1. Audit Summary – Risk Management Review

Background and Context

1.1 Risk management is the culture, process and structures that are directed towards effective management of potential opportunities and threats to the Council achieving its priorities and objectives and is a key element of the Council's governance framework. Under the NAO Code of Audit Practice 2020 and Value for Money requirements, the Council must have in place effective arrangements for the management of risk.

1.2 An internal audit review of risk management takes place annually to enable the Chief Internal Auditor to provide an opinion on risk management arrangements, which in turn informs the overall opinion on the Council's internal control, governance and risk management arrangements.

1.3 This review was undertaken in February 2022 as part of the Internal Audit Plan for 2021/22. A follow-up of management actions from the previous review of risk management (May 2021) was also undertaken.

Scope and Objectives

1.4 The scope of the assignment included the following areas:

- Consideration of how the Council ensures it has identified a complete list of key risks relevant to the Council;
- Assessment of whether these risks are adequately defined and properly understood;
- Assessment of the extent to which clear actions and milestones have been set to effectively mitigate and manage identified risks;
- Assessment of the extent to which risk owners are held to account in the delivery of actions to mitigate risks and drive improvement or that senior management has accepted the risk of not taking action; and
- Assessment of the extent to which risks impacted by Covid-19 have been considered and managed within the Risk Management framework.

Audit Opinion

1.5 Overall, Internal audit obtained **limited assurance** that effective risk management measures were in place.

Key Messages and Findings:

1.5.1 We recognise the significant progress which has been made in developing the tools and resources to improve the clarity and ease of risk management processes and to facilitate effective discussion of risk at DMT, EDM, CMB and CLB meetings. Indeed, all but one of the management actions identified in our May 2021 report, have been implemented. The remaining action related to undertaking a cultural review is in progress and due for completion by September 2022. We also noted clear evidence of risks impacted by the pandemic being considered and managed.

1.5.2 The new risk management systems, processes, guidance and training are being rolled out but, in some areas, improvements are in their infancy and remained to be embedded at the time of our audit. Clarity is required on some risk definition and to improve staff understanding of roles and responsibilities. The Council is continuing to provide training, support and briefings to teams to embed improvements further and improve the evidence of its operation and effectiveness, through audit trails and risk reporting

1.6 We raised one high priority, three medium priority and two low priority findings. These have been grouped as follows:

1.6.1 **Management and mitigation of risks:** The high priority finding related to review of the trajectory of the current risk scores against tolerance risk scores over the last year highlighted a lack of clear review and challenge where risk tolerance scores are unlikely to be met and it may be necessary to consider the effectiveness of the mitigating actions and whether they are the right mitigating actions.

1.6.2 For each of the three risks sampled, the risk owner could demonstrate progress made with the actions set out in the corporate risk report to manage the risk. However, risk reports and Pentana did not always fully reflect all actions being taken. We understand from discussions with leadership that to enable the appropriate focus managers have sought to record more concise / succinct updates. However, for CRR35 (Organisational resilience) the main emphasis of actions being taken related to workforce resilience, and this was not clearly referred to in the risk report or captured in Pentana.

1.6.3 **Risk definition and recording:** Internal audit reviewed the risk definitions of three sampled risks. From the information provided in the Corporate Risk Report we identified overlap in the definitions of two of the risks, and in the actions and progress summarised for each. For example, the scope of risk CRR35 was broad in nature, and encapsulated a multitude of smaller sub-risks, which need to be managed across various Council departments, making it difficult for one owner to manage all aspects of the risk and commission actions across the Council.

1.6.4 From discussion with individuals involved in the management of risk, we found that, at the time of our audit, the quality and detail of risk discussions held at DMT was inconsistent across divisions, and whilst guidance is available on the Pentana risk portal, some staff still lacked clear understanding around their responsibilities for adding risks to the risk register.

Management Response

1.7 The findings of the report have been accepted by management who have agreed management actions to address them. These include:

- Holding meetings and workshops with all Corporate Risk Owners to review and re-baseline corporate risks;
- Explore the use of sub-risks within Pentana where key interdependent or overlapping risks are identified;
- Corporate Risk Management Group will regularly review and challenge risk definitions;
- Guidance updated so that inherent and residual risks are frequently considered (including as part of the Council's business planning process);
- DMT/EDM risk reports to provide information on current risk status, outstanding actions, forecast direction of travel and proposed action if the residual risk is beyond tolerance;
- Roll out a continuous programme of training and support to new risk owners; and
- Continue support to and attendance at DMTs by the Risk and Insurance Team.