Financial Scrutiny and Audit Committee
14 February 2012
Agenda Item No 9

Implementation of Internal Audit Recommendations: Summary of Progress

Report by Director of Change Management and Resources

Summary:	This report updates members on progress in implementing Internal Audit recommendations arising out of audits carried out since 2008/09.
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 2008/09. 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 It is encouraging to note that only three substantive recommendations remain outstanding from audits carried out prior to 2011/12, two of which are Low priority. The most significant of these relates to the compilation of policies and procedures for the new Tolls Management System, which is on target to be implemented during February 2012. In addition work has now commenced on the review of the Fraud and Corruption Policy, which will incorporate controls to ensure that the Authority complies with the requirements of the Bribery Act 2010. The third recommendation relates to the review of a job description within the ICT Section, which has been delayed due to the extreme work pressures within the Team at the present time.

3 Internal Audit Programme 2011/12

3.1 Three audits have so far been carried out during 2011/12. Details are set out below.

3.2 Corporate Governance and Risk Management

3.2.1 This audit generated two Medium priority recommendations, both of which have been implemented, and received an "Adequate" assurance. Following the Risk Management Workshop in October 2011 the Strategic Risk Register has been reviewed and updated, and is the subject of a separate report within this agenda.

3.3 Planning

3.3.1 This also generated two Medium priority recommendations, one of which has been implemented and one of which is underway. It received an "Adequate" assurance.

3.4 Tolls Management System

3.4.1 The Authority requested that an audit be carried out of the Tolls Management System and this was subsequently performed at a time when the system was running in parallel with the legacy HARPS system and due to be fully implemented three months later, i.e. during February 2012.

3.4.2 The audit was extremely helpful in that it identified a number of issues which needed to be addressed before the system goes live, as well as some longer term issues resulting from the introduction of the new arrangements. In total nine recommendations were raised, of which one was High priority and the remainder were Medium priority. Consequently the audit received a "Limited" assurance.

3.4.3 As is the usual practice a summary of the key issues identified was reported to officers at the Audit Debrief Meeting. Procedures were put in place with immediate effect to address two of the recommendations – relating to Password Controls (the High priority recommendation) and Password Encryption – and were implemented before the final report was published in December 2011. Short timeframes were also set for a further six recommendations, all of which are scheduled for completion by the end of February 2012. This leaves one recommendation which has been assigned an implementation date of July 2012 – a slightly longer timescale was required here to enable the updating of the Corporate Business Continuity and Disaster Recovery Plans.

Background papers: Internal Audit Report BA/12/02 – Planning, dated October 2011
Internal Audit Report BA/12/04 – Tolls Management System, dated December 2011

Author: Rob Holman
Date of report: 25 January 2012

Appendices: APPENDIX 1 – Summary of Actions/ Responses to Internal Audit Recommendations 2008/09 – 2011/12

APPENDIX 1

Summary of Actions/Responses to Internal Audit Recommendations

Annual Governance Statement: September 2008

Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
6. **Fraud and Corruption Policy** The Fraud and Corruption Policy should be reviewed and updated, as appropriate, on an annual basis.	L	Director of Change Management and Resources	Not yet implemented due to other priorities.	By 31/12/10 Revised Target: 31/3/12

Toll Income: January 2009

Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
1. **Policies and Procedures** Management should compile written procedures for all aspects of toll income, e.g. identification, receipt, banking and the collection of unpaid tolls, including timescales for taking action.	M	Head of ICT and Collector of Tolls	Still outstanding pending completion of the Tolls Management System. However good progress is being made on this and the system is now almost ready for implementation in February 2012. Once the final system is delivered it will be possible to draw up the detailed policies and procedures.	By 30/11/10 Revised Target: 31/10/12

IT Governance and Strategy: October 2010

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
2.	**Job Descriptions require review** Management should ensure that the minor changes that certain job descriptions require are implemented as soon as possible.	L	Head of ICT and Collector of Tolls	Still outstanding. A more significant change to job roles is required as a result of the decision to make one post redundant on 30 April 2011.	By 31/3/11 Revised Target: 31/3/12

Corporate Governance and Risk Management: May 2011

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
1.	**Periodic Review of Risks** All risks identified on the Risk Register should be subject to quarterly review in line with the Authority's Risk Management Policy. In addition responsibility for each risk should be assigned to individuals rather rhan a group or committee.	M	Director of Change Management and Resources	Implemented. The Risk Management Strategy has been updated to provide for six monthly, rather than quarterly reviews, as agreed by this Committee in July 29011, and all risks are now assigned to individual officers.	By 31/7/11
2.	**Risk Management Training** Risk management training should be provided on an annual basis, and/or when there is a substantial change to the risk management process.	M	Director of Change Management and Resources	Implemented. A Risk Management Workshop was held for members and relevant officers on 18 October 2011.	By 31/12/11

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	Agreed. A review of all policies and working practices is underway, and will be recorded.	31 March 2012
2.	**Maximisation of Planning Fee Income** Additional control should be introduced to provide assurance that all planning application fee income due is received in full. This could be achieved through: • Recording of receipt numbers in the planning system and independent verification of the income receipted in the financial management system upon sign off decision notices; and/or • Independent reconciliation of expected planning income due to actual receipts in the financial management system on a periodic basis.	M	Head of Development Management	Implemented. A system has been introduced to ensure that all payments are recorded and reconciled against the planning applications received.	31 October 2011

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
1.	**<u>Access Controls</u>** **Password Controls** Management should work with the developer of the Tolls Management System to strengthen password controls to current good practice standards including: • implementing a minimum of seven characters; • enabled and enforced password complexity; • regular change periods of 30 - 90 days; and • lockout following three unsuccessful access attempts. Ideally, the enhancements should include the ability to report bad password attempts to system administrators within the audit logs.	H	Head of ICT and Collector of Tolls	Implemented. The authentication scheme of the package has been changed from that set by the developer and now uses LDAP to validate users. Passwords therefore are no longer maintained within the system. For a user to gain access to the tolls system their active directory login name must exist in the users table and be linked to a valid security profile. This change has been tested and proven with three incorrect logons resulting in the users account being locked, requiring a reset by a domain administrator.	Not applicable
2.	**Password Encryption** Management should ensure that passwords cannot be viewed in clear text at any time.	M	Head of ICT and Collector of Tolls	Implemented. Passwords are no longer stored within the system.	Not applicable

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
	Data Input				
3.	**Obfuscation of Credit Card Data** Management should review the processes for redacting credit card data on relevant forms as the data is still visible.	M	Head of ICT and Collector of Tolls	Implemented**.** With immediate effect an adhesive label is being placed over the credit card data in addition to obscuring the information with black marker pen. Testing of this method shows it to be effective as no card data is visible on the scanned forms. To permanently eradicate this risk a new application form will be designed whereby the credit card data capture area can be removed from the form and destroyed prior to scanning.	31 January 2012
4.	**Stress Testing of Online Payments** Management should look at implementing a programme of stress tests against the online payments process, or assurance from the supplier that the implementation will function within acceptable tolerances under expected current and future peak loads.	M	Head of ICT and Collector of Tolls	Volunteers are being sought to undertake stress testing of the new system.	31 January 2012

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
5.	**<u>Backups</u>** **Integrity/Housekeeping Database Jobs** Management should explore the Oracle database management and housekeeping functionality to better understand and implement database housekeeping jobs. These should be run on a periodic basis as part of a wider database management routine.	M	Head of ICT and Collector of Tolls	Current integrity tasks will be confirmed, monitored and extended as required.	31 December 2011
6.	**Offsite Tape Storage** Management should review the process that takes backup tapes home overnight.	M	Head of ICT and Collector of Tolls	This was reviewed by the Authority's Corporate IT Group at its meeting on 27 January 2012. The Group agreed that in future backup tapes should be kept on a weekly basis, initially at the Field Base and then at the Dockyard when suitable arrangements have been put in place.	29 February 2012
7.	**Business Continuity and Disaster Recovery** Management should work with other departments to refresh the existing Corporate Business Continuity and Disaster Recovery Plans in line with changed Authority requirements. Both plans should undergo regular, formal testing.	M	Head of ICT and Collector of Tolls	The Corporate Business Continuity and Disaster Recovery Plans will be updated to ensure that they are in line with the Authority's current requirements.	31 July 2012

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
8.	**<u>Support System and Change Controls</u>** **Formal Support Agreement** Management must ensure that the current support arrangements are formalised and signed off as soon as possible, and no later than the go live date.	M	Head of ICT and Collector of Tolls	This is being pursued with the supplier, who has been requested to provide a copy of the Service Level Agreement as agreed in 2007.	31 December 2011
9	**Change Controls** Management should ensure that adequate change control processes are put in place to manage changes within the Tolls Management System once it has gone live. These processes can mimic the existing SharePoint processes that the implementation project has put in place and should include back out plans should any implemented change fail.	M	Head of ICT and Collector of Tolls	A new Change Management Log will be created to record changes requested after the system has gone live, with the previous change log being archived.	31 January 2012