Committee:	Date:
Audit and Risk Management Committee	24 July 2017
Subject: Internal Audit Update Report	**Public**
Report of: The Head of Internal Audit and Risk Management **Report author** Jeremy Mullins – Audit Manager	**For Information**

Summary

This report provides an update on internal audit activity since the last Committee report to the February 2017 meeting.

The outcomes of the internal audit work finalised since the last Committee are summarised in Appendix 1. Since the last report to the Committee 25 audits have been finalised. Two audits resulted in Red Assurance (Chamberlain's IT Cyber Security – SekChek and IT Asset Management); ten audits resulted in Amber assurance opinions; and 13 in Green opinions. Both Amber and Green opinions represent adequate control environments.

As at 23 June 2017, 95% of the 2016-17 internal audit plan had been completed to draft report stage, together with three audits at work in progress stage, the profiled target was 95% to be completed by 31 March 2017.

Recommendation

- That this report is noted.

Main Report

Background

1. This report sets out internal audit activity since the last report to Committee and the opinion of the Head of Audit and Risk Management in relation to the adequacy and effectiveness of the control environment.

Current position

2. The outcomes of the internal audit work finalised since the last Committee have been reported to Members through our Members Briefings. A summary of the outcome of our audit work can be seen in **Appendix 1**. Two audits resulted in Red Assurance (Chamberlain's IT Cyber Security – SekChek and IT Asset Management); ten audits resulted in Amber assurance opinions; and 13 in Green opinions. Both Amber and Green opinions represent adequate control environments.

3. Work on the internal audit plan 2017-18 is progressing and a summary of the current position can be seen in **Appendix 2.** Seven reviews have been completed to Draft Report stage and the fieldwork for seven further reviews has been progressed to fieldwork stage.

IT Cyber Security – SekChek (Red Assurance)

4. Effective use of security updates and hotfix patches helps ensure that Domain Controllers are not vulnerable to attacks known security issues and weaknesses. Review of the system configuration information identified that while 178 security updates were applied when the Domain Controller was installed in 2015; no security updates were applied in 2016 or 2017. There is an increased risk that the network will remain open to known high risk vulnerabilities unless automated patch management settings are enforced and appropriate key performance indicators (KPIs) are established and applied to monitor the effective delivery of security patch management activities.

5. It was recommended that management should ensure that the Network Domain Controllers (DCs) are made subject to an effective security patch management solution that is monitored for achievement via appropriate Key Performance Indicators.

6. In response, IT Management stated that: There will be a significant reduction in the number of DCs within the environment as the transition to a managed desktop environment progresses this year. A Security and Patch Management policy is currently being developed as part of the IT Transformation programme. This will set the policy intention, and the managed service provider will retain responsibility for adherence to this policy.

7. An urgent review would be undertaken to ensure DCs have appropriate security patches applied. In addition, Agilisys to provide IT Management with a regular patching report to demonstrate compliance with contractual obligations and security compliance.

IT Asset Management (Red Assurance)

8. Audit testing identified a stockpile of non-marked hard-drives being kept in the decommissioning room. No satisfactory information was provided on their provenance and purpose or on the reason for them to be kept there. Where hard-drives are being removed from their corresponding desktops/laptops, there is a risk that sensitive information contained within them is not appropriately erased.

9. It was recommended that: Hard drives should be securely disposed of along with the desktops/laptops to which they pertain.

10. In response, IT Management stated that: There is a disposal process that is generally adhered to. Agilsys will ensure that the Field Engineer team are reminded of the process to follow and regular internal checks will be implemented. The hard disks will be audited by SC cleared personnel and then decommissioned, re-used or securely stored accordingly.

11. There is not a Disposal Policy for IT Assets in place. Where the disposal activity is not guided, there is a risk that inappropriate decisions are taken which could result in assets not being disposed of as expected and or not being disposed of in accordance with the requirements to which the City is subjected.

12. It was recommended that: A Disposal Policy for IT Assets should be introduced.

13. In response, IT Management stated: There is a Disposal Policy in place; however it will be reviewed to ensure it meets requirements.

Internal Audit Section Performance and Delivery 2016-17

14. Performance levels against KPIs continue to be generally good, and the team has achieved the annual target of audits completed to draft report stage for 2016-17. Completion of the 2016/17 audit plan to at least draft report stage was 95% in line with the profiled target by end March 2017, with three audits (5%) at work in progress stage.

15. Details of performance levels against targets for 2016-17 are set out below:

Performance Measures	Target	Actual
1 Completion of audit plan	95% of planned audits completed to draft report stage by end of plan review period (31 March 2017)	95%
2 Timely production of draft report	Average time taken to issue draft reports within 28 days of end of fieldwork i.e. exit meeting date.	20 days
3 Timely response to draft report	Average time taken to obtain a full management response within 28 days of the draft report being issued.	25 days
4 Timely issue of final report	Average time taken to finalise the review within 7 working days on full response from management	6 days
5 Customer satisfaction	Through key question on post audit surveys – target 90%	<5 responses received
6 Percentage (%) of audit section staff with relevant professional qualification	Target 75%	78%

I

Internal Audit Performance and Delivery 2017-18

16. Performance levels against KPIs for 2017-18 indicate that by the end of Quarter 1 9% of the plan has been completed to draft report stage. A further 9% of the plan has been progressed to fieldwork stage. The audit plan completion profile for Quarter 1 was 14% and there has been some delay in starting audit work due to agreeing audit timings with Chief Officers. It is anticipated that ground will be made up during Quarter 2 when a number of audits currently at fieldwork stage plus those currently at planning stage have been progressed.

Conclusion

17**.** Internal Audit's opinion of the City's overall internal control environment is that it remains adequate and effective although some areas of the financial and operational framework do require strengthening by management as identified in the Amber reports highlighted to the Committee in Members Briefings.

Appendices

Appendix 1 Internal Audit Plan Schedule of Projects 2016-17
Appendix 2 Internal Audit Plan Schedule of Projects 2017-18

Pat Stothard, Head of Audit and Risk Management
T: 020 7332 1299 E:Pat.Stothard@cityoflondon.gov.uk
Jeremy Mullins, Audit Manager
T: 020 7332 1279 E:Jeremy.mullins@cityoflondon.gov.uk