ABERDEEN CITY COUNCIL

COMMITTEE	Audit, Risk and Scrutiny Committee
DATE	25 September 2019
EXEMPT	No
CONFIDENTIAL	No
REPORT TITLE	Internal Audit Report AC2004 – Risk Management
REPORT NUMBER	IA/AC2004
DIRECTOR	N/A
REPORT AUTHOR	David Hughes
TERMS OF REFERENCE	2.2

1. PURPOSE OF REPORT

1.1 The purpose of this report is to present the planned Internal Audit report on Risk Management.

2. RECOMMENDATION

2.1 It is recommended that the Committee review, discuss and comment on the issues raised within this report and the attached appendix.

3. BACKGROUND / MAIN ISSUES

3.1 Internal Audit has completed the attached report which relates to an audit of Risk Management.

3.2 Management Comments

3.2.1 This audit has been supportive in confirming the workplan already in place within the Assurance Team in Governance, a key part of which will be the Risk Management Policy and related procedures.

3.2.2 The most significant findings relate to the development of a risk appetite for the Council against which an assessment of threats and opportunities can be made. This will encourage consistency in our risk management approach and will ensure that all Clusters are clear about the level and type of risk that we can tolerate. The audit also highlights as significant the need for risk registers to be kept under regular review by Chief Officers and used as a “live” document to support them in service design and delivery.

4. FINANCIAL IMPLICATIONS

4.1 There are no direct financial implications arising from the recommendations of this report.

5. LEGAL IMPLICATIONS

5.1 There are no direct legal implications arising from the recommendations of this report.

6. MANAGEMENT OF RISK

6.1 The Internal Audit process considers risks involved in the areas subject to review. Any risk implications identified through the Internal Audit process are as detailed in the attached appendix.

7. OUTCOMES

7.1 There are no direct impacts, as a result of this report, in relation to the Local Outcome Improvement Plan Themes of Prosperous Economy, People or Place, or Enabling Technology, or on the Design Principles of the Target Operating Model.

7.2 However, Internal Audit plays a key role in providing assurance over, and helping to improve, the Council's framework of governance, risk management and control. These arrangements, put in place by the Council, help ensure that the Council achieves its strategic objectives in a well-managed and controlled environment.

8. IMPACT ASSESSMENTS

Assessment	Outcome
Equality & Human Rights Impact Assessment	An assessment is not required because the reason for this report is for Committee to review, discuss and comment on the outcome of an internal audit. As a result, there will be no differential impact, as a result of the proposals in this report, on people with protected characteristics.
Privacy Impact Assessment	Not required
Duty of Due Regard / Fairer Scotland Duty	Not applicable

9. APPENDICES

9.1 Internal Audit report AC2004 – Risk Management.

10. REPORT AUTHOR DETAILS

David Hughes, Chief Internal Auditor
David.Hughes@aberdeenshire.gov.uk
(01467) 537861

Internal Audit Report

Governance

Risk Management

Issued to:
Fraser Bell, Chief Officer – Governance
Jonathan Belford, Chief Officer – Finance
Vikki Cuthbert, Assurance Manager
Ronnie McKean, Corporate Risk Lead
External Audit

Date of Issue: August 2019 **Report No. AC2004**

EXECUTIVE SUMMARY

The Council's Risk Management Framework defines risk as the combination of the likelihood of an event occurring and its impact, should it occur. Once risks have been identified, the Council must respond to them in a way which maximises the Council's chances of achieving its corporate objectives. Risk management is a tool through which threats to those objectives may be identified, assessed and controlled. It may also be necessary to take calculated risks and to seize properly risk-assessed opportunities as they arise. Risk management in this context requires actions which maximise benefits whilst simultaneously minimising threats to success.

Therefore, risk management should be applied throughout the Council's structure, from the overall Council approach through the Corporate Management Team, to each and every employee of the Council.

The objective of this audit was to provide assurance over the risk management arrangements that are currently in operation within the Council. Since the approval of the current Risk Management Framework by the Audit, Risk and Scrutiny Committee in February 2018 work has progressed to implement revised and improved risk registers and supporting processes. In general, these are appropriate and maintained up to date, with limited exceptions.

Improvements have been recommended, including development of the Council's risk appetite, clarifying and improving accessibility of elements of procedure, and further reviewing the extent and frequency of risk register reviews to ensure it can be evidenced that these are being completed in line with policy and best practice.

The Service has agreed to take these on board as part of a revised Risk Management Policy which will be presented to Committee in December 2019, and through the Assurance 365 project, which aims to digitise governance processes and improve accessibility and reporting.

1. INTRODUCTION

1.1 The Council's Risk Management Framework states:

"All change and improvement activity comes with some degree of risk. Risk can be defined as the combination of the likelihood of an event occurring and its impact, should it occur. Once risks have been identified, the Council must respond to them in a way which maximises the Council's chances of achieving our corporate objectives.

Risk management is a tool through which threats to those objectives may be identified, assessed and controlled. This is often referred to as downside risk management. At the same time, we operate in an environment of reducing revenue streams and simultaneously changing demographics and increasing customer-led demand for services. In order to meet these challenges, it may be necessary to take calculated risks and to seize properly risk-assessed opportunities as they arise. Risk management in this context requires actions which maximise benefits whilst simultaneously minimising threats to success. This is referred to as upside risk management."

1.2 Therefore, risk management should be applied throughout the Council's structure, from the overall Council approach through the Corporate Management Team, to each and every employee of the Council.

1.3 The objective of this audit was to provide assurance over the risk management arrangements that are currently in operation within the Council.

1.4 The factual accuracy of this report and action to be taken with regard to the recommendations made have been agreed with Fraser Bell, Chief Officer – Governance, Vikki Cuthbert, Assurance Manager, and Ronnie McKean, Corporate Risk Lead.

2. FINDINGS AND RECOMMENDATIONS

2.1 Written Policies and Procedures

2.1.1 The current Risk Management Framework was approved by the Audit, Risk and Scrutiny Committee in February 2018. It was then published in April 2018 and was due for review in April 2019. Review of the framework is currently ongoing, and the expected completion date is December 2019.

2.1.2 The current framework combines both policy and procedural elements within it and does not clearly delineate the difference between the two. Policy decisions are reserved to Council or an appropriate Committee, and must be subject to periodic review, whereas operational procedures are developed, updated and applied by Officers. There is a risk of reducing operational flexibility by presenting both in combination, as future operational updates will need to wait for policy approval before they can be implemented.

Recommendation
There should be clear separation between risk management policy and procedures.

Service Response / Action
Agreed. The Corporate Management Team approved a Policy Framework in May 2019 and this is now being implemented corporately. One of the aims of the Framework is to separate policy from associated procedures. The Risk Management Framework is currently being reviewed in accordance with that Framework and will be presented as a Risk Management Policy to the Audit, Risk and Scrutiny Committee in December. Associated procedures and guidance will be developed at the same time.

Implementation Date	Responsible Officer	Grading
December 2019	Corporate Risk Lead	Important within audited area

2.1.3 The current framework covers all areas required in the process of analysing and rating risks. It also describes how to rate controls and mitigants and track them. Additional supporting documentation provides more detail in some areas, including risk identification techniques.

2.1.4 The Risk Management Framework states that development and adoption of a risk appetite statement will be considered. The Council does not currently have a defined risk appetite. Development and adoption of a risk appetite would provide a clearer basis for identifying and addressing the most relevant risks, and support decisions to take on further risks, or not to mitigate certain risks, where this may be appropriate.

Recommendation
A risk appetite should be established and documented.

Service Response / Action
Agreed. This is a key workstream within Governance and will help to ensure that our risk management approach is fully embedded and understood at all levels of the organisation. Instruction to develop risk appetite will be sought from Audit, Risk and Scrutiny Committee in December 2019 and this will be reported next year.

Implementation Date	Responsible Officer	Grading
June 2020	Corporate Risk Lead	Significant within audited area

2.1.5 The majority of information available about risk management is accessible to all employees of the Council from the 'Risk Management' page within The Zone. However, some of the information on this page is out of date, in that it refers to systems and Officers that are no longer part of the process. There is also no directly accessible link to current risk registers, to aid staff in their understanding of the risks affecting their work.

2.1.6 The risk register template within the framework covers all areas required within a risk register and ensures that there is a good level of supporting detail. However, this is only available within the framework document on The Zone as a page within a PDF document which does not make it accessible for those looking to create a new risk register. A project is ongoing to develop a new system for recording and managing risks in a more accessible manner.

2.1.7 The Risk Management Framework mentions that Programme / Project risk registers are used to deal with risk which "could hamper or terminate the delivery of one of our major programmes or projects, potentially impacting on the functional or corporate tiers of risk." However, the template for these is not available on the Risk Management Page within The Zone. It is available on the Project Management Page within The Zone but is formatted differently to the Corporate and Cluster risk registers. Variations between different levels of risk register presents a risk that important information may be missed or not flow through to the appropriate level.

Recommendation
Risk Management information and templates should be updated on The Zone.

Service Response / Action
Agreed. Short term measures will be taken to make templates available in one location on the Zone. Consistency between templates will be addressed as part of the Assurance 365 project, which aims to digitise governance processes and improve accessibility and reporting.

Implementation Date	Responsible Officer	Grading
December 2019	Corporate Risk Lead	Important within audited area

2.1.8 Project and programme risk registers are also not collated centrally or reviewed regularly by the Corporate Risk Lead. Whilst during the project or programme's lifetime it will be subject to its own agreed governance processes, this means that risk management information may not be derived consistently across all of the Council's activities.

Recommendation
Project risks should have a clear link / escalation process to other levels in the risk management framework.

Service Response / Action
Agreed. This will also be addressed as part of the Assurance 365 project.

Implementation Date	Responsible Officer	Grading
December 2019	Corporate Risk Lead	Important within audited area

2.2 Risk Registers

2.2.1 The corporate risk register is maintained by the Corporate Risk Lead and is reviewed monthly, in detail, by the Corporate Management Team (CMT) and annually by the Audit, Risk and Scrutiny Committee.

2.2.2 The register contains details and descriptions of what are considered to be the most significant risks and their impact, a risk rating derived from severity of impact and anticipated likelihood, details of mitigants and controls and consideration of their effectiveness (with explanations and action plans to bring these to fully effective where required), residual risk, dates for the completion of control actions, risk owners and risk managers. The format should be used as the template for all risk registers as per the Risk Management Framework.

2.2.3 While the majority of Cluster risk registers matched the formatting described within the Risk Management Framework, the Operations and Protective Services risk register is presented in a different format. It does not include a clear definition of the level of risk before and after mitigation and controls, review dates, assurance of the effectiveness of mitigants and controls, a specific risk owner, and a specific risk manager. Additionally, it contains risks that are being managed at a corporate level, such as the EU Exit.

Recommendation
The standard risk register format should be used across the Council.

Service Response / Action
Agreed.

Implementation Date	Responsible Officer	Grading
December 2019	Corporate Risk Lead	Significant within audited area

2.2.4 CMT has agreed with the Senior Management Teams (SMTs) of the various Clusters that their risk registers should be reviewed monthly at their SMT meetings. However, the only written instructions relating to updating registers is within the Risk Management Framework, which states that reviews at this level require to be completed quarterly. Whilst Officers stated that registers are being reviewed monthly and were able to demonstrate their inclusion on management team agendas, this did not always result in updated registers – in some cases review dates had passed for specified actions in response to identified risks but no updates had been appended.

2.2.5 There is currently no update and sign-off process to demonstrate that registers are being 'reviewed' to a specified extent at the required frequency – the only indication is where dates within various sections of the document change between one version and the next. Without regular review new and emerging risks may be missed and controls and mitigants may not be in place to address the associated impact.

2.2.6 In contrast, Corporate risks tend to be longer term than those on Cluster registers and therefore may not change significantly on a monthly basis. Whilst regular CMT review is positive and reflects the prioritisation of risk management within the organisation, once the Risk Management Framework is more fully developed and embedded an exception reporting mechanism may provide sufficient assurance at this level.

2.2.7 Cluster risk registers are reviewed annually by the Corporate Risk Lead before being presented to the Audit, Risk and Scrutiny Committee, and the aligned Policy Committee for the relevant Cluster. There is currently no independent scrutiny of Cluster registers on a more regular basis. Whilst risks and the associated actions are owned and managed by appropriate Officers within each Cluster, it will be difficult for them to objectively appraise their own mitigating controls. Separate review by the Corporate Risk Lead or a form of peer review by other Clusters, on a periodic basis, could enhance compliance, provide challenge where appropriate, and encourage cross-seeding of ideas.

2.2.8 Risks may be escalated to higher level registers or de-escalated to lower level registers. De-escalated risks are those which are considered to no longer affect the relevant Cluster, or for which mitigants and controls are considered fully effective. It will also include risks which management have decided to accept and not mitigate against. In any case it is important that the risks are still given periodic consideration, as circumstances and the effectiveness of controls may change.

2.2.9 Escalating risks provides the opportunity for the next tier of management to consider them and determine whether additional actions are required. De-escalating risks removes them from the relevant register. There are no formal controls over de-escalating risks – i.e. to ensure they are added to a lower level register, and only removed where appropriate and agreed. Within the Cluster Risk Registers only the Governance Risk Register continues to track risks that have been de-escalated. While this method has been shared with other Clusters it is not yet in use.

2.2.10 The Risk Management Framework also indicates that assurance mapping should be carried out to demonstrate consideration of the strength of the sources of assurance in respect of mitigating controls over risks. Assurance maps have been developed in relation to Corporate Risks and Bond Governance, though only the latter has been scored to demonstrate the current level of assurance provided by each source.

Recommendation
The extent and frequency of risk register reviews, and their recording, should be reviewed.

Service Response / Action
Agreed. This will be determined within the Risk Management Policy (previously Framework) when it is presented to Committee.

Implementation Date	Responsible Officer	Grading
December 2019	Corporate Risk Lead	Significant within audited area

AUDITORS: D Hughes
C Harvey
C Johnston

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	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. Financial Regulations have been consistently breached.
Significant within audited area	Addressing this issue will enhance internal controls. An element of control is missing or only partial in nature. The existence of the weakness identified has an impact on a system's adequacy and effectiveness. Financial Regulations have been breached.
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.