



ABERDEEN CITY COUNCIL

Internal Audit Report Risk Management

Issued to:

Angela Scott, Chief Executive
Richard Ellis, Interim Director of Corporate Governance
Steven Whyte, Head of Finance
Neil Buck, Performance and Risk Manager
Anne MacDonald, Audit Scotland

EXECUTIVE SUMMARY

Risk Management is the process of identifying risks, assessing the likelihood and impact of their occurrence and determining the most effective methods of managing or reducing them to an acceptable level. The objective of this review was to undertake a review of the Council's adopted Risk Management procedures to identify its risks and ensure that they are adequately managed.

A new Risk Management Strategy was approved by the Audit, Risk and Scrutiny Committee on 26 February 2015 and this replaced the Strategy that had been approved in October 2013.

The overall conclusion drawn by Internal Audit in relation to Risk Management is that the Council has shown good self-awareness regarding its position relating to implementing a revised Risk Management process throughout the organisation. Reports to Committee have highlighted where progress has been made and where improvements are required. The revised process is being driven forward by senior management and there appears to be general 'buy-in' to the strategy.

However, progress is not as advanced as anticipated and the required next steps are to improve progress, ensure that further tiers of management receive training in the risk management process so that it can become further embedded in the organisation, and ensure that reporting arrangements are in place and complied with to ensure that appropriate senior officer and member scrutiny can be applied in an effective way.

1. INTRODUCTION

- 1.1 Risk Management is the process of identifying risks, assessing the likelihood and impact of their occurrence and determining the most effective methods of managing or reducing them to an acceptable level.
- 1.2 The objective of this review was to undertake a review of the Council's adopted Risk Management procedures to identify its risks and ensure that they are adequately managed. This did not extend to consideration of the actual risks identified, how they had been ranked, or the controls in place to mitigate against those risks materialising. These controls will be reviewed in other planned Internal Audit work over a number of years.
- 1.3 The factual accuracy of this report and action to be taken with regard to the recommendations made have been agreed with Angela Scott, Chief Executive and Acting Director of Corporate Governance, and Neil Buck, Performance and Risk Manager.

2. FINDINGS AND RECOMMENDATIONS

2.1 System of Risk Management

2.1.1 In February 2014, the then Director of Corporate Governance presented a report to the Audit and Risk Committee outlining the characteristics of good risk management along with an assessment of the Council's practice at that time. The report identified that the system of risk management is made up of a number of elements:

- A risk management **Strategy**
- A **System**, generally an IT system, for helping to record the assessment and management of risk
- An organisational **Structure** which ensures that the management of risk is spread across individuals who are well placed to manage the risk
- **Staff** with the necessary **Skills** to manage risk
- **Shared Values** – a culture where risks (threats) are actively managed and risks (opportunities) are taken.

2.1.2 The focus of the report was on the **Structure** element comprising management responsibility and the use of corporate and service risk registers to demonstrate delegation. This highlighted that there were a number of areas where the Council's procedures demonstrated good practice. It also identified areas where improvement was needed and what needed to be done to achieve that improvement. Further reports were to be submitted to each cycle of the Committee informing members of the status of each component and plans for improvement.

2.1.3 In May 2014, the Audit and Risk Committee received an update report on the structure element and a focus on the **Skills** element. The Strategic Risk Register, which reflects the risk management structure, had been revised and approved by the Corporate Management Team. Each of the strategic risks, those that have the highest level of potential impact on the Council's ability to carry out its core and statutory duties, to provide essential services, and protect the workforce and communities from harm, were categorised into four high level themes of:

- Capacity
- Capability
- Harm
- Compliance.

The report detailed progress and where further work was required.

2.1.4 In relation to the skills element, the report identified the skills required by key officers as:

- Risk identification
- Assignment of risk ownership
- Risk evaluation (identifying existing controls, planned or developing mitigation, analysing risk events or incidents related to the risk and examining risks at the operational level which may have influence on higher risk)
- Assessment of risk appetite (assessing the level of risk the Council is prepared to accept when considering the cost of mitigation)
- Response (Tolerate, Treat, Transfer, Terminate)

- and for members as

- Assurance
- Embed and review.

2.1.5 The report identified a need for officer training and stated that members of the Audit and Risk Committee had received training. A report to the Audit and Risk Committee in September 2014 stated that it was the intention to monitor progress with completion of training modules and Online Interaction Learning courses by service at the CMT level through a suite of performance indicators reported through the Corporate Performance Dashboard. The Dashboard available on The Zone is incomplete and does not cover the above performance data.

<u>Recommendation</u>		
In order to meet its intention to monitor progress with the completion of training modules the Council should put arrangements in place to capture and report data as stated.		
<u>Service Response / Action</u>		
Agreed.		
<u>Implementation Date</u>	<u>Responsible Officer</u>	<u>Grading</u>
TBC	Performance and Risk Manager.	Significant within audited area.

2.1.6 The report also stated that the Strategic Risk Register (attached to the report) was considered at each monthly meeting of CMT, will be continuously updated to reflect changes at both the corporate and service levels, and that the register is now included in the Corporate Performance Dashboard. The note of meeting for CMT on 24 September 2015 acknowledged that work on the register is ongoing. Officers have stated that work is continuing within the Council on the content of the Strategic Risk Register with the intention to report this to the Audit, Risk and Scrutiny Committee when complete. A recommendation is made here to track progress.

<u>Recommendation</u>		
The Strategic Risk Register should be updated, approved and reported to the Audit, Risk and Scrutiny Committee.		
<u>Service Response / Action</u>		
Agreed.		
<u>Implementation Date</u>	<u>Responsible Officer</u>	<u>Grading</u>
March 2016.	Interim Director of Corporate Governance.	Significant within audited area.

2.1.7 There is a “box” for the Strategic Risk Register in the Corporate Performance Dashboard on The Zone, but it is not populated. The Corporate Governance service risk register was stated to be incorporated into the Service’s performance dashboard. Again, there are boxes in the dashboard held on The Zone for each function within Corporate Governance, but they are empty.

Recommendation

Performance Dashboards held on The Zone should be populated with the required data.

Service Response / Action

Agreed.

Implementation Date

March 2016

Responsible Officer

Performance and Risk
Manager.

Grading

Important within audited
area.

- 2.1.8 In June 2014, the Audit and Risk Committee received an update report on the structure and skills elements and a focus on the **System** element. It stated that an effective risk management information system will encompass:
- Risk profile data, values and information
 - Risk registers
 - Risk improvement and action plans
 - Business Continuity Plans and responsibilities
 - Risk incident information
 - Governance, monitoring and reporting functionality
- 2.1.9 In relation to risk incidents, the following had been identified as having particular significance:
- ICT Security
 - ICT Operations
 - Data Breaches / Information Security
 - Facilities (Operational)
 - Facilities (Security)
 - Health and Safety
- 2.1.10 It was reported that, in general, more work was required to capture learning from such events.
- 2.1.11 A new Risk Management Strategy was approved by the Audit, Risk and Scrutiny Committee on 26 February 2015 and this replaced the Strategy that had been approved in October 2013. The Strategy confirms the Council's commitment to the development of an Enterprise Risk Management approach and details the governance and reporting arrangements around the Council's management of risk whilst providing strategic direction with regard to the Council's approach to risk and opportunity. The Strategy is the principal point of reference for all officers and elected members involved in the risk management process and will be subject to annual review. Guidance is given on roles and responsibilities, the control environment, the assessment of risk appetite, governance around risk management in the Council Group, the integration of health and adult social care, and the management of, and response to, risk incidents.
- 2.1.12 The Risk Management Strategy is supported by a Risk Management Manual dated 2014 which details the Risk Management Process and is supported on The Zone by other Risk Management material. This shows that Service Management Teams are required to carry out monthly reviews of risks and prepare registers for reporting to committees. Committees are to review Service risk registers at least quarterly.
- 2.1.13 The Risk Management Manual pre-dates the approved Strategy. In order to ensure that it complements the Strategy in all respects there is a need to review and update the document.

Recommendation

The Risk Management Manual should be reviewed and updated where appropriate.

Service Response / Action

Agreed.

Implementation Date

March 2016.

Responsible Officer

Performance and Risk
Manager.

Grading

Important within audited
area.

- 2.1.14 There is evidence of the Corporate Governance risk registers being considered by the Service Management Team on a regular basis with a stated aim of reviewing those relating to other Services due to Corporate Governance having a more corporate resource and support role in these. The Education and Children's Service's risk register was considered by the Directorate Leadership Team in July 2015 and it was minuted that some changes were necessary before passing the register to Corporate Governance. Progress is being made with updating the Communities, Housing and Infrastructure risk registers, although these are not being considered by the Service Management Team on a regular basis.
- 2.1.15 It is clear that Services are not as far advanced with the completion and monitoring of their risk registers as anticipated by reports to the Audit, Risk and Scrutiny Committee. There is a potential that risks and mitigating controls are not being identified in a timeous manner, and that the Council may be exposed as a result of this.
- 2.1.16 The Corporate Governance Risk Register was reported to the Finance, Policy and Resources Committee on 15 September 2015 after being advised at its meeting on 9 June 2015 that quarterly performance reports would be submitted to the Committee and two of these each year would include the Service's Risk Register. The Communities, Housing and Infrastructure Risk Register was reported to the CH&I Committee on 19 May 2015. There have been no reports relating to the Education and Children's Services risk register to a Policy Committee, although it is understood that the first will be reported in November 2015.

Recommendation

Services should bring their risk registers up-to-date and these should be monitored through CMT and Service Management Teams, and reported to Committee in accordance with an agreed timetable.

Service Response / Action

Agreed.

Implementation Date

March 2016.

Responsible Officer

All Directors.

Grading

Significant within audited
area.

- 2.1.17 The Risk Management Strategy states that all Services will be represented on the Corporate Risk Management Group which will meet quarterly. When Internal Audit (PWC) audited the Council's risk management arrangements in November 2011, it was reported, under identified good practice, that the Corporate Risk Management Group had met regularly and had been well attended. The last meeting of the Group was in June 2014 (un-minuted) and the previous meeting was held in September 2013.

Recommendation

The Council should ensure that the Risk Management Group meets on a regular basis and that attendance is monitored.

Service Response / Action

The on-going need for the Risk Management Group will be considered in light of the senior leadership and attention being given to risk now within the organisation.

Implementation Date

March 2016.

Responsible Officer

Director of Corporate Governance.

Grading

Significant within audited area.

- 2.1.18 There are currently no terms of reference for the Corporate Risk Management Group detailing its purpose or composition.

Recommendation

Terms of Reference should be agreed for the Corporate Risk Management Group to ensure clarity of purpose.

Service Response / Action

The on-going need for the Risk Management Group will be considered in light of the senior leadership and attention being given to risk now within the organisation.

Implementation Date

March 2016.

Responsible Officer

Director of Corporate Governance.

Grading

Significant within audited area.

- 2.1.19 The Risk Management Strategy states that a Statement of Internal Control, which details the strength of the Council's response to various factors detailed in the Strategy will be presented to the Audit, Risk and Scrutiny Committee annually. The last report of this nature was dated September 2013.

Recommendation

A Risk Management annual report should be prepared and presented to the Audit, Risk and Scrutiny Committee.

Service Response / Action

The Council moved to adopt a broader governance statement which incorporated the required elements of the old statement of control. This was not reflected in the Risk Management Strategy so action needs to be taken to amend the Strategy to reflect adoption of the governance statement.

Implementation Date

TBC

Responsible Officer

Performance and Risk Manager.

Grading

Significant within audited area.

- 2.1.20 The Risk Management Strategy states that the provision of Risk Management training will be subject to annual benchmarking. The Council participates in the CIPFA / ALARM Risk Management Benchmarking Club. The 2014 report shows that the level of training and guidance that is in place to ensure that people have the right levels of skills and competencies to manage risks they face is below average for the Club and ranked 25th out of 32 participating Councils. Whilst the scoring and ranking is based on a self-assessment, the conclusion of this audit (as detailed in the Executive Summary) is that the Council has demonstrated good self-awareness in relation to Risk Management and this is likely to be reflected in the Benchmarking report.

- 2.1.21 It is understood that the Performance and Risk Manager has been meeting with HR&OD to discuss training and this needs to be progressed to fruition in order to improve performance in this area.

<u>Recommendation</u>		
The provision of required training should be progressed.		
<u>Service Response / Action</u>		
Agreed. The first training session takes place on 6 November 2015 with two further sessions already scheduled.		
<u>Implementation Date</u>	<u>Responsible Officer</u>	<u>Grading</u>
Implemented.	Performance and Risk Manager.	Significant within audited area.

- 2.1.22 A previous Internal Audit of the Council's Risk Management Arrangements identified that there was not enough awareness of the risks posed to the Council through ALEOs. The new Strategy includes comment on risk management in the Council Group and states that the Strategy provides a framework for the Council's ALEOs within which risk management arrangements may be implemented as part of internal governance arrangements. It goes on to list the minimum requirements in relation to the ALEOs.

- 2.1.23 The Council has introduced an ALEO Governance Hub which met for the first time in June 2015 with the next meeting scheduled for December 2015. The minutes of the June 2015 meetings covering the Council's Tier 1 ALEOs were considered by the Audit, Risk and Scrutiny Committee in June 2015. They show that the risk registers presented to the Governance Hub had been considered and challenged where appropriate by the Performance and Risk Manager, providing assurance over these. However, the Governance Hub does not yet extend to the Council's Tier 2 ALEOs.

<u>Recommendation</u>		
Arrangements should be put in place to ensure that the risks associated with the Council's Tier 2 ALEOs are captured and monitored through the ALEO Governance Hub.		
<u>Service Response / Action</u>		
Agreed.		
<u>Implementation Date</u>	<u>Responsible Officer</u>	<u>Grading</u>
May 2016.	Senior Democratic Services Manager.	Significant within audited area.

- 2.1.24 The Risk Management Strategy also covers the Integration of Health and Adult Social Care. Whilst the Aberdeen City Health and Social Care Partnership Integration Scheme's section on Risk Management does not cover the requirements of the Council's RM Strategy it does satisfy the requires of the Scottish Government in this respect. There is a risk register in place which was reported to the Council's Audit, Risk and Scrutiny Committee in September 2015. The Risk Management process is due to be managed using the NHS Datix system rather than the Council's Covalent System in order to allow for a common approach across the three Grampian partnerships.

AUDITOR: D Hughes

Appendix 1 – Grading of Recommendations

GRADE	DEFINITION
Major at a Corporate Level	The absence of, or failure to comply with, an appropriate internal control which could result in, for example, a material financial loss, or loss of reputation, to the Council.
Major at a Service Level	<p>The absence of, or failure to comply with, an appropriate internal control which could result in, for example, a material financial loss to the Service/area audited.</p> <p>Financial Regulations have been consistently breached.</p>
Significant within audited area	<p>Addressing this issue will enhance internal controls.</p> <p>An element of control is missing or only partial in nature.</p> <p>The existence of the weakness identified has an impact on a system's adequacy and effectiveness.</p> <p>Financial Regulations have been breached.</p>
Important within audited area	Although the element of internal control is satisfactory, a control weakness was identified, the existence of the weakness, taken independently or with other findings does not impair the overall system of internal control.