

Committee(s):	Date(s):
Audit & Risk Management Committee	25 th June 2013
Subject: Internal Audit Recommendations Follow-up	Public
Report of: Chamberlain	For Information

Summary

This report provides an update on the implementation of audit recommendations by management since the last update, provided to the Audit & Risk Management Committee on the 5th March 2013.

At the end of May 2013, there are no outstanding red priority actions from reviews previously concluded and reported to this Committee.

Cumulative performance in the implementation of audit recommendations over the last 24 months, has been monitored with 73% of audit recommendations confirmed as implemented, when formal audit follow-ups were undertaken. Where red and amber priority recommendations were still to be implemented at the time of audit follow-up, further updates have been sought from management to confirm the implementation of red and amber priority recommendations.

Management status updates on all agreed red and amber actions is provided in **Appendix 1**.

There has been a delay in the implementation of three amber priority recommendations from the iTrent application review, which had been previously reported to this Committee. Action is now in progress to complete one of these recommendations, which concerned configuration hardening for web servers and will be completed by the end of July 2013. Two further recommendations have now been closed, following further review by internal audit and assessment of the risk as minimal. The original management response from IS Division was that implementation of these recommendations may not be practical, and would require further investigation. This has proved to be the case. Investigation of compliance with Data Protection Act and Public Secure Network (PSN) requirements was however undertaken as originally agreed and compliance confirmed in relation to existing arrangements.

Analysis of the implementation of red and amber priority recommendations, requested at the last Committee, shows that whilst 39% of recommendations are implemented by the originally agreed date, 61% of amber priority recommendations are implemented after the originally agreed date, with 35% implemented more than 6 months afterwards. This is clearly an area for improvement. Further analysis will be undertaken to identify those departments where the more significant delays in implementation are occurring. Targeted follow-up with Chief Officers will be undertaken to ensure originally agreed timescales for the implementation of recommendations are kept to wherever possible.

In addition to the 15 amber open actions, there are 240 open green priority actions as of May 2013.

Members are asked to:

- Note the recommendations follow-up report
- Note that a clear improvement is required in ensuring originally agreed timescales for the implementation of recommendations are achieved.

Main Report

Formal Audit Follow-ups

1. No formal audit review follow ups have been conducted since the 5th March 2013 update to the Committee. Internal audit work has been targeted on the completion of the 2012/13 audit plan and, in many cases, evidence of recommendation implementation is being provided by Departments, as actions are being completed, which is often negating the need to undertake formal follow-up reviews.
2. Cumulative performance in the implementation of audit recommendations has been monitored over the last 24 months and reported to the Audit and Risk Management Committee. As at May 2013, cumulative performance in the implementation of audit recommendations when formal audit follow-ups were undertaken, over the last 24 months, is as follows:-

Implementation at time of audit follow-up	Red	Amber	Green	Total
Recommendations Agreed	6	97	327	430
Recommendations Implemented	5	65	245	315
% implemented	83%	67%	75%	73%

3. Where red and amber priority recommendations were still to be implemented at the time of formal audit follow-up, further updates have been sought from management to confirm the implementation of red and amber priority recommendations. The one red priority recommendation that was not implemented at formal follow up stage, reported to the March 2012 Committee, was implemented subsequently. At the end of May 2013, there are no outstanding red priority actions from reviews previously concluded and reported to this Committee.

Red and Amber Priority Recommendations Status

4. In addition to this formal audit follow-up process, internal audit obtains status updates from recommendation owners on a quarterly basis for any open red or amber priority recommendations. The outcome from these status checks are reported in Appendix 2 and summarised in the following table. The table shows that there are no open red priority actions and that there are 15 amber priority actions open from internal audit work reported previously to Committee. This table only shows open amber actions and does not include amber actions agreed and subsequently implemented. An analysis and commentary on the extent to which actions have been implemented according to their originally agreed timescales is provided later in the report at paragraph 9.

Audit Actions Status based on Management reports		Progress to agreed timescales			Implementation due in future		
	Open Actions	Progressing according to original agreed timescales	Action slipped, new target dates agreed	Revised Date to be agreed	next 3 months	Next 3 to 6 months	More than 6 months
Red actions	-	-	-	-	-	-	-
Amber actions	15	3	12	-	8	4	3*
Total	15	3	12	-	8	4	3

* Details of the three amber priority recommendations with future target dates of greater than 6 months are as follows. (Additional information is in Appendix 1):-

- Two amber recommendations are linked to the requirements of the Hutton report on public sector pension reform and the resulting legislation (Public Service Pensions Act 2013) which received Royal Assent on the 25th April 2013. Due for implementation by April 2014 as originally agreed.
- The other amber priority recommendation is outstanding in respect of addressing the poor quality of management information available from the car park barrier system at Smithfield. The replacement equipment will not now be in place until November 2014 when the new off street car park contract is let.

iTrent application (Payroll & HR database)

5. There were three amber priority recommendations reported as outstanding at the last Committee meeting relating to the iTrent application (Payroll & HR database system). One recommendation concerning configuration hardening for web servers had not been progressed due to lack of resources. Action is now in

progress, with new software installed and configuration hardening for web servers in progress, which will be completed by the middle of July 2013.

6. Two further recommendations have been reviewed between internal audit and IS Division and have now been closed. The first concerned writing audit trails to a secure server. Most importantly, audit logs are written to a securely configured server and this ensures a proper audit/management trail. However, applying a division of duty between administrators, automated log review and alerts, while being investigated, still have not been implemented. The original management response from IS Division was that these issues may not be practical and this has proved to be the case. The policy has been reviewed on a cost/risk basis and judged not to be realistic. This position is accepted by internal audit as the risk is minimal and will be addressed again under the IS outsourcing arrangements.
7. The second recommendation concerns the automated reconciliation of security logs and the investigation of compliance with Data Protection Act (DPA) Principle 7 and Public Secure Network (PSN) requirements (CoCo PRO.2 and PRO.3). The concerns arising from this recommendation have now been investigated. The IS policy for this area (i.e. Protective monitoring – logs') with security logs now being kept in a central location for six months achieves compliance with the DPA and PSN requirements. Not all data is subject to this policy, but importantly it is applied to critical data (e.g. domain controllers, firewalls, and file cluster). This position is accepted by internal audit as the risk is minimal and will be reviewed again under the IS out-sourcing arrangements.
8. In any organisation the security policy has to be considered on a cost/risk basis while being in line with the legislation, guidelines and standards of the industry. The City of London Corporation is no exception to this and the IS division's security policy considers cost/risk and resources and prioritises accordingly.

Implementation of Recommendations according to agreed timescales

9. At the March 2013 Committee meeting, members requested an analysis of the extent to which priority audit recommendations are implemented according to originally agreed timescales or revised target dates were agreed. The following table provides an analysis from data held in the MK Audit Automation system relating to the implementation dates for now closed Amber and Red priority recommendations over the last 15 months.

Red and Amber Priority Recs – Implementation according to original target date

Implemented 1 month or more ahead of time	8%
Implemented in due month	31%
Less than 1 month after	4%
Less than 3 months after	18%
Less than 6 months after	4%
More than 6 months after	35%

10. The analysis shows that whilst 39% of recommendations are implemented by the originally agreed date, 61% of amber priority recommendations are implemented after the originally agreed date, with 35% implemented more than 6 months afterwards. This is clearly an area for improvement. Further analysis will be undertaken to identify those departments where the more significant delays in implementation are occurring. Targeted follow-up with Chief Officers will be undertaken to ensure that the importance of keeping to the originally agreed timescales for the implementation of recommendations is understood.
11. The vast majority of recommendations owners are keeping internal audit updated on any delays in implementing recommendations prior to any agreed target dates being passed, with revised implementation dates agreed with internal audit. All live red and amber recommendations are being tracked through the MK audit automation software, which is enabling a pro-active approach to audit recommendation follow up and reporting. The use of this system is now enabling a deeper analysis of the progress in implementing recommendations to be undertaken.
12. At previous Committee meetings, the Chairman stressed that unilateral decisions by Departments to permit slippage in the implementation of audit recommendations were not acceptable. Any delays in implementing to an agreed timetable were only acceptable if and when agreed, at a minimum, with Internal Audit. This message has been and will continue to be reinforced with Departments. Most recently, this message was communicated and discussed with Chief Officers at the April 2013 Chief Officer Group meeting where they undertook to remind recommendation owners of this requirement.

Conclusion

13. There is a very high level of acceptance of internal audit recommendations, although implementation according to the originally agreed timescales is often not achieved and requires improvement. Internal audit work focused on obtaining status update information from management of open recommendations, in addition to formal audit follow-up reviews is ensuring appropriate management attention is given to completing agreed audit actions.

Appendices

- **Appendix 1 – Red and Amber actions status update**
- **Appendix 2 – Audit Follow-up process and recommendation priority definitions**

Background Papers:

2013/14 Internal Audit Plan

Paul Nagle

Head of Audit & Risk Management

T: 020 7332 1277

E: Paul.Nagle@cityoflondon.gov.uk