EXETER CITY COUNCIL

AUDIT AND GOVERNANCE COMMITTEE
12 MARCH 2014

INTERNAL AUDIT PROGRESS REPORT

1. PURPOSE OF THE REPORT

1.1 To report on internal audit work carried out during the period 1st October to 31st December 2013, to advise on overall progress against the Audit Plan and to report any emerging issues requiring consideration.

2. BACKGROUND

2.1 This Committee is responsible for the implementation and active monitoring of audit processes and actions, which includes performance against the annual audit plan, reviewing quarterly internal audit progress reports and seeking responses and assurance from management regarding audit recommendations that have not been accepted or those not implemented within a reasonable timescale. The 2013/14 Audit Plan was approved at Scrutiny Resources Committee on 20th March 2013 and a revision to the plan was approved by this committee in November.

2.2 The purpose of Internal Audit is to provide an independent and objective review of the adequacy and effectiveness of the Council's arrangements for internal control, risk management and governance. The activities we audit are given an assurance rating as follows:

Excellent	★★★★★	The areas reviewed were found to be well controlled, internal controls are in place and operating effectively. Risks against achieving objectives are well managed.
Good	★★★★	Most of the areas reviewed were found to be adequately controlled. Generally risks are well managed but a few areas for improvement have been identified.
Some improvement required	★★★	There is a basic control framework in place, but not all risk are well managed and a number of controls are required to be strengthened.
Significant improvement required	★★	Most of the areas reviewed were not found to be adequately controlled. Risks are not well managed and require controls to be strengthened to ensure the achievement of system objectives
Fundamental weakness	★	Controls are seriously lacking or ineffective in their operation. No assurance can be given that the system's objectives will be achieved

3. WORK UNDERTAKEN

3.1 Internal Audit's objective is to examine the Council's financial and non-financial systems to check that there are adequate internal controls in place to prevent loss due to frauds, errors and inefficiency, and due attention is paid to corporate governance and risk management.

3.2 A summary of progress against the annual audit plan to date is shown at Appendix A, together with the current status of each area for review and the outcomes of the review, where completed.

3.3 The table is based on the audit plan and the systems grouped into the twelve strategic purposes as per the Corporate Plan.

3.4 A further summary of the outcomes of audits completed can be found at Appendix B.

3.5 Progress against the annual audit plan is on target.

4. ISSUES FOR CONSIDERATION

Recommendations Not Accepted

4.1 ICT Operations Management - report issued 4th November 2013 - Medium Risk

ICT have recently purchased a new piece of software to allow audit logs to be monitored and better managed. In order to try and help reduce the storage capacity required for such logs a recommendation was made to conduct a risk assessment to determine:
a) which audit logs need to be maintained
b) what information the audit logs must contain
c) how they should be monitored and by whom
d) how long they should be retained for
And that written procedures on monitoring audit logs should be updated to incorporate the results of the risk assessment. All relevant staff should be made aware of them.

The ICT Customer Services Manager, did not agree with this recommendation and advised that:

"This would not be practical as audit logs for different applications may have different retention requirements. As the current backup process generally involves taking a copy of a whole server it would not be practical to scan the tapes to identify and delete individual audit logs"

4.2 ICT Operations Management - report issued 4th November 2013 - Medium Risk

The Council allows the use of its own authorised USB safesticks (memory sticks) or other removable devices provided there is genuine business need and the relevant manager has authorised the use of such. However, it was found that there does not appear to be any agreed process in place to ensure that safesticks are recovered and disabled when staff leave. There is also no process to recover/disable safesticks issued for temporary use at the end the period. The audit identified cases where staff had left and sticks had not been returned. Therefore, a recommendation was made that:
a) written procedures should be produced for the return/disabling of safesticks from staff that are leaving or no longer have authorisation for a stick;
b) that the procedures should include:

- the immediate disabling of a safestick on the date an employee leaves (obtained from the leavers form);
- the input of review/diary dates to disable safesticks at the end of the temporary issue period

The ICT Customer Services Manager, did not agree with this recommendation and advised that:

"It was not always easy to identify leavers and to retrieve their safesticks. He sometimes only receives notification of a leaver within a few days of them leaving or even after they have left, making it difficult to retrieve the safestick. Staff will ensure that safesticks are immediately disabled on the date an employee leaves, if notified. The calendar facility on the CMDB system will be used to input diary/review dates for safesticks on temporary issue."

4.4 During the second quarter of this year, there are no instances of management accepting a recommendation which was not subsequently implemented within a reasonable timescale.

5. RECOMMENDATIONS

5.1 That the Internal Audit Progress Report for the third quarter of the year 2013/14 be noted.

5.2 That the Committee decide whether the audit report recommendations not accepted by management, as detailed in section 4 above, are acceptable risks to the Council.

Audit Managers

Local Government (Access to Information) Act 1985 (as amended)
Background papers used in compiling this report: None