Financial Scrutiny and Audit Committee
10 February 2015
Agenda Item No 11

Implementation of Internal Audit Recommendations: Summary of Progress

Report by Head of Finance

Summary:	This report updates members on progress in implementing Internal Audit recommendations arising out of audits carried out since 2013/14.
Recommendation:	That the report be noted.

1 Introduction

1.1 It has been agreed that this Committee will receive a regular update of progress made in implementing Internal Audit report recommendations, focusing on outstanding recommendations and including timescales for completion of any outstanding work.

1.2 This report summarises the current position regarding recommendations arising out of internal audit reports which have been produced since 2013/14. It sets out in the appendix details of:

- recommendations not yet implemented
- recommendations not implemented at the time of the last meeting which have since been implemented
- new recommendations since the last meeting

2 Summary of Progress

2.1 In the previous report to this Committee in September, one medium priority recommendation relating to Procurement policies and procedures was identified as outstanding. This has now been completed. Details of all actions taken are set out in the appendix.

3 Internal Audit Programme 2014/15

3.1 End User Controls

3.1.1 An audit of End User Controls was completed in December, receiving an “adequate” audit opinion with three medium and five low priority recommendations being raised.

3.1.2 The audit consisted of a review of the systems and controls in place on Authority issued devices such as PCs, mobile devices such as laptops and smartphones, to mitigate the loss of these devices and the data contained on them.

3.1.3 The audit identified the following areas of weakness:

- Screensaver controls that lock a user's PC or laptop when not in use should be deployed to mitigate the risk of unauthorised access to the network and help to ensure the security of the network
- Mobile device password controls should be implemented to improve the security of the Blackberry devices and reduce the risk of unauthorised access
- Controls over USB devices needs to be introduced to protect the Authority's data and ensure the security of the network

3.1.4 A number of positive finding were identified in relation to:

- There are controls in place to help prevent non-IT users from installing unauthorised applications
- PC, laptop and mobile device procurement is controlled via a centralised IT budget that the Head of IT monitors
- Unauthorised devices cannot connect to the network and gain access to network resources
- Mobile devices (primarily Blackberry devices) are encrypted by default;
- Blackberry devices are managed by the Blackberry Enterprise Server, which allows for the remote wipe of connected devices should they be lost or stolen
- There are processes in place that effectively act as asset reviews via the use of Anti-Virus and patch management systems

3.1.5 The eight recommendations raised have been agreed and actions are identified to deliver these. Details of which are set out in the appendix.

3.2 Another audit has been undertaken since the last meeting of the Committee on the Consultation Activities and Partnership Provisions Audit. The outcomes from this will be reported to the next committee meeting. An audit of the regular annual Key Controls audit will be undertaken in quarter four.

3.3 Details of actions to date in response to outstanding recommendations are set out in the appendix.

Background papers:	None
Author:	Emma Krelle
Date of report:	28 January 2015
Broads Plan Objectives:	None
Appendices:	APPENDIX 1 – Summary of Actions / Responses to Internal Audit Recommendations 2013/14 – 2014/15

Summary of Actions / Responses to Internal Audit Recommendations 2013/14 – 2014/15

Procurement: October 2013

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
3.	**Purchase Ledger Review** Monitoring and reporting of data from the purchase ledger should be undertaken on a periodic basis. In particular, a review of aggregate supplier spending (cumulative total of >£5k), should be undertaken to determine whether correct procurement procedures have been applied. This analysis should be undertaken in line with the review of the Contracts Register to determine whether the Contracts Register includes all contracts. Instances of non-compliance with Contract Standing Orders should be reported to senior management and recurring issues identified to inform staff training.	Medium	Head of Finance	Completed. The aggregate supplier spend data for 2013/14 has been reviewed as part of year-end processes. Of the 36 suppliers identified as part of the review Management Team reviewed the procurement processes used and agreed that the procurement methods had been appropriate. In future an annual review of aggregate supplier spend and the contract register will be undertaken after the financial year end.	By 30/04/2014 Revised Target Date: 31/10/2014

APPENDIX 1

Summary of Actions / Responses to Internal Audit Recommendations 2013/14 – 2014/15

End User Controls: December 2014

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
1.	**Screensaver configuration** The Authority should deploy screensaver controls that include the following: • The configuration of a default screensaver that cannot be changed by the user; • Implementation of an appropriate screen lock timeout, i.e. 10 minutes after inactivity, that initiates the screensaver automatically; and A requirement for the user to re-enter their network password to unlock the screensaver when returning to their screens.	Medium	Head of IT and Collector of Tolls	Agreed with the Head of IT and Collector of Tolls at the debrief meeting.	By 31/05/2015
2.	**Corporate IT Group Terns of Reference** The Authority should undertake a review of the Terms of Reference for the Corporate IT Group as the current document references individuals no longer with the Authority or where roles have changed. The review	Low	Head of IT and Collector of Tolls	Completed. Terms of Reference Reviewed and Agreed by Corporate ICT Group on 21 January 2015.	By 31/05/2015

Summary of Actions / Responses to Internal Audit Recommendations 2013/14 – 2014/15

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
	should also confirm that the group's remit continues to reflect the needs of the Authority.				
3.	**Formal Disposal Policy** The Authority should give consideration to formally documenting an IT Disposal policy.	Low	Head of IT and Collector of Tolls	Agreed with the Head of IT and Collector of Tolls at the debrief meeting.	By 31/05/2015
4.	**WEEE Destruction certificates** The Authority should ensure that a formal destruction certificate matching the receipts when items are collected, is received for every WEEE consignment.	Low	Head of IT and Collector of Tolls	Completed - Destruction certificates obtained for equipment recycled in 2014.	By 31/05/2015
5.	**Laptop hardware encryption** The Authority should give consideration to deploying hardware encryption to every laptop under its control.	Low	Head of IT and Collector of Tolls	Agreed with the Head of IT and Collector of Tolls at the debrief meeting.	By 31/05/2015
6.	**Blackberry device password controls** The Authority should ensure that appropriate mobile device password controls are implemented as part of the deployment of Blackberry Enterprise Server (BES) version 12.	Medium	Head of IT and Collector of Tolls	Agreed with the Head of IT and Collector of Tolls at the debrief meeting.	By 31/05/2015

Summary of Actions / Responses to Internal Audit Recommendations 2013/14 – 2014/15

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
7.	**USB device controls** Recommendation - The Authority should ensure that appropriate controls over USB devices are implemented when Windows Server 2008 is deployed. Such controls could include the following: • Restrict usage to specific, Authority approved, devices only; • Restrict the ability to copy data to, or from, devices not permitted by the Authority; and • Ensure that appropriate Anti-Virus/Malware scanning is initiated on reading the device's data.	Medium	Head of IT and Collector of Tolls	Agreed with the Head of IT and Collector of Tolls at the debrief meeting.	By 31/05/2015
8.	**Asset tags** The Authority should initiate a process whereby all devices under its control are asset tagged and recorded within an appropriate asset register.	Low	Head of IT and Collector of Tolls	Agreed with the Head of IT and Collector of Tolls at the debrief meeting.	By 31/05/2015