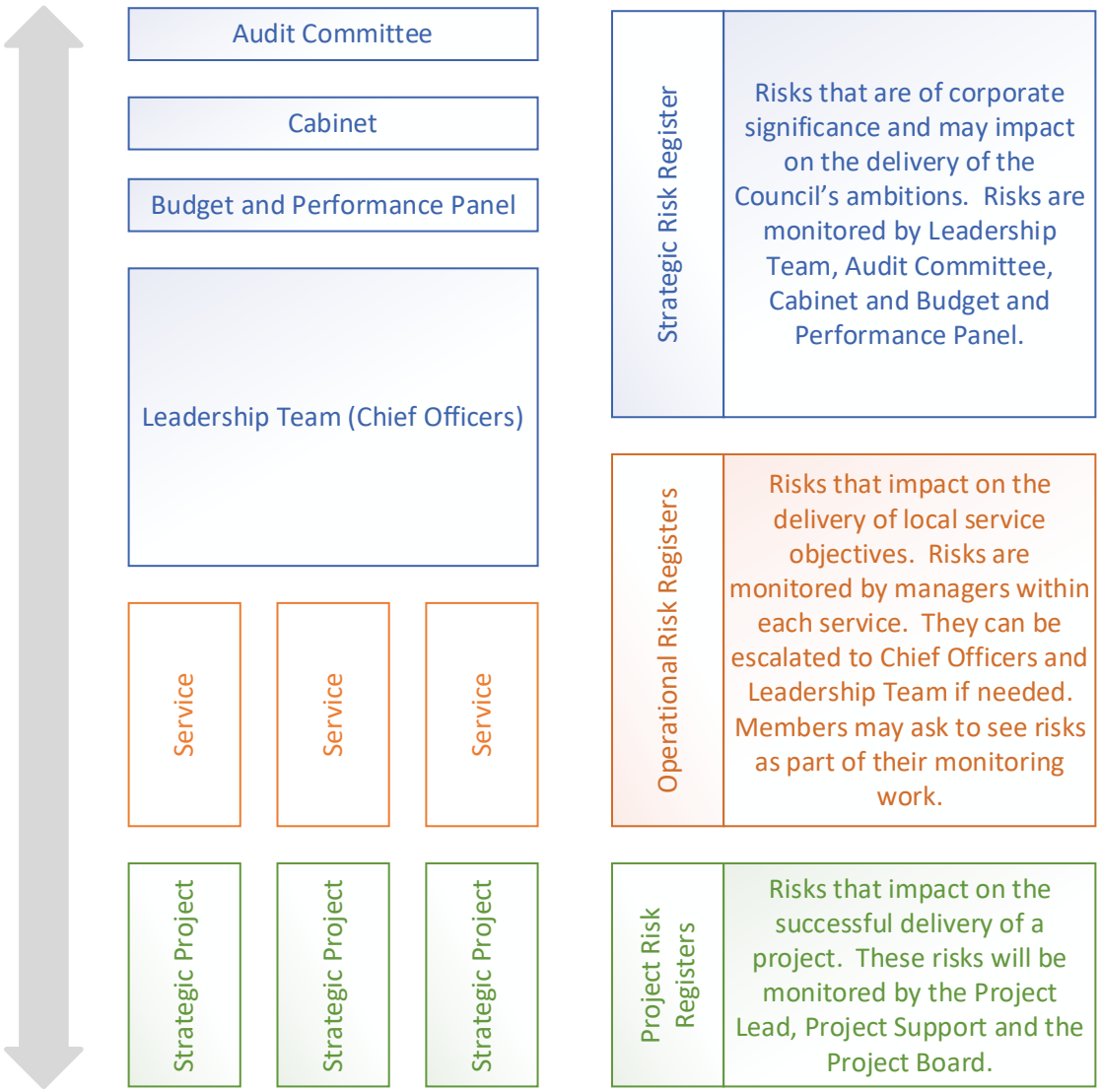
Policy and Performance Team (part of the People and Policy service)

- 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 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 lead 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.

Risk Management at Lancaster City Council



11.0 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.

12.0 Culture

The council will be open in its approach to managing risks and will seek to avoid a blame culture. Lessons from events that lead to loss or reputational damage will be shared as well as lessons from things that go well. Discussion on risk in any context will be conducted in an open and honest manner.

13.0 Training and Awareness

Having documented a robust approach and established clear roles and responsibilities and reporting lines, it is important to provide officers and Councillors with the knowledge and skills necessary to enable them to manage risk effectively. Colleagues within the Policy and Performance team will act as administrators for the council's Grace risk management system and will provide advice and arrange training for colleagues and Councillors as required.

14.0 Summary

This policy and the ongoing efforts to embed sound risk management principles into the council's 'fabric' will improve the way in which services are delivered. A solid, well-documented and comprehensive approach to risk management and its adoption into the decision-making process is good practice, essential to good management and strengthens the council's governance framework.

Appendix 1 – Measures of Likelihood and Impact

Table 1

Impact					
	Very High – 4	**4**	**8**	**12**	**16**
	High – 3	**3**	**6**	**9**	**12**
	Medium – 2	**2**	**4**	**6**	**8**
	Low – 1	**1**	**2**	**3**	**4**
		Unlikely – 1	**Possible – 2**	**Likely – 3**	**Very Likely – 4**

Likelihood

Likelihood Measures

	Unlikely - 1	**Possible - 2**	**Likely - 3**	**Very Likely - 4**
Probability	**Less than 10%** chance of circumstances arising	**10% to 40%** chance of circumstances arising	**41% to 75%** chance of circumstances arising	**More than 75%** chance of circumstances arising
Timescale	Is **unlikely** to occur.	Possible in the **next 3 or more years**.	Likely to occur in the **next 1-2 years**.	Occurred in the **past year** or is very likely to occur in the **next year**.

Impact Measures

Example	Low - 1	Medium - 2	High - 3	Very High - 4
People / Duty of Care	Low level of foreseeable minor injuries	High level of foreseeable minor injuries Low level of foreseeable serious injuries	High level of foreseeable severe injuries	Foreseeable long-term injury, illness
Financial Impact	Less than 5% over budget	5-10% over budget	11-25% over budget	More than 25% over budget
Legal Impact	Minor civil litigation	Major civil litigation and/or local public enquiry	Major civil litigation and/or national public enquiry	Legal action certain Section 151 or government intervention or criminal charges
Service Impact	Short term service disruption	Noticeable service disruption affecting customers	Significant service failure but not directly affecting vulnerable groups	Serious service failure directly affecting vulnerable groups
Project Delivery	Minor delay to project	Significant delay to project	Project fails to deliver target impacting on the service performance	Project fails to deliver target impacting on council's performance
Intervention Required	Intervention by Service Manager, Project Manager or equivalent	Intervention by Chief Officer or equivalent.	Intervention by the Executive or Board	Intervention by Board or Council
Reputation Impact	Short term negative local media attention	Significant negative local media attention	Sustained negative local media attention and/or significant national 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)**	**Cautious (Score 6-8)**	**Open (Score 9)**	**Eager (Score 12-16)**
Strategy (Cautious, Score 6-8) 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 6-8) 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 9) 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 6-8) 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 9) 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 6-8) Risks arising from not managing finances in accordance with requirements and financial constraints resulting in poor returns from investments, failure to manage assets/liabilities or to obtain value for money from the resources deployed, and/or non-compliant financial reporting.	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).
Commercial (Open, Score 9) Risks arising from weaknesses in the management of commercial partnerships, supply chains and contractual requirements, resulting in poor performance, inefficiency, poor value for	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	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

money, fraud, and/or failure to meet business requirements/objectives.			senior management. Management through leading indicators.		indicators rather than close control.
People (Cautious, Score 6-8) 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 9) 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 6-8) 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 6-8) 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	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 9) 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.