Causeway Coast and Glens Borough Council

Internal Audit Report
Risk Management

July 2017
Final

MOORE STEPHENS

INTERNAL AUDIT REPORT

Risk Management

Executive Summary

This internal audit was completed in accordance with the approved annual Internal Audit Plan for 2017/18. This report summarises the findings arising from a review of Risk Management which was allocated 10 days.

Through our audit we found the following examples of good practice:

- A Risk Management Strategy is in place which contains key definitions relating to risk management; sets out the roles and responsibilities across Council in relation to risk management; and contains the main elements of a risk management process
- A Corporate Risk Register is in place; which is managed centrally and reported quarterly to the Audit Committee.

Four areas (Priority 2) where controls could be enhanced was noted during our review:

- Our testing showed that, whilst a positive start has been made to implementing risk management within Council, there is an ad hoc approach to risk management which indicates that there is a need to deepen the culture of risk management across the Council. This requires a systemic and consistent approach to risk management and wider awareness of and full implementation of the Risk Management Strategy. Council should therefore review the need for additional training and awareness raising in relation to the Risk Management Strategy and process.

- Our testing found a lack of clarity over the levels at which risk registers should be in place (ie directorate or service) and inconsistencies in approach to risk management. To address the lack of clarity and promote consistency, SMT should discuss and agree the risk management process at directorate and/or service level

- There were inconsistencies in the implementation of the Council's Risk Management Strategy in terms of the development of risk registers, document templates and framework for escalating significant risks to corporate level.

- The monitoring and review of risks recorded on the risk registers is not documented and those with responsibility for ensuring that mitigating actions are implemented (ie the risk owner) are not always identified.

The following table summarises the total number of findings/recommendations from our audit:

Risk	Number of recommendations & Priority rating		
	1	2	3
There may be an unsupportive internal environment in relation to risk management, leading to a poor culture of risk management and increased risk that Council risks will not be managed effectively	-	2	1
It may be that risks are not identified and assessed consistently at both corporate and service level and are not linked to corporate and service objectives and priorities leading to potential non-achievement of Council business objectives	-	1	-
There may be no mechanism in place to monitor, review and report progress of actions which have been identified to mitigate risks, leading to the risk of mitigating actions not being implemented or potential new Council risks going unnoticed	-	1	-
Total recommendations made	**0**	**4**	**1**

Based on our audit testing we are able to provide the following overall level of assurance:

Satisfactory	Overall there is a satisfactory system of governance, risk management and control. While there may be some residual risk identified this should not significantly impact on the achievement of system objectives.

Points for the attention of Management

We have identified a number of system enhancements during the course of the audit which do not form part of our formal findings, but may help enhance the existing controls. These are detailed at Appendix III.

Table of Contents

Auditor:	Catriona McHugh
Distribution:	Audit Committee Chief Executive Director of Corporate Services
	July 2017

Audit progress	Date
Audit commenced	26 June 2017
Draft Report issued to senior management for response	26 July 2017
Responses Received	13 September 2017
Responses Agreed	13 September 2017
Report Issued	13 September 2017

All matters contained in this report came to our attention while conducting normal internal audit work. Whilst we are able to provide an overall level of assurance based on our audit work, unlike a special investigation, this work will not necessarily reveal every issue that may exist in the Council's internal control system.

1 Objective

The areas for inclusion in the scope of the audit were determined through discussion with management. The scope of this audit is to review the arrangements in place within the Council in relation to risk management, focusing on the main risks associated with:

- General arrangements
- Identifying and assessing risks (Corporate and Service levels)
- Reducing risks (Corporate and Service levels)
- Monitoring, review and reporting processes

The audit focus will be primarily on the structures and processes used in risk management rather than being an assessment of the outcomes achieved in applying the risk management processes

2 Background

Risk Management describes all of the activities required to identify and control exposure to risk which may have an impact on the achievement of an organisation's objectives. It is important that the Council has a risk management framework in place to enable the risk management process to be carried out to ensure all significant risks are identified, evaluated, controlled, monitored and reported in accordance with good practice.

The COSO (Committee of Sponsoring Organisations) "Enterprise Risk Management – Integrated Framework" (2013) is one of the most influential frameworks in relation to risk management globally. The COSO framework identifies three categories of objectives; operations, reporting, and compliance, and consists of five integrated components of internal control:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring activities

Each of these categories and components must operate effectively in order for risk management to be fully embedded across an organisation.

Causeway Coast and Glens Borough Council recognises risk management to be an essential part of its corporate governance arrangements and a Risk Management Strategy was approved in October 2015 (and reviewed at Audit Committee in June 2017). The strategy contains the key elements of a risk management process. This process involves: identifying risks to achieving the Council's objectives at the corporate level and Directorate/Service level; prioritising these in terms of potential impact and likelihood of occurrence; ensuring that appropriate actions are taken to mitigate the identified risks; and monitoring and reporting.

The strategy lays out the key responsibilities for risk management within Causeway Coast and Glens Borough Council. The Director of Performance has operational responsibility for risk management particularly in relation to:

- Exercising oversight of the staff of Council responsible for the management of risk within the organisation.
- Providing assurance to Councillors that all identified risks are being managed.
- Providing SMT with regular briefings on all aspects of risk management
- Ensure the Risk Register is updated when new risks are identified and notified or when a change in circumstances concerning risks already in the register are notified to the Risk Management Co-Ordinator or Head of Service.
- Agree the ownership and management of risks.

The Senior Management Team (SMT) are responsible for developing and reviewing risk registers and action plans, at both Corporate and Service Level and for providing annul assurance statements at the service level.

3 Risks

The risks identified by Internal Audit relating to risk management and agreed with management are as follows:

1. There may be an unsupportive internal environment in relation to risk management, leading to a poor culture of risk management and increased risk that Council risks will not be managed effectively
2. It may be that risks are not identified and assessed consistently at both corporate and service level and are not linked to corporate and service objectives and priorities leading to potential non-achievement of Council objectives
3. There may be no mechanism in place to monitor, review and report progress of actions which have been identified to mitigate risks, leading to the risk of mitigating actions not being implemented or potential new Council risks going unnoticed

4 Audit Approach

Our audit fieldwork comprised:

- Documenting the systems via discussions with key staff
- Consideration of the key risks within each audit area
- Examining relevant documentation
- Carrying out a preliminary evaluation of the arrangements and controls in operation generally within the Council
- Testing the key arrangements and controls
- Testing the completeness and accuracy of records.

The table below shows the staff consulted with and we would like to thank them for their assistance and co-operation.

Job title
Director of Performance
Director of Leisure and Development
Director of Environmental Services
Head of Planning
Chief Finance Officer

5 Findings and Recommendations

This section of the report sets out our findings in relation to control issues identified and recommendations. A summary of all the key controls that we considered is included in Appendix II to this report.

5.1 Risk 1 – Framework and Culture for Risk Management

ISSUE 1 – Risk Management Culture
a) Observation- We found that a positive start has been made to implementing risk management within Council – a Risk Management Strategy and elements of a risk management process are in place and initial risk management training has been provided to the majority of Directors and Heads of Service. However, we found from discussions and our testing that there is an ad hoc and inconsistent approach to Risk Management practice e.g. updated risk registers are not in place for all Directorates, inconsistent review of existing risk registers, no formal evidenced review of mitigating actions identified to reduce risk etc. (The detailed findings on this are discussed further in Issues 2-5)
b) Implication- A consistently embedded culture of risk management (which includes clear recording of, accountability for and ownership of specific risks and risk areas) is not yet in place within Council which leads to increased risk that Council risks will not be managed effectively.
c) Priority Rating- 2
d) Recommendation- Risk management practices should be promoted to support the embedding of a culture of risk management across the Council. Consideration should therefore be given to the need for • additional training and awareness raising in relation to the Risk Management Strategy and process; and • identification of personnel to be responsible for overseeing the risk management process at the different levels of Council.

e) Management Response-Agreed

f) Responsible Officer & Implementation Date- Director of Corporate Services, March 2018

ISSUE 2 – Risk Management Framework

a) Observation-

The Risk Management Strategy contains key definitions, outlines responsibilities and contains the key steps for a risk management process. We found from our discussions with members of the SMT that there is an understanding and acceptance of the need to fully implement the Risk Management Strategy and process. Our testing found however that the process of risk assessment is not yet being consistently applied at all levels of the Council:

- 2 Directorate areas have put in place directorate and service level risk registers
- 1 has a directorate level risk register but no service level risk registers
- 2 directorates have plans to put directorate level risk registers in place (no documented risk assessments completed currently), but are unsure whether they are required to put in place separate service level risk registers.

We also found that there is no consistency in the risk register templates used to capture risk assessment information.

We noted that the risk management strategy is not explicit in setting out at which level risk registers should be maintained i.e. one per service area or one per directorate.

b) Implication-

A consistent process of risk management is not yet fully established which leads to increased risk that Council risks will not be managed effectively.

c) Priority Rating-

2

d) Recommendation-

To address the lack of clarity in terms of risk management process, and to promote consistency, SMT should:

a. Agree the level at which a risk register is required (e.g. at every service level or at Directorate level),
b. Prepare a flow-chart or summarise the risk management process steps and deadlines in a short 1-2 page document, and
c. Agree a template for the Directorate/Service level risk register which includes a reference to Council's objectives (see Issue 2 also).

e) Management Response- Agreed

f) Responsible Officer & Implementation Date-Director of Corporate Services, March 2018

ISSUE 3 – Linking Risk Management to Corporate and Business Planning
a) Observation- The corporate risk register contains a column 'Aligned Corporate Objective' which should be completed for each risk identified, however it has not been completed. From our testing of the risks registers in place within the 3 directorates that have completed them, we found that 2 had columns within their risk registers for recording alignment to corporate objectives. This column was not completed for 2 of the 6 service level risk registers within one of the directorates. The second directorate used a different template but did align risks to service level aims. The third directorate used another template which contained no reference to objectives (at any level). We noted that Directorate Annual Business Plans include Strength, Weakness, Opportunity and Threat (SWOT) and Political, Economic, Social, Technological, Environmental and Legal (PESTEL) analysis. This analysis helps identify areas of risk and creates a linkage between the business planning cycle and risk management; it is not sufficient however to ensure formal integration of risk assessment and business planning.
b) Implication- In the absence of clear and consistent linkage between risk management and corporate and business planning there is a risk that council risks to achievement of objectives are not properly identified and managed effectively.
c) Priority Rating- 3
d) Recommendation- To develop directorate/service operational Risk Registers, the risks relating to achievement of operational objectives (outlined in the Directorate Annual Business Plans) as well as corporate objectives should be identified. The Business Plan format should therefore be reviewed to determine how to better reflect risk management. This may require including a brief section summarising risks identified during the preparation of the Annual Business Plan (e.g. as a result of SWOT and PESTEL analysis); and the introduction of a mechanism to ensure these risks identified are reflected in the risk registers. Entering information in the column "Aligned Corporate Objective" within the risk register template (which is used within the Directorate of Performance) would also help with this integration.
e) Management Response- Agreed
f) Responsible Officer & Implementation Date-Director of Corporate Services, March 2018

5.2 Risk 2 – Consistent Identification of Risks Linked to Objectives

ISSUE 4 – Identification of Risks
a) Observation- As noted in Issue 1, not all directorate/service level risk registers are yet in place. As noted in Issue 2, we found that for those directorate/service level risk registers which were in place, there was insufficient evidence of appropriate consideration of corporate and service objectives and priorities. In addition, we found that: • The template being used for risk registers varies and for one directorate the template did not include an assessment of inherent and residual risk • On one risk register, 2 of the risks were not considered to be tolerable and a need that further action was required was noted - no actions were however identified • Inconsistencies exist between the information in the corporate risk register and the corporate risk map (the corporate risk matrix contains 12 risks whilst the Corporate Risk Register contains 14 risks). We also found that there is no clear procedure to ensure that significant service level risks are considered for inclusion in the corporate risk register. We noted from our discussions that some discussion of the corporate risk register takes place at SMT meetings but this is not documented. We were also advised that a fully developed process of reviewing existing (directorate/service level) risk registers is yet to be established.
b) Implication- If risk registers are not in place at all appropriate levels within Council, and not reviewed in an ongoing manner, then Council risks are not being identified and assessed consistently at both corporate and service level. This increases the risk of non-achievement of Council objectives
c) Priority Rating- 2
d) Recommendation- To ensure that the Risk Management Strategy is implemented the following should be addressed: • Risk Registers should be developed for all directorate/service levels (on a template agreed by SMT, see Issue 1) and key directorate/service level risks should be clearly identified and assessed for inherent and residual risk ratings • A determination of how tolerable the residual risk is should be recorded on the risk register, and where it is considered not tolerable, further actions should be identified and recorded. Responsibilities and deadlines should be assigned to implement any actions identified

- During compilation and ongoing review of directorate/service level risk registers the need to escalate any operational risks from the Directorate/Service level to the Corporate level, should be considered
- The Corporate Risk Register and Corporate Risk Matrix should be reviewed and updated at SMT.

e) Management Response- Agreed

f) Responsible Officer & Implementation Date-Director of Corporate Services, March 2018

5.3 Risk 3 – Monitoring and Review of Risk Management

ISSUE 5 – Monitoring and Review

a) Observation-
The Risk Management Strategy sets out that risk registers (corporate and directorate/service) should be reviewed monthly. Formal monthly reviews of the risk registers may not however be necessary at all levels.

We noted that there is no formal evidence of review of the corporate risk register by SMT or discussion of mitigating actions. The Director of Performance has advised that, following the recent updates to the Risk Management Strategy, there will be a formal evidenced review of the Corporate Risk Register and mitigating actions at the SMT; and reporting to the Audit Committee will continue. We were also advised that whilst risks are discussed at Directorate level via regular management team meetings there is no documented evidence of risk register review or of monitoring of progress of actions to reduce risk.

b) Implication-
This could lead to the risk of mitigating actions not being implemented or a potential new risk not being assessed. Additionally, formal monthly reviews of risk registers may be too frequent in some cases and may lead to the perception of a 'risk management bureaucracy', where risk management is seen as only completing a risk register document, rather than this being considered a tool to support effective risk management.

c) Priority Rating-
2

d) Recommendation-
A mechanism should be put in place to retain evidence of periodic Risk Register reviews and of the actions being taken to mitigate risk, at both the Corporate and Directorate level. In addition, evidence of the outcome of the review of Risk Registers and monitoring progress of mitigating actions should be recorded and retained (at all levels).

	SMT discussion of risk management (e.g. annual review of risk management arrangements, review of Corporate Risk Register, reports on progress of mitigating actions etc.) should be documented in the SMT minutes. The frequency of review at each Council level should also be discussed and agreed by the SMT.
e)	**Management Response**- Agreed
f)	**Responsible Officer & Implementation Date-Director of Corporate Services, March 2018**

Appendix I: Definition of Assurance Ratings and Hierarchy of Findings

Satisfactory Assurance
Evaluation opinion: Overall there is a satisfactory system of governance, risk management and control. While there may be some residual risk identified this should not significantly impact on the achievement of system objectives.

Limited Assurance
Evaluation opinion: There are significant weaknesses within the governance, risk management and control framework which, if not addressed, could lead to the system objectives not being achieved.

Unacceptable Assurance
Evaluation opinion: The system of governance, risk management and control has failed or there is a real and substantial risk that the system will fail to meet its objectives.

Hierarchy of Findings

This audit report records only the main findings. As a guide to management and to reflect current thinking on risk management we have categorised our recommendations according to the perceived level of risk. The categories are as follows:

Priority 1: Failure to implement the recommendation is likely to result in a major failure of a key organisational objective, significant damage to the reputation of the organisation or the misuse of public funds.

Priority 2: Failure to implement the recommendation could result in the failure of an important organisational objective or could have some impact on a key organisational objective.

Priority 3: Failure to implement the recommendation could lead to an increased risk exposure.

Appendix II: Summary of Key Controls Reviewed

Budgetary Control

Risk	Key Controls

There may be an unsupportive internal environment in relation to risk management, leading to a poor culture of risk management and increased risk that Council risks will not be managed effectively	• There is a Risk Management Framework in place which includes;
	  • A Risk Management Strategy which defines and steers risk management,
	  • Clearly defined roles, responsibilities and accountabilities of various stakeholders across Council,
	  • A defined risk management process - this is subject to an audit recommendation
	  • Guidance, templates and tools to support risk assessment and monitoring of progress to mitigate risk - this is subject to an audit recommendation
	• Heads of Service are trained in risk management and aware of their role and responsibility in relation to risk management
	• Staff are engaged in the risk management process
	• Risk management is integrated into the corporate and annual business planning cycle, financial planning and performance management. - this is subject to an audit recommendation
	• An anonymous whistleblowing policy is in place

It may be that risks are not identified and assessed consistently at both corporate and service level and are not linked to corporate and service objectives and priorities leading to potential non-achievement of Council business objectives	• A corporate risk register is in place, held centrally and updated regularly • The corporate risk register was prepared considering corporate objectives and priorities • The corporate risk register clearly sets out the corporate risks, assesses each risk and identifies how they will be mitigated • The service level risk registers were prepared considering both corporate and service objectives and priorities - this is subject to an audit recommendation • Service level risk registers clearly set out the service's risks, assesses each risk and identifies how they will be mitigated - this is subject to an audit recommendation • Significant service level risks are considered for inclusion in the corporate risk register - this is subject to an audit recommendation • Adequate time is set aside with meetings at various Council levels to develop and update the risk registers - this is subject to an audit recommendation
There may be no mechanism in place to monitor, review and report progress of actions which have been identified to mitigate risks, leading to the risk of mitigating actions not being implemented or potential new Council risks going unnoticed	• There is a documented schedule for reviewing mitigating actions and updating the corporate and service level risk registers - this is subject to an audit recommendation • Key corporate level risks are identified and regularly monitored by the Senior Management Team - this is subject to an audit recommendation • The service risk registers and progress of mitigating actions are discussed regularly at service level staff meetings - this is subject to an audit recommendation • Risk register reviews by Heads of Service are assessed and approved by the appropriate Director

Risk	Key Controls
	• The service risk registers and progress of mitigating actions are discussed at Senior Management Team meetings - this is subject to an audit recommendation • Consideration is given to emerging and new corporate and service level risks and risk registers are updated accordingly - this is subject to an audit recommendation • The Corporate Risk Register is discussed at the Audit Committee meetings • The corporate risk register and progress of mitigating actions is reported to Council, at least bi-annually

Appendix III: Points for the Attention of Management

Communication relating to Risk Management
Communication and consultation are important during each step of risk management to ensure deepening of the risk management culture. All staff play a role in risk management and all staff should therefore be advised of the recently-updated Risk Management Strategy and its location on the Council's staff intranet.
Management response: agreed

Health and Safety – Risk Assessments
We found from our testing of Health and Safety inspection reports that the majority of risk assessments (RAs) which Health and Safety inspectors expected to see in place have been carried out, although there were a small number of exceptions (e.g. absence of [4 out of 5] Fire Risk Assessments) and there is need for comprehensive updating of risk assessments across Council. We were advised that the Health and Safety officers are currently undertaking an exercise to ensure all Fire RAs are put in place across Council. The Health and Safety officers should continue with this exercise, until all Fire Risk Assessments are in place, and also remind all relevant staff of the need to continuously review and update all risk assessments.
Management response: agreed