Report to Audit Committee

Mazars External Audit Recommendations

Portfolio Holder: Councillor Abdul Jabbar MBE – Deputy Leader and Cabinet Member for Finance and Low Carbon

Officer Contact: Anne Ryans, Director of Finance

Report Author: Mark Stenson
Ext. 4783

23 June 2020

Reason for Decision

Following the 2018/19 Statement of Accounts audit, the Council's external auditors, Mazars, made recommendations in the Audit Completion Report. In line with best practice principles, the Council implemented the recommendations in the workplan for 2019/20 and as part of the preparation of the Council's 2019/20 Statement of Accounts.

Executive Summary

The report sets out the Council's response to the recommendations highlighted in the Mazars Audit Completion report for 2018/19. The recommendations centred mainly around the Council's general IT controls.

Recommendations

It is recommended that the Audit Committee notes the responses to the recommendations highlighted by the Council's external auditors, Mazars, in the Audit Completion Report and how the Council has implemented the recommendations in the Council's general IT controls.

1. Background

1.1 This report presents the Council's response to the recommendations highlighted in the 2018/19 Audit Completion Report provided by the Council's external auditors, Mazars, on completion of the 2018/19 Statement of Accounts audit.

1.2 The recommendations centre mainly on the Council's general IT controls. When Mazars had completed their testing of IT general controls they concluded that the controls in place were designed effectively, operating as expected and while there were no control deficiencies identified, their audit work identified some minor matters which resulted in three low priority recommendations.

1.3 The recommendations on the general IT controls related to the following policies:

- Corporate Information Security Policy
- IT Backup Policy
- IT 'Logical Access' Policy

2. Corporate Information Security Policy

2.1 During the 2018/19 audit it was highlighted that the Council's Corporate Information Security Policy was dated 2009. Although the auditors found no control deficiencies in their testing of access controls, as IT and Cyber-related risks have changed in the past 10 years it is important to ensure that the Council's Policy is up to date and able to respond to the new challenges and risks. The recommendation was that the Council review and update its Corporate Information Security Policy.

2.2 The Council has reviewed and updated the Corporate Information Security policy. The landscape of risks and threats to the secure management of information is constantly evolving. The Information Management Team (IMT) provide timely advice and guidance depending on threat profile. This is provided through various forms of communication including staff communications and content on the IMT intranet pages. The policy informs staff to ensure they are kept up to date with guidance provided by IMT considering the evolving landscape of risk. The Corporate Information Security Policy dated 2009 has been removed from the intranet. The policy was updated in May 2019 and also in May 2020 and this has been placed on the intranet.

3. IT Backup Policy

3.1 Although the Mazars testing of IT General Controls did not include testing the operating effectiveness of the Council's IT backup routines, they did however note from their discussions and walkthrough testing that the Council does not have a formal documented Backup Policy. The recommendation was that the Council should consider documenting a formal Backup Policy.

3.2 Referenced within the Corporate Information Security Policy, to fulfil its responsibility of maintaining and implementing technical controls relative to the security and resilience of the ICT estate, Unity ICT will introduce, manage and enforce relevant policies as part of their Service Management System. As such, Unity ICT is responsible for the establishment of backup procedures for the retrieval of vital data in accordance with business objectives for servers, databases and other key systems. The scope of this responsibility covers any information held locally within Oldham and/or any externally hosted data where the third-party contractual relationship resided with Unity ICT. In fulfilling its responsibility Unity ICT have introduced an Information Backup policy, dated February 2020.

4. **IT 'Logical Access' Policy**

4.1 Following discussions during the 2018/19 audit, Mazars identified that the Council did not have a formal logical access policy, to set out the approach and procedures for areas such as granting new starters IT access, removing leavers' IT access and maintaining appropriate access for existing staff. Although testing confirmed that the Council did have controls in place to ensure access is set up, removed, and maintained appropriately, this wasn't governed by a formal policy. The recommendation was that the Council should consider documenting a formal logical access policy.

4.2 The Council as part of annual review, updated the IT Access Control Policy in March 2020. IMT are working with the Deputy Senior Information Risk Officer of the Council to further understand processes, carry out process reviews and development relating to new starters IT access, removing leavers IT access and maintaining appropriate access and ensuring controls are reflected in and governed by the policy.

5. **Options/Alternatives**

5.1 The options that Audit Committee Members might consider in relation to the contents of this report are:

a) note the Council's response and implementation of the recommendation highlighted in the 2018/19 Audit Completion report.
b) not to note the Council's response and implementation of the recommendation highlighted in the 2018/19 Audit Completion report.

6. **Preferred Option**

6.1 The preferred option is option a at paragraph 5.1 (a).

7. **Consultation**

7.1 Consultation has taken place with the Councils External Auditors, Mazars LLP.

8. **Financial Implications**

8.1 There are no financial implications included within this report.

9. **Legal Services Comments**

9.1 There are no Legal implications.

10. **Co-operative Agenda**

10.1 Improving the quality and timeliness of the financial information available to citizens of Oldham supports the cooperative ethos of the Council.

11. **Human Resources Comments**

11.1 There are no Human Resource implications.

12. **Risk Assessments**

12.1 The report sets out that the Policies have been updated as required. In relation to the IT Logical Access Policy there is an ongoing review to support the policy ensuring access for leavers is removed in a timely manner (Mark Stenson)

13. **IT Implications**

13.1 IT implications are included within this report.

14. **Property Implications**

14.1 There are no Property implications.

15. **Procurement Implications**

15.1 There are no Procurement implications.

16. **Environmental and Health & Safety Implications**

16.1 There are no Environmental and Health & Safety implications as a result of this report.

17. **Equality, community cohesion and crime implications**

17.1 There are no equality, community cohesion and crime implications.

18. **Equality Impact Assessment Completed?**

18.1 Not Applicable

19. **Key Decision**

19.1 No

20. **Key Decision Reference**

20.1 Not Applicable.

21. **Background Papers**

21.1 The following is a list of background papers on which this report is based in accordance with the requirements of Section 100(1) of the Local Government Act 1972. It does not include documents which would disclose exempt or confidential information as defined by the Act:

Background papers and policies for internal use only are available on the Council's intranet.

22. **Appendices**

22.1 Not Applicable