Financial Scrutiny and Audit Committee
11 February 2014
Agenda Item No 13

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 2011/12.
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 2011/12. 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: and
- 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 Planning policies and procedures was identified as outstanding. This has since been completed and details are set out in the appendix.

3 Internal Audit Programme 2013/14

3.1 Two audits have been completed since the last meeting of this Committee.

3.2 Procurement (2013/14)

3.2.1 An audit of Procurement was completed in October, with the objective of examining whether procurement systems and controls were operating adequately, effectively and efficiently. This resulted in an “adequate” audit opinion with four medium and two low priority recommendations being raised.

3.2.2 The audit identified areas for improvement relating to:

- the completeness and use of the Contracts Register;
- the need for periodic analysis of the purchase ledger to identify significant aggregate supplier spend;
- two instances where waivers of Standing Orders required reporting to the Authority; and
- four contracts requiring further investigation.

3.2.3 Good practice was noted relating to the availability of up to date policies and procedures, and the communication of procurement issues and policies.

3.2.4 Two of the recommendations raised have been completed and the remaining four are currently in progress.

3.3 **Network Security (2013/14)**

3.3.1 An audit of Network Security was completed in January, receiving a "limited" audit opinion with three high, five medium and four low priority recommendations being raised.

3.3.2 The audit focused on:

- Domain accounts policies;
- Audit policy settings;
- User privileges;
- Trusted and trusting hosts;
- User accounts and passwords;
- Services and drivers;
- Home directories, logon scripts;
- Registry key settings;
- Logical drives;
- Default login accounts; and
- Discretionary access controls (DACLs).

3.3.3 The audit identified the following areas of weakness:

- the Domain accounts policy settings required review to adhere to leading practice and to help provide further security;
- a review of accounts should be undertaken whose passwords are not changed regularly to confirm that they are actively required. This will help to ensure that the number of such accounts are kept to an absolute minimum and secure the network; and
- a review of accounts that never expire should be conducted to improve security and reduce the risk of inappropriate access.

3.3.4 Medium priority recommendations were raised in relation to the following items:

- a periodic review of the Windows audit trail should be conducted to monitor key audit trail events. This will help to detect potential malicious activity on a more proactive basis;
- a review of generically-named user accounts should be conducted to ensure that the number of these is reduced where possible to increase accountability over activities;
- certain system privileges that should not be granted to users were found to have been assigned to certain user accounts. These are high privilege permissions that should only be granted to system accounts and which could compromise the network should they be granted inappropriately;
- the built-in Administrator account should not be being used and should be renamed to increase accountability; and
- a review of security option setting should be conducted to enhance security.

3.3.5 Positive finding were identified in relation to the existence of a relatively small number of user accounts, which are generally being well managed in terms of the number of expired accounts, and that the Guest account has been disabled.

3.3.6 Members may wish to note that the audit made use of a computer audit tool which benchmarked the Authority's network security against other Active Directory domains (the type of Microsoft network used by the Authority) within the Government sector. This tool found the Authority's network security to be "about average" compared with the comparator group.

3.3.7 Three of the recommendations (including one high priority) have been implemented. The remaining two high priority recommendations relate to the same area / issue of passwords used with service accounts and will be subject to review. Actions to address the remaining recommendations are in progress.

3.4 Details of all new recommendations and the Authority's actions to date in response are set out in the appendix.

Background papers:	None
Author:	Titus Adam
Date of report:	27 January 2014
Broads Plan Objectives:	None
Appendices:	APPENDIX 1 – Summary of Actions / Responses to Internal Audit Recommendations 2011/12 – 2013/14

APPENDIX 1

Summary of Actions / Responses to Internal Audit Recommendations 2011/12 – 2013/14

Planning: October 2011

Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
1. **Policies and Procedures** All planning policies and work instructions should be reviewed and updated to take account of current working practices, responsibilities and the functionality enabled by the CAPS planning system. Documents should be subject to periodic review.	M	Head of Development Management	Completed. Details of the Authority's policies and working practices have been documented and consolidated and are correct as at January 2014. These will be kept under review to take account of ongoing legislative and regulatory changes.	By 31/03/12 Revised Target Date: 31/03/13

Procurement: October 2013

Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
1. **Procurement Training** The Authority should provide a refresher procurement training exercise to officers with responsibilities for procurement.	Low	Head of Finance	Partially completed. Training has been provided to the Environment and Design Team in September and this training material made available to all staff. It is not considered practical to provide periodic procurement	By 31/12/2013 Revised Target Date: 30/06/2013

Summary of Actions / Responses to Internal Audit Recommendations 2011/12 – 2013/14

Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
			training on resource/capacity grounds. A review of finance induction training materials to ensure appropriate coverage of procurement issues is planned for early 2014/15.	
2. **Contracts Register** The Authority should review and update its contract register to confirm that all known contracts are recorded. Responsible officers for individual contracts should be identified. The Contracts Register should be a record of all current contracts and used as a management tool to identify contracts which are due to expire and as a result prompt review and timely procurement activity.	Medium	Head of Finance	The contract register will be reviewed and updated. Development work is planned with a view to integrating the records of tenders, waivers of standing orders and contracts within a single access database. The scope for capturing additional information and use of increased reporting / triggers for renewal activity will also be explored.	By 30/04/2014
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	Medium	Head of Finance	The aggregate supplier spend data for 2012/13 will be reviewed alongside the development of the updated contract register. The feasibility of undertaking	By 30/04/2014

Summary of Actions / Responses to Internal Audit Recommendations 2011/12 – 2013/14

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
	>£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.			an annual review of supplier spend and the contract register will be explored with a view to implementing a new process after the 2013/14 financial year end.	
4.	**Waivers** All exemptions to CSOs should be authorised in line with the Authority's CSOs and reported to Broads Authority. The following procurement exercises should be reviewed and reported to Broads Authority. Where appropriate, retrospective waivers/exemptions should be raised and authorised: • Toyota GB PLC - Purchase of vehicles. • Inland Dredging Services - Dredging Project.	Medium	Head of Finance Waivers: Director of Operations Head of Governance and Executive Assistant	Completed. Waivers in respect of these procurements have been prepared and were reported to the Broads Authority at its meeting 22 November 2013.	By 22/11/2013
5.	Contract Investigation	Medium	Director of	Partially completed. The	By 31/03/2014

Summary of Actions / Responses to Internal Audit Recommendations 2011/12 – 2013/14

Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
The Authority should investigate the following payments to determine whether current arrangements meet Authority CSOs and whether the Authority would benefit from implementing formalised contracts: • Octagon - Telephone maintenance contract; • Chatterbox - Audio publication supplier; • Rix Petroleum (East Anglia) Ltd - Boat fuel supplier; and • A & W Cushion Ltd - Timber supplier.		Operations Head of Comms	Authority's contract with Octagon has been renegotiated and renewed for a further year under a waiver of Standing Orders. The contract with Chatterbox will not be renewed as an alternative approach is being trialed. Work is underway to review the procurement arrangements in place with Rix Petroleum. The arrangements with the remaining supplier will be subject to further investigation.	
6. **Retention of Tender Documentation** The Authority should ensure that all tender documents are retained.	Low	Head of Finance	Completed. Tender documentation is retained as a matter of course and it is believed that this represents an isolated incident where files have been misplaced, possibly during the office relocation. The work to integrate the contract register and tender records will provide a further	18/10/2013

Summary of Actions / Responses to Internal Audit Recommendations 2011/12 – 2013/14

Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
			opportunity to review and verify whether there are any remaining gaps in records retention. Prior to this audit taking place, a reminder notice was circulated to all staff by the Head of Finance emphasising the importance of retaining tender documentation.	

Network Security: January 2014

Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
1. **Domain accounts policy** Management should conduct a review of the Domain Account Policy in the following areas: • Password complexity should be enabled; • Locked user accounts should be set to stay locked permanently and only unlocked by an administrator on request. The current setting is ten minutes, which resets a locked account automatically after that	High	Head of IT and Collector of Tolls	Completed. All recommendations have been implemented.	By 10/01/2014

Summary of Actions / Responses to Internal Audit Recommendations 2011/12 – 2013/14

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
	time period has elapsed; • Password history size should be increased to 22 or more. The setting is currently five passwords remembered; • Lockout counter in minutes should be set to 1440 minutes. The current setting is ten minutes; and • The built in administrator and Guest accounts should be renamed.				
2.	**Audit policy settings** The following audit policy events should be reviewed: • Directory service events currently set to "none"; • Object access events currently set to "none"; • Privilege use events currently set to "none"; • Process tracking events currently set to "none"; • System events currently set to "none"; and • Policy change events currently set to "Success" only. Consideration should be given to	Low	Head of IT and Collector of Tolls	Completed. Four of these settings were the default windows settings. All have been updated as recommended.	By 10/01/2014

Summary of Actions / Responses to Internal Audit Recommendations 2011/12 – 2013/14

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
	auditing failure events as a minimum and adding the Failure event to the Policy change event setting.				
3.	**Periodic review of the Windows audit trail** Management should implement a process whereby the Windows audit trail is reviewed on a regular basis.	Medium	Head of IT and Collector of Tolls	Agreed in principle. The Authority is investigating implementing a process of regular review of the Windows audit trail, although this will be a challenge given the limited resources available in the IT team.	By 01/03/2014
4.	**Accounts with generic names** Management should conduct a review of generically named accounts.	Medium	Head of IT and Collector of Tolls	Agreed in principle.	By 01/05/2014
5.	**Rights that should be granted to no one** Management should conduct a review of the permissions that should not be granted to any account as there are accounts with five of these privileges. The privileges are as follows: • Act as part of the operating system; • Adjust memory quotas for a process; • Debug programs; • Log on as a batch job; and • Log on as a service.	Medium	Head of IT and Collector of Tolls	Agreed in principle. The built-in administrator account has all five privileges whereas the user accounts have two of the privileges by virtue of inherited rights as domain admins. These privileges will be removed.	By 01/03/2014

APPENDIX 1

Summary of Actions / Responses to Internal Audit Recommendations 2011/12 – 2013/14

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
6.	**Accounts where passwords are not changed regularly** A review of all accounts where the password is not being changed regularly should be conducted to better understand whether the accounts are still required or should have their settings changed to force password changes more regularly.	High	Head of IT and Collector of Tolls	Agreed in principle. A large number of these accounts are service accounts with passwords that never expire the others are mostly group accounts. All will be reviewed.	By 01/03/2014
7.	**Accounts with passwords that never expire** Management should conduct a review of all accounts where passwords are set to never expire. Additionally, the built in Administrator account should have its password manually changed on a periodic basis, for example when a staff member who has knowledge of the password leaves.	High	Head of IT and Collector of Tolls	Agreed in principle. These are mostly service accounts, the number is currently superficially high as the new DMS system, currently under development, uses a different set of service accounts to the existing version. A review of the accounts will take place.	By 01/03/2014
8.	**Housekeeping issues** Management should conduct a review of disabled, locked and expired accounts on the domain. A review of the 23 empty local groups and 11 empty global groups should be included. A process to regularly review accounts that have been locked, disabled and/or expired should also be implemented.	Low	Head of IT and Collector of Tolls	Agreed in principle. The guest account has always been disabled the fact that it is locked out is therefore irrelevant.	By 01/06/2014

APPENDIX 1

Summary of Actions / Responses to Internal Audit Recommendations 2011/12 – 2013/14

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
9.	**The Built-in Administrator account** Management should rename the built in Administrator account and not use it on a regular basis. Ideally, named user accounts with equivalent permissions should be used instead.	Medium	Head of IT and Collector of Tolls	Completed. The built in Administrator account has been renamed.	By 01/03/2014
10.	**Regular review of services and drivers** Management should implement a process whereby a periodic, documented review of installed services and drivers is conducted.	Low	Head of IT and Collector of Tolls	Agreed in principle.	By 01/06/2014
11.	**Security option settings** Management should review the following configurations: • "Do not display last user name in logon screen" should be enabled so that the username field is blank when a user logs into the network; • "Unsigned non driver installation behaviour" should be set to "warn, but allow installation" as a minimum. The current setting of "silently succeed" is not advised; and • Implement a warning message concerning unauthorised access to the network when users log in.	Medium	Head of IT and Collector of Tolls	Agreed in principle, except Management Team has reviewed the proposal to implement a warning message concerning unauthorised access every time a user logs on and has concluded that this is unnecessary. All users are required to sign the Authority's electronic communications policy periodically.	By 01/04/2014

APPENDIX 1

Summary of Actions / Responses to Internal Audit Recommendations 2011/12 – 2013/14

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
12.	**Review of Discretionary Access Controls** Management should implement a process whereby DACLs are reviewed on a regular basis.	Low	Head of IT and Collector of Tolls	Agreed in principle.	By 01/06/2014