City of BRADFORD METROPOLITAN DISTRICT COUNCIL

Report of the Assistant Director of Transformation and Change to the meeting of the Governance and Audit Committee to be held on 29 November 2018

X

Subject:

External Audit Report Recommendations IT Update.

Summary statement:

This report shows the Council's progress on implementing two External Audit Recommendations from the 2016 review undertaken by Mazars.

David Cawthray
Assistant Director of Transformation and Change

Keith Hayes
Head of IT Services

Report Contact: Colum Sheridan-Small
Customer Service and Compliance Manager
Phone: (01274) 434047
E-mail: colum.sheridan-small@bradford.gov.uk@bradford.gov.uk

Portfolio: Leader and Corporate

Overview and Scrutiny Area: Corporate

1. SUMMARY

1.1 The Council's external auditors Mazars undertook an audit in the first quarter of 2016 to assess a selection of key Council IT systems as part of the audit of the financial statements.

1.2 Two recommendations from the report remain outstanding and were identified as such in the 2017 external audit report on IT.

1.3 The outstanding recommendations were aimed at improving two areas managed by IT Services. Namely the process for managing the close down of computer accounts when staff leave the organisation referred to as "the Leavers" process, and the management of the annual review and testing of key Council IT systems in line with the Council's Business Continuity planning process. A revised plan to implement the two recommendations is attached. (See appendix A).

2. BACKGROUND

2.1 The Council has many IT systems that support internal back office processes and support the delivery of services to citizens. A number of these IT systems are deemed critical due to the safeguarding and financial implications associated with them. As part of the annual external audit process Mazars test these critical IT systems to ensure that adequate controls are in place to prevent information loss, protect information integrity and to block unauthorised access to information.

2.2 The audit process requires the Council to provide a range of information on the use and management of the IT systems selected for review. Typically this is evidence of documentation for managing who accesses the system, how IT system updates are managed with formal change process controls and the technical security measures and processes that are in pace to preserve IT system integrity.

2.3 Mazars adopted the following approach while undertaking the 2016 and 2017 IT audit reviews.

2.3.1 Objective

As part of the audit of the financial statements for the period ending 31st March 2016 the objective of this work is to provide an assessment on the design & implementation and operating effectiveness of key IT General Controls of applications supporting the aforementioned financial statements of the City of Bradford Metropolitan District Council.

2.3.2 Approach

Our review of the IT General Controls covers the following areas:

- Security;
- Change Management; and
- IT Operations.

And is performed according to the following approach

- Understanding the IT environment;
- Controls testing;
- Reporting the key findings.

2.3.3 **Limitations**

- We have been focused on SAP, AIM, Swift AIS / SystmOne, CommCare / Controcc and Northgate as the key systems materially relevant for the financial statements.
- The scope of our work is strictly limited to the context described in this document.
- Our findings should not be considered as a comprehensive record of all weaknesses that may exist or improvements that could be made.

.

2.4 Once the requested information is passed over to the auditors, Mazars, then carry out an off-site review of the information provided. Based on the review areas of risk are identified along with recommendations to resolve them. The two outstanding recommendations are identified below:

Recommendation 1

2.4.1 In order to ensure proper and timely recovery in case of a disaster or major incident, we recommend testing the Disaster Recovery Plan at least on an annual basis.

Recommendation 2

2.4.2 In order to avoid unauthorised access to the Council's network and programs, we recommend ensuring that formal access disabling requests are issued for all leavers before their leaving date.

2.5 IT Services started to work on the recommendations and developed “Business Continuity” and “User Access” plans to address the areas of concern. The plans to address both recommendations became protracted due to operational issues.

2.6 IT Services undertook an assessment of the Council’s IT Disaster Recovery capability and a rolling programme of annual IT infrastructure testing was established. The outstanding activity was to establish an annual Disaster Recovery plan involving Council departments for testing the Council’s critical IT systems.

2.7 A Leavers process to manage “user access” was developed by December 2017 but required further refinement. IT Services had mitigated areas of concern raised by the external auditor by improving internal “user access” management processes and applying technical improvements to the existing Leavers system as an interim solution.

2.8 The following paragraphs provide the current position on both recommendations and the plans to complete their implementation.

Business Continuity

2.9 IT Services are engaged with the Council departments considered to be primary in progressing this work along with the Council's Emergency Planning team to determine the IT requirements in a Disaster Recovery situation. These departments are Health and Wellbeing, Children's Services and Revenues and Benefits Services. IT Services will continue to work with the Emergency Planning team and extend the scope to include Financial Services, HR and other departments across the Council.

2.10 A plan is being developed to manage this activity which will result in the identified departments undertaking a "desktop" IT Disaster Recovery scenario walkthrough of their business continuity plan. This activity will be reviewed annually and next year will see a planned coordinated IT system outage with a selected IT system in each department. This will be a rolling programme of activity as IT Services works with each of the Council departments to formalise and schedule their IT Disaster Recovery testing plans.

User Access

2.11 The scope of the originally planned "leavers" process was extended to include new starters and employee movement across the Council and was agreed with key IT Services teams who are involved with the User Management process. This resulted in a re-scoped project called "User Management" being initiated to incorporate Cherwell workflow processes for new starters, movers and leavers as an end to end solution. After significant consultation with departmental stakeholders a new workflow and supporting system is being developed and is scheduled to go live in March 2019**.**

2.12 It has to be noted that while this project work has been underway and since the external audit recommendations were issued, existing user management systems have been updated to improve the management of staff leaving the organisation. To further support this IT Services have been undertaking a review of network logon accounts to ensure none are missed within the current leavers process, any identified account issues are followed up with the relevant Council departments to validate if their removal is appropriate.

2.13 Once the user management system goes live in March 2019, the external audit Recommendation 2 will have been implemented.

2.14 A follow on piece of work will then be conducted to further automate the process across HR and Payroll.

3. OTHER CONSIDERATIONS

3.1 There are no other considerations.

4. FINANCIAL & RESOURCE APPRAISAL

4.1 There are no financial issues arising at this point.

5. RISK MANAGEMENT AND GOVERNANCE ISSUES

5.1 There is risk associated with not undertaking an annual review and testing of Council IT systems from a business continuity perspective. Annual review and testing ensures that the business continuity requirements of the service are matched to the Council's IT Disaster Recovery provision and meet the changing needs of the service. This also provides an assurance that the IT Disaster Recovery systems will work when invoked.

5.2 Existing IT user access controls and supporting manual review processes manage the risk of any unauthorised access to the Council's IT systems. The Council's IT systems and infrastructure conforms to the Governments Public Services Network Authority compliance framework which provides a high level of technical assurance.

6. LEGAL APPRAISAL

6.1 While there is no legal mandate to undertake an annual review and testing of Council IT systems, there are Data Protection Act (DPA) implications for holding information linked to computer accounts of staff who have left the organisation beyond the agreed retention period.

7. OTHER IMPLICATIONS

7.1 EQUALITY & DIVERSITY - no direct implications
7.2 SUSTAINABILITY IMPLICATIONS - no direct implications
7.3 GREENHOUSE GAS EMISSIONS IMPACTS - no direct implications
7.4 COMMUNITY SAFETY IMPLICATIONS - no direct implications
7.5 HUMAN RIGHTS ACT - no direct implications
7.6 TRADE UNION - no direct implications
7.7 WARD IMPLICATIONS - no direct implications
7.8 AREA COMMITTEE ACTION PLAN IMPLICATIONS
(for reports to Area Committees only) - no direct implications
7.9 IMPLICATIONS FOR CORPORATE PARENTING - no direct implications
7.10 ISSUES ARISING FROM PRIVACY IMPACT ASSESMENT - no direct implications

8. NOT FOR PUBLICATION DOCUMENTS – none.

9. OPTIONS – none.

10. RECOMMENDATIONS

10.1 That the update on the External Audit Report Recommendations relating to the Council's Information Technology systems be noted.

11. APPENDICES

11.1 Appendix A - External Audit Recommendations Implementation Plan

12. BACKGROUND DOCUMENTS .

12.1 Mazars – IT Audit Conclusions Report for 2016.
12.2 Mazars – IT Audit Conclusions Report for 2017.

Appendix A - External Audit Recommendations - Implementation Plan								
External Audit Recommendations	Actions	Sep-18	Oct-18	Nov-18	Dec-18	Jan-19	Feb-19	Mar-19
User Access								
User Management Implementation.	Project Go-Live.							
Business Continuity								
Determine IT DR Requirements	Meetings with senior operational managers in H&WB, Children's and Revs and Bens.							
Assess department IT DR requirements against existing IT DR capacity.	IT Services teams to assess IT system requirements against existing IT DR infrastructure and provide capability statement.							
Test the departments IT DR Business Continuity Plans.	Undertake "desktop" scenario disaster recovery walkthrough with senior managers from each department.							
Establish Annual Review Process.	Establish annual review of IT DR requirement in line with department business continuity planning process.							