

Committee(s)	Dated:
Performance and Resources Sub (Police) Committee	26 th September 2017
Subject: Internal Audit Update Report	Public
Report of: The Chamberlain	For Information
Report author: Pat Stothard, Head of Audit and Risk Management Jeremy Mullins, Audit Manager	

Summary

The purpose of this report is to provide the Committee with an update on the work of Internal Audit that has been undertaken for the City of London Police (CoLP) since the last report in May 2017.

Work is completed to a minimum of draft report stage on the 2016-17 planned internal audit work and it is anticipated that all audits will be completed by 29th September 2017. There were seven full assurance audits included in the original plan: five audits (CoLP Community Consultation; CoLP Policies and Procedures; the Economic Crime Academy; SKYNet Grants Audit Verification; and Governance Framework and Performance Measures) have all been completed. The remaining two planned audits: Police Budget Monitoring, and Income Streams and Income Generation, have been completed to draft report stage and will be finalised by the end of September 2017. The completion of the two remaining audits: Police Budget Monitoring; and Income Streams and Income Collection have been delayed. This is due limited Police staff availability to meet with the audit staff within anticipated timescales.

An unplanned audit requested by the Commissioner to determine how two former civilian staff members were paid after they had resigned has been completed to draft report stage and will also be finalised by the end of September 2017.

As previously agreed with your Committee, where findings and recommendations from corporate-wide audit reviews impact on the City Police details will be reported at the next committee meeting. There are ten planned corporate audits for 2017-18, and five of these have been completed to draft report stage to date.

Work is progressing on the Internal Audit Plan for 2017-18. There were eight full assurance audits planned for the financial year 2017-18. Two 2017-18 audits have been completed to draft report stage: Police Project Management and Police Seized goods. Fieldwork is progressing on two further audits: Police Bank Accounts (Defendants Funds) and Demand and Events Policing. It has been necessary to defer two of these audits: IT Technology Refresh Project and Action Fraud. A further audit of IT Network Security has been deleted. Discussions are on-going with Management to identify other audit work that can be undertaken in order to utilise the existing audit resources.

Recommendation

Members are asked to:

- Note the report.

Main Report

Internal Audit Plan 2016-17

1. There were seven full assurance audits included in the original plan: five audits (CoLP Community Consultation; CoLP Policies and Procedures; the Economic Crime Academy; SKYNet Grants Audit Verification; and Governance Framework and Performance Measures) have all been completed. The remaining two planned audits: Police Budget Monitoring, and Income Streams and Income Generation, have been completed to draft report stage and will be finalised by the end of September 2017. An unplanned audit requested by the Commissioner to determine how two former civilian staff members were paid after they had resigned has been completed to draft report stage and will also be finalised by the end of September 2017. Details of these audits and progress against the 2016-17 Internal Audit Plan are contained in Appendix 1.
2. The completion of the two remaining audits: Police Budget Monitoring; and Income Streams and Income Collection have been delayed. This is due limited Police staff availability to meet with the audit staff within anticipated timescales.

Internal Audit Planned Work 2017-18

3. Work is progressing on the Internal Audit Plan for 2017-18. There were eight full assurance audits planned for the financial year 2017-18. Two 2017-18 audits have been completed to draft report stage: Police Project Management and Police Seized goods. Fieldwork is progressing on two further audits: Police Bank Accounts (Defendants Funds) and Demand and Events Policing. Details of all these audits and progress against the 2017-18 Internal Audit Plan are contained in Appendix 2.
4. It has been necessary to defer three of these audits: IT Network Security; IT Technology Refresh Project; and Action Fraud.

Deferred and Deleted Audits

5. IT Network Security – Discussion with the Director of IT has confirmed that the intended scope of this audit has been primarily covered in the IT Network Infrastructure (SekChek) audit completed in May 2017. The outcome of this audit is provided below and the recommendations are currently being addressed by the City of London Corporation. A summary of the outcome of this corporate review has been included below (paragraph 8) for your information.
6. IT Technology Refresh Project – discussion with the Director of IT has established that due to the implementation timetable of this project, it will be more appropriate for this audit to be undertaken as part of the 2018-19 Audit Plan.

7. Action Fraud – the fraud reporting and data capture system is currently being delivered via an extended existing contract. The City of London Police and Corporate Procurement are currently working with IBM, who have been contracted to provide an improved fit for purpose Action Fraud service. Due to the interim arrangements in place and ongoing negotiations on service delivery, it is deemed too early to undertake an audit in this area and the audit has, therefore, been deferred to 2018-19.
8. Discussions are on-going with the City of London Police to identify other audit work that can be undertaken in order to utilise the existing audit resources.

City of London IT Network Infrastructure (Corporate Review 2016-17)

9. The key findings are as follows:

- Overall, the use of security controls is in line with those applied to other Active Directory domains used in the Government sector.
- System Wide Domain Security Settings – An effective password policy has been established and applied. However, two amber recommendations were raised in this area to improve the effectiveness of the intruder alert lockout policy settings and to rename the default system administration account.
- Audit Policy Settings – As little use is currently being made of the audit policy settings and alerts two amber recommendations were raised to help address this.
- Event Log Settings - System event log settings currently overwrite event records as needed, which means that log records are not archived. An amber recommendation was therefore raised to improve accountability by addressing the risk that potentially important entries will be overwritten and lost.
- Security Options – No significant risk issues were identified in the examination of the security option settings although one green recommendation was raised to “warn but allow” the installation of uncertified device drivers rather than to simply allow them to “silently succeed”.
- User Accounts – 8,010 accounts exist of which 43.6% are disabled Two green recommendations were raised in this area to review the inconsistencies found in the use of home directories, logon scripts and profiles to resolve the single end user account for which no password is required.
- Rights and Privileges – While rights and privileges are well defined and applied one amber recommendation was raised in this area to support the current management initiative to review administrator rights and privileges.
- Trusts and Remote Access Services – No trust relationships were found to exist with any other domains and while no Windows Remote Access Service (RAS) servers were identified, excluding disabled accounts, 428 (5.3%) of users have permission to dial-in via RAS including 7 administrator accounts. An amber recommendation has been raised to address this as RAS passwords are transmitted in clear text.
- Services and Drivers – No issues were identified following the detailed examination of the 383 services and drivers installed in the domain.

- Updates and Patches – The latest Windows service pack was found installed on the Network Windows AD server and 177 Security Patch updates were applied to the DC server when it was first installed in 2015. However, no security updates have been applied since then and a red recommendation was raised to address this.
- Discretionary Access Control Lists (DACLS) - No issues were identified following the examination of the 96,110 DACLS defined on the domain.
- Logical Drivers and Network Shares – No issues were identified as the domain server access is protected by the use of secure (NTFS) drives.
- Backup and Restore Arrangements - No assurance can currently be provided in this area as no evidence was provided in response to the audit request for information at the time of the audit.

Conclusions

10. The 2016-17 Internal Audit plan is scheduled for completion to draft report stage for remaining audits by 29th September 2017.
11. Work is progressing on the 2017-18 Internal Audit plan and two audits have been completed to draft report stage. Fieldwork is progressing on two further audits.
12. It has been necessary to delete one audit and defer two further audits from the 2017-18 Audit Plan. Discussions are on-going with the City Police to identify audit areas to utilise the resources available.

Appendices

- Appendix 1 - Schedule of Internal Audit Planned Work 2016-17
- Appendix 2 - Schedule of Internal Audit Planned Work 2017-18

Pat Stothard, Head of Audit and Risk Management
T: 07796 315078 E: pat.stothard@cityoflondon.gov.uk

Jeremy Mullins, Audit Manager
T: 020 7332 1279 E: jeremy.mullins@cityoflondon.gov.uk