Carlisle City Council
Report to Audit Committee

Report details

Meeting Date:	8 December 2022
Portfolio:	Finance, Governance and Resources
Key Decision:	Not applicable
Policy and Budget Framework	YES
Public / Private	Public
Title:	Internal Audit Report – Risk Management
Report of:	Corporate Director Finance & Resources
Report Number:	RD47/22

Purpose / Summary:
This report supplements the report considered on Internal Audit Progress 2022/23 and considers the risk-based Internal Audit review of Risk Management.

Recommendations:
The Committee is requested to

(i) receive the final audit report outlined in paragraph 1.1;

Tracking

Executive:	Not applicable
Scrutiny:	Not applicable
Council:	Not applicable

1. Background

1.1. An audit of Risk Management was undertaken by Internal Audit in line with the agreed Internal Audit plan for 2022/23. The audit (Appendix A) provides reasonable assurances and includes 1 high and 3 medium-graded recommendations.

2. Risks

2.1 Findings from the individual audits will be used to update risk scores within the audit universe. All audit recommendations will be retained on the register of outstanding recommendations until Internal Audit is satisfied the risk exposure is being managed.

3. Consultation

3.1 Not applicable

4. Conclusion and reasons for recommendations

4.1 The Committee is requested to

i) receive the final audit report outlined in paragraph 1.1

5. Contribution to the Carlisle Plan Priorities

5.1 To support the Council in maintaining an effective framework regarding governance, risk management and internal control which underpins the delivery the Council's corporate priorities and helps to ensure efficient use of Council resources

Contact details:

Contact Officer: Michael Roper Ext: 7520

Appendices attached to report:

- **Internal Audit Report – Risk Management– Appendix A**

Note: in compliance with section 100d of the Local Government Act 1972 the report has been prepared in part from the following papers:

- None

Corporate Implications:

Legal - In accordance with the terms of reference of the Audit Committee, Members must consider summaries of specific internal audit reports. This report fulfils that requirement
Property Services - None
Finance – Contained within report
Equality - None
Information Governance- None

CARLISLE CITY COUNCIL

www.carlisle.gov.uk

Audit of Risk Management

Draft Report Issued: 3rd November 2022
Director Draft Issued: 10th November 2022
Final Report Issued: 21st November 2022

Audit Report Distribution

Client Lead:	Chief Executive's Office Manager
Chief Officer:	Deputy Chief Executive Chief Executive
Others:	Corporate Director of Finance and Resources Corporate Director of Economic Development Corporate Director of Governance and Regulatory Services
Audit Committee:	The Audit Committee, which is due to be held on 8th December 2022 will receive a copy of this report.

Note: Audit reports should not be circulated wider than the above distribution without the consent of the Designated Head of Internal Audit.

1.0 Background

1.1. This report summarises the findings from the audit of Risk Management. This was an internal audit review included in the 2022/23 risk-based audit plan agreed by the Audit Committee on 23rd March 2022.

1.2. Risk management is the planned and systematic approach to identifying, evaluating and controlling risk. Its objectives are to secure Council assets and to help ensure continual financial and organisational well-being.

1.3. The Council's Financial Procedure Rules and Risk Management Assurance Framework provide direction on Council risk management arrangements. The Framework's strategic aim is to establish sustainable and effective risk management arrangements that identify, assess, control and manage major risks to the Council's objectives.

2.0 Audit Approach

Audit Objectives and Methodology

2.1 Compliance with the mandatory Public Sector Internal Audit Standards requires that internal audit activity evaluates the exposures to risks relating to the organisation's governance, operations and information systems.

2.2 A risk-based audit approach has been applied which aligns to the five key audit control objectives (see section 4). Detailed findings and recommendations are reported within section 5 of this report.

Audit Scope and Limitations.

2.3 The Client Lead for this review was Chief Executive's Office Manager and the agreed scope was to provide independent assurance over management's arrangements for ensuring effective governance, risk management and internal controls of the following risks:

- Risk Management Assurance Framework is inaccurate, incomplete and does not align to other relevant corporate guidance or best practice
- Risk is not managed in line with the Risk Management Assurance Framework
- Risk is not reviewed in a timely and transparent manner
- Council's risk management approach is not subject to continuous improvement

2.4 There were no instances whereby the audit work undertaken was impaired by the availability of information.

3.0 Assurance Opinion

3.1 Each audit review is given an assurance opinion intended to assist Members and Officers in their assessment of the overall governance, risk management and internal control frameworks in place. There are 4 levels of assurance opinion which may be applied (See **Appendix C** for definitions).

3.2 From the areas examined and tested as part of this audit review, we consider the current controls operating within Risk Management provide **reasonable assurance**.
Note: as audit work is restricted by the areas identified in the Audit Scope and is primarily sample based, full coverage of the system and complete assurance cannot be given to an audit area.

4.0 Summary of Recommendations, Audit Findings and Report Distribution

4.1 There are two levels of audit recommendation; the definition for each level is explained in **Appendix D**. Audit recommendations arising from this audit review are summarised below:

Control Objective	High	Medium
1. **Management** - achievement of the organisation's strategic objectives achieved (see section 5.1)	1	3
2. **Regulatory** - compliance with laws, regulations, policies, procedures and contracts (N/A)	-	-
3. **Information -** reliability and integrity of financial and operational information (see section 5.2)	-	-
4. **Security** - safeguarding of assets (N/A)	-	-
5. **Value** – effectiveness and efficiency of operations and programmes (see section 5.3)	-	-
Total Number of Recommendations	**1**	**3**

4.2 Management response to the recommendations, including agreed actions, responsible manager and date of implementation are summarised in Appendix A. Advisory comments to improve efficiency and/or effectiveness of existing controls and process are summarised in Appendix B for management information.

4.3 **Findings Summary (good practice / areas for improvement):**
The Corporate Risk Management Group (CRMG) and Risk Management Sub-Group (RMSG) have met recently with minutes recorded and actions assigned, although the CRMG did not meet between March 2021 and September 2022 and the RMSG did not meet between July 2021 and August 2022 to review Council risk.

The Transformation Board which oversees major Council Projects has not met for a significant length of time. In lieu of a formal Corporate risk review in February 2022, and prior to submission of a twice-yearly risk report to Scrutiny, comments and observations were requested from Group members.

There is a clear, recent example where the Council's risk management arrangements have not identified a major project with escalating risks. This has resulted in a single high-level recommendation.

The Risk Management Task and Finish Group has an opportunity to use recommendations from the Zurich Municipal report and this audit, to influence the development of a robust Unitary Authority risk management process.

Comment from the Deputy Chief Executive:

Thank you for the helpful recommendations contained in this report. We will address these through our Corporate and Operational Risk Management groups.

We accept the comments made concerning the frequency of meetings between the group, but would also like to note that our ongoing, everyday relationships between group members have also given us the opportunity to monitor risks and escalate any that may have required management attention.

5.0 Audit Findings & Recommendations

5.1 Management – Achievement of the organisation's strategic objectives

5.1.1 The Financial Procedure Rules in the Council's Constitution detail that a monitoring process regularly reviews the effectiveness of risk reduction strategies and the operation of these controls. The Financial Procedure Rules also require that the risk management process is conducted on a continuing basis.

5.1.2 Responsibility for monitoring delivery of the Risk Management Assurance Framework sits with the Corporate Risk Management Group (CRMG). The CRMG are also responsible for continual review of the Council's Corporate Risk Register.

5.1.3 The CRMG met recently in September 2022. Minutes were recorded, actions were assigned to individuals and a full review of the Corporate Risk Register was undertaken. The Risk Management Assurance Framework alludes to a quarterly meeting requirement for the CRMG, although archived minutes indicated that the previous formal CRMG meeting was held some 17 months earlier in March 2021.

5.1.4 Significant risks to Council objectives during the group's hiatus include the global pandemic, Local Government Reorganisation and major Council projects. If a full review of the Corporate Risk Register is not carried out on a continuing basis, the likelihood that informed decisions are being taken on escalating risks, is significantly reduced.

5.1.5 In lieu of a formal Corporate risk review in February 2022, and prior to submission of a twice-yearly risk report to Scrutiny, comments and observations were requested from Group members, although only one email response has been verified.

5.1.6 The reduction in formal Corporate risk reviews is mitigated to an extent through having a small and experienced Senior Management Team, although regular, formal, recorded corporate risk reviews are recommended.

5.1.7 The Risk Management Assurance Framework details that the CRMG provides twice yearly reports to Scrutiny. It is noted that while CRMG was not meeting on a regular basis during 2021, only one report was provided to Scrutiny.

Recommendation 1 – Corporate Risk Management Group to formally review and agree the Corporate Risk Register on a continuing basis, in line with the Council's Financial Procedure Rules.

5.1.8 The Risk Management Sub-Group (RMSG) met recently in August 2022. Minutes were recorded and actions assigned to individuals. The Risk Management Assurance Framework details that the Group meets on a 4 to 6 weekly basis. Archived minutes indicate that the previous meeting was held some 12 months earlier in July 2021.

5.1.9 Historically, the RMSG has carried out a detailed review of individual operational risk registers on a cyclical basis, demonstrating continual improvement. Standing agenda items also included Insurance, Audit, Safety, Health and Environment Risks.

5.1.10 The Risk Management Assurance Framework details that it is the Corporate Risk Management Group's responsibility to monitor delivery of the Framework. Historically, minutes of the RMSG have been reviewed by the CRMG to verify the effectiveness of the RMSG. Due to the reduction in formal meetings of both groups, the review was not undertaken between March 2021 and September 2022.

Recommendation 2 – Corporate Risk Management Group to formally review and agree the effectiveness of the Risk Management Sub-Group, on a continuing basis.

5.1.11 The Risk Management Assurance Framework details that project risks should be reviewed by the wider project team. The Council's Risk Officer regularly contacts major Council Project Managers to ask if there are any escalating project risks. It is advised that in addition, management may wish to consider seeking demonstratable evidence that project risks have been regularly reviewed by wider project teams.

5.1.12 The Risk Management Assurance Framework details that project risks fall within the remit of the Transformation Board. Audit were informed that the Transformation Board has not met for a considerable length of time. Minutes of the last meeting held were not available. The reduction in oversight arrangements has significantly increased the risk that major project risks could escalate with Senior Management unaware. There is a very clear, recent example where the Transformation Board was unable to make informed decisions on escalating major project risks because it was in hiatus and the Council's risk management arrangements had not identified that the project required Senior Management intervention. This significantly increased the risk of both financial loss and reputational damage to the Council.

5.1.13 It is noted that there is limited Project risk management direction available in either the Risk Management Assurance Framework or Project Managers' Handbook.

5.1.14 A risk management task and finish group has been set up to aid the transition of risk management arrangements ready for Local Government Reorganisation vesting day and beyond. The Group may wish to consider further robust direction for Unitary Authority projects including review regularity, evidence of wider project team review and clear oversight/ reporting arrangements to evidence that Council project risk management is working effectively.

Recommendation 3 – Corporate Risk Management Group to formally review and agree the effectiveness of major project risk management arrangements on a continuing basis.

5.1.15 The Council's Risk Officer regularly contacts Operational risk Managers, reminding them to update their operational risk registers in line with the Risk Management Assurance Framework. A recent review of the Operational risk registers identified that 5 registers had not been updated for that quarter.

5.1.16 Zurich Municipal issued a report on Council Operational Risk Management in November 2020. The report recommended that all key personnel within the Service area should be involved in the process of undertaking risk assessments and reviewing the operational risk register. The aim is to provide broader risk insights and help embed understanding of the risk management process within the wider team. It is advised that management may wish to consider seeking demonstratable evidence that operational risks have been regularly reviewed by wider key service personnel.

5.1.17 It is noted that some operational risk registers include a significant number of low scoring risks. To help maximise added value to the Council, Operational Managers may wish to consider recording only key risks to not achieving operational objectives. (max 7 to 10 risks). This will also help ensure proportionality of the operational risk management process.

Recommendation 4 – Risk Management Sub-group to formally review and agree the effectiveness of operational risk management arrangements, on a continuing basis.

5.1.18 Documenting terms of reference helps to increase transparency of governance group activities and accountability for decision making. Terms of reference for key risk management governance groups were found to be either unavailable or requiring review and update to align with current practice.

5.1.19 It is advised that the Risk Task and Finish Group may wish to further consider the purpose, authority, responsibility and regularity of Unitary Authority risk governance groups, and how this will be captured in terms of reference.

5.2 Information – reliability and integrity of financial and operational information

5.2.1 The Council's Risk Management Assurance Framework describes the Council's approach to risk, its strategic aim and objectives surrounding risk management. It also describes how the framework will be put in to practice with performance measured and evaluated.

5.2.2 The Framework details that it is owned by the CRMG and will be reviewed at least annually. Audit found that The Framework has not been reviewed for a significant length of time and there are several examples that demonstrate reduced alignment to current practice. Lack of regular, formal review significantly reduces Framework robustness and is likely to erode confidence in those tasked with risk management responsibility.

5.2.3 Under normal circumstances, regular formal review in line with the Risk Management Assurance Framework would be recommended. Given the impending Local Government Reorganisation, this is not now considered likely to now add significant value. It is advised that the task and finish group consider putting an arrangement in place to verify that current practice remains aligned to the new Unitary Authority framework on a continuing basis.

5.2.4 The Council's Risk Management Assurance Framework is a comprehensive document. There is an increased risk with a document of this size that key risk messages become lost in the detail. It is advised that the task and finish group may wish to consider reducing the Framework size in the new Unitary Authority.

5.2.5 It is noted that the Framework specifies meeting regularity for the Risk Management Sub-Group, but not for the Corporate Risk Management Group or Transformation Board. It is advised that the task and finish group may wish to consider if the Unitary Authority Risk Management Assurance Framework should specify meeting regularity for all Risk Governance groups.

5.3 Value – effectiveness and efficiency of operations and programmes

5.3.1 The Zurich Municipal report (5.1.16) detailed 9 recommendations on improvements to Council operational risk management. Although there is some evidence that an action plan to progress the Zurich recommendations was reviewed historically, there is insufficient evidence that all recommendations have been regularly reviewed and fully implemented. This is largely due to the lengthy RMSG hiatus, although action plan progress was revisited at the group's recent meeting in August 2022.

5.3.2 Periodic 'Corporate Risk Management – Policies and Processes' training is provided to interested Councillors, Managers and Officers. The evidence provided to Audit indicated that attendance is low and only three training sessions have been held in the last five years.

5.3.3 There is an increased risk that those tasked with managing corporate, operational and major project Council risks cannot do so effectively without clear direction through training attendance. Management may wish to consider making risk management training compulsory for Service and Major Project Managers and use of alternative delivery platforms such as Skill Gate.

5.3.4 An enterprise risk assessment framework provides a systematic way to assess internal and external risk factors. It is advised that the Risk Management Task and Finish Group may wish to consider which of the following frameworks identified by the Institute of Internal Auditors, may be applicable as a basis for organisational risk management planning in the new Unitary Authority.

- The Committee of Sponsoring Organisations of the Treadway Commission (COSO) framework
- International Standard for Organisation (ISO) 31000 framework (referenced in the current Risk Management Assurance Framework).
- Guidance on Risk Management, Internal Control and Related Financial and Business Reporting (Turnbull Guidance)

It is further advised that the Risk Management Task and Finish Group may wish to consider how best to embed the chosen risk assessment framework, ensuring it is actively applied on a continuing basis throughout the new Authority.

Appendix A – Management Action Plan

Summary of Recommendations and agreed actions					
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**
Recommendation 1 – Corporate Risk Management Group to formally review and agree the Corporate Risk Register on a <u>continuing basis,</u> in line with the Council's Financial Procedure Rules.	M	Risks to Corporate objectives escalate and management unable to make informed decisions on corrective action.	Regular meetings of the CRMG to be scheduled up until Vesting Day. Corporate Risk owners to be e-mailed monthly checking for any escalations/ identification of new corporate level risks. Special meeting of the CRMG can be called when required. The City Council's current corporate risk register is part of discussions at an LGR Task & Finish Group, this will ensure that the relevant risks migrate to the new Cumberland authority. It will also ensure examples of best practice from across the districts can be best utilised going forward.	Chief Executive's Office Manager	November 2022 November These meetings are taking place regularly as of October 2022

Summary of Recommendations and agreed actions					
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**
Recommendation 2 – Corporate Risk Management Group to formally review and agree the effectiveness of the Risk Management Sub-Group, on a continuing basis.	M	Risk Management Sub-Group is not operating effectively with reduced oversight of risks to operational objectives.	RMSG minutes to be a standing item on the CRMG agenda. The RMSG has agreed the need to continue to meet beyond Vesting Day CRMG to have a discussion as to how best carry out the review and identify actions/timescales	Chief Executive's Office Manager	November 2022
Recommendation 3 – Corporate Risk Management Group to formally review and agree the effectiveness of major project risk management arrangements on a continuing basis.	H	Risks to major Council projects escalate and management unable to make informed decisions on corrective action.	Project Managers to continue to be requested to identify escalating risks and flag these with the Chief Executive's Office to arrange necessary escalation routes. A discussion to take place at CRMG around adding this to the role of that Group.	Chief Executive's Office Manager	On-going

Summary of Recommendations and agreed actions					
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**
Recommendation 4 – Risk Management Sub-group to formally review and agree the effectiveness of operational risk management arrangements, on a <u>continuing basis</u>.	M	Risks to service objectives escalate and management unable to make informed decisions on corrective action.	This process is about to re-commence with the consideration of the HR operational risk register at the November meeting of the RMSG. At the end of the RSMG the next operational risk register for consideration will be identified and agreed and the penholder invited to attend the next meeting to present.	Chief Executive's Office Manager	On-going

Appendix B – Advisory Comments

Ref	Advisory Comment
5.1.11	Seek demonstratable evidence that project risks have been regularly reviewed by wider project teams.
5.1.14	Task and Finish Group to consider further robust direction for Unitary Authority projects including review regularity, evidence of wider project team review and clear oversight/ reporting arrangements to evidence that Council project risk management is working effectively.
5.1.16	Seek demonstratable evidence that operational risks have been regularly reviewed by wider key service personnel.
5.1.17	To help maximise added value to the Council, Operational Managers may wish to consider recording only key risks to not achieving operational objectives. (max 7 to 10 risks).
5.1.19	Task and finish group to consider the purpose, authority, responsibility and regularity of Unitary Authority risk governance groups, and how this will be captured in terms of reference.
5.2.3	Task and finish group to consider putting an arrangement in place to verify that current practice remains aligned to the new Unitary Authority framework on a continuing basis.
5.2.4	Task and finish group may wish to consider reducing the Framework size in the new Unitary Authority.
5.2.5	Task and finish group may wish to consider if the Unitary Authority Risk Management Assurance Framework should specify meeting regularity for all Risk Governance groups.
5.3.3	Management may wish to consider making risk management training compulsory for Service and Major Project Managers and use of alternative delivery platforms such as Skill Gate.
5.3.4	Task and Finish Group may wish to consider which of the risk assessment frameworks identified by the Institute of Internal Auditors may be applicable as a basis for organisational risk management planning in the new Unitary Authority. Task and Finish Group may wish to consider how best to embed the chosen risk assessment framework, ensuring it is actively applied on a continuing basis throughout the new Authority.

Appendix C - Audit Assurance Opinions

There are four levels of assurance used; these are defined as follows:

	Definition:	Rating Reason
Substantial	There is a sound system of internal control designed to achieve the system objectives and this minimises risk.	The control framework tested are suitable and complete are being consistently applied. Recommendations made relate to minor improvements or tightening of embedded control frameworks.
Reasonable	There is a reasonable system of internal control in place which should ensure system objectives are generally achieved. Some issues have been raised that may result in a degree of unacceptable risk exposure.	Generally good systems of internal control are found to be in place but there are some areas where controls are not effectively applied and/or not sufficiently embedded. Any high graded recommendations would only relate to a limited aspect of the control framework.
Partial	The system of internal control designed to achieve the system objectives is not sufficient. Some areas are satisfactory but there are an unacceptable number of weaknesses that have been identified. The level of non-compliance and / or weaknesses in the system of internal control puts achievement of system objectives at risk.	There is an unsatisfactory level of internal control in place. Controls are not being operated effectively and consistently; this is likely to be evidenced by a significant level of error being identified. High graded recommendations have been made that cover wide ranging aspects of the control environment.
Limited/None	Fundamental weaknesses have been identified in the system of internal control resulting in the control environment being unacceptably weak and this exposes the system objectives to an unacceptable level of risk.	Significant non-existence or non-compliance with basic controls which leaves the system open to error and/or abuse. Control is generally weak/does not exist.

Appendix D

Grading of Audit Recommendations

Audit recommendations are graded in terms of their priority and risk exposure if the issue identified was to remain unaddressed. There are two levels of audit recommendations; high and medium, the definitions of which are explained below.

	Definition:
High	Significant risk exposure identified arising from a fundamental weakness in the system of internal control
Medium	Some risk exposure identified from a weakness in the system of internal control

The implementation of agreed actions to Audit recommendations will be followed up at a later date (usually 6 months after the issue of the report).