Internal Audit

Police and Crime Commissioners for Norfolk and Suffolk and Chief Constables of Norfolk and Suffolk Constabularies

Audit Progress Report – Suffolk

2017/18

December 2017

FINAL

INTRODUCTION

1. This summary report provides an update on the progress of our work at the Police and Crime Commissioners for Norfolk and Suffolk and Chief Constables of Norfolk and Suffolk Constabularies as at 22nd November 2017. The report is based on internal audit work carried out by TIAA and management representations that have been received during the period since our last progress report.

PROGRESS AGAINST THE 2017/18 ANNUAL PLANS

2. Our progress against the Annual Plans for 2017-18 is set out in Appendix A. The results of these reviews are summarised at Appendix B.

AUDITS COMPLETED SINCE THE LAST REPORT TO COMMITTEE

5. The table below sets out details of audits finalised since the previous meeting of the Audit Committee.

		Key Dates			Number of Recommendations			
Review	**Evaluation**	**Draft issued**	**Responses Received**	**Final issued**	**1**	**2**	**3**	**OE**
ICT Mobile Devices	**Reasonable**	**23/08/2017**	**19/10/2017**	**23/10/2017**	**0**	**4**	**1**	**1**
IM Data Quality	**Limited**	**27/10/2017**	**10/11/2017**	**21/11/2017**	**0**	**3**	**1**	**2**
Norfolk & Suffolk joint PFI	**Substantial**	**03/10/2017**	**06/10/2017**	**10/10/2017**	**0**	**0**	**2**	**0**

Copies of the finalised reports are available to Audit Committee Members on request. The details for Norfolk only reports will not be included in the Suffolk progress report.

CHANGES TO THE ANNUAL PLAN 2017/18

6. There has been one change made to the annual plan since the last meeting:

- Two additional days added to temporary recruitment to allow further analysis of temporary recruitment with previous employees.

FRAUDS/IRREGULARITIES

7. An audit has identified a potential irregularity which is currently under investigation.

LIAISON

8. Liaison is undertaken with the following:

- Liaison with the Chief Finance Officers: Regular progress meetings are held with the Chief Finance Officers.
- Liaison with PSD: Regular meetings are held with PSD during the year.
- Liaison with Risk Management: Increased liaison has commenced, to directly link internal audit with risk management.
- Liaison with external audit: We have liaised with EY during the year and kept them informed of our work and will make available to them all final audit reports.

PROGRESS ACTIONING PRIORITY 1 (URGENT and NOT APPROVED RECOMMENDATIONS)

9. We have made no urgent recommendations (i.e. fundamental control issues) since the previous Progress Report:

8. We have made no recommendations which have not been approved by management since the previous Progress Report.

RESPONSIBILITY/DISCLAIMER

10. This report has been prepared solely for management's use and must not be recited or referred to in whole or in part to third parties without our prior written consent. The matters raised in this report not necessarily a comprehensive statement of all the weaknesses that exist or all the improvements that might be made. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any other purpose. TIAA neither owes nor accepts any duty of care to any other party who may receive this report and specifically disclaims any liability for loss, damage or expense of whatsoever nature, which is caused by their reliance on our report.

.

Appendix A

Progress against the Annual Plan for 2017/18

System	Planned Quarter	Planned Days	Actual Days to date	Current Status	Audit Committee Reporting	Assurance	Comments
2017/18 Plan							
NSC1802 ICT Mobile Devices	1	10	10	Final Report	December 2017	Reasonable	
NSC1803 IM Audit Team Assessment	1	8	8	Final Report	September 2017	Substantial	
NSC1805 ill Health Retirement	1	8	8	Draft Report	March 2018		
NSC1806 Transport – Use of Vehicles	1	10	10	Final Report	September 2017	Reasonable	
NSC1808 Estates Contract Management	1	10	10	Final Report	September 2017	Substantial	
NSC1809 Purchase Ordering	1	10	10	Final Report	September 2017	Reasonable	
NSC1810 Temporary Recruitment	1	7	9	Draft Report	March 2018		
NSC1811 CSO Compliance and STA	1	17	17	Final Report	September 2017	Reasonable	
NSC1812 Business Interests	1	8	8	Draft Report	March 2018		
NSC1816 ICT Governance	2	12	9	In progress	March 2018		
NSC1817 IM Data Quality (Athena)	2	12	12	Final Report	December 2017	Limited	
NSC1818 IM MOPI Project	2	10	10	Draft Report	March 2018		
NSC1820 Joint PFI – Police Investigation Centres	2	14	14	Final Report	December 2017	Substantial	
NSC1821 Norfolk PFI – Norfolk only	2	14	14	Final Report	December 2017	Substantial	Norfolk only report
NSC1823 Overtime, Expenses, Add Payments	2	14	14	In progress	March 2018		

System	Planned Quarter	Planned Days	Actual Days to date	Current Status	Audit Committee Reporting	Assurance	Comments
NSC1801 Governance & Ethics	3	12	1	Scheduled	December 2017		
NSC1815 ICT Data Assurance	3	12	1	In progress	March 2018		
NSC1819 HR Absence Management	3	12	8	In progress	March 2018		
NSC1824 Purchase Cards	3	10	10	Draft Report	March 2018		
NSC1825 Corporate Policies	3	10	1	Scheduled	March 2018		
NSC1829 Payroll incl ERP	3	10	8	Scheduled	March 2018		
NSC2830 Accounts Payable	3	10	10	Draft Report	March 2018		
NSC1804 HR Learning and Development	4	12	1	Scheduled	March 2018		Moved from Q1 to Q3, due to department transformation
NSC1807 Estates 3i Property Database	4	4					May not go ahead
NSC1814 Risk Management – Mitigating Controls	4	11	1	Scheduled	March 2018		Moved from Q2 to Q3 - Workshop to be delivered
NSC1822 Safeguarding and Investigations	4	10	1	Scheduled	March 2018		
NSC1826 ERP / Athena	4	12		Scheduled	March 2018		
NSC1827 Commissioners Grants	4	18		Scheduled	March 2018		Separate reports for Norfolk and Suffolk
NSC1813 Recovered Property	4	10	1	Scheduled	June 2018		
NSC1828 Key Financials	4	30	2	Scheduled	March 2018		
Follow Up Work		12	4	Ongoing			Year-end reporting June / in-year reporting December
Contingency b/fwd	1-4	(62)					
Contingency c/fwd	1-4	11					
Audit Management	1-4	20	15	Ongoing			
Total Days	-	330	227				

KEY:

	=	To be commenced
	=	Site work commenced
	=	Draft report issued
	=	Final report issued

Appendix B

Summaries of Finalised Audit Reports issued since the last report

Audit Report: ICT Mobile Devices (NSC1802)

Report: 23rd October 2017

SCOPE

The scope of the review focussed on the implementation of the devices across both Constabularies, with a further review in 2018/19 to assess how this is operating.

MATERIALITY

Robust management of all relevant mobile devices in scope is critical to ensuring the integrity and security of the data that is processed on the devices.

KEY FINDINGS

- A process for monitoring mobile devices is not in place, to ensure they remain compliant with relevant Security Policies.
- Updates to the Android Operating System installed on the mobile devices are not managed via a formal change control process.
- The process to request a new app to be added to the app whitelist requires enhancement to include a more detailed business case.
- Mobile device procurement and provisioning processes were found to be adequate.

OVERALL ASSURANCE ASSESSMENT

ACTION POINTS

Urgent	Important	Routine	Operational
0	4	1	1

Recommendations – Urgent (Priority 1), Important (Priority 2) and Not Approved

Report Ref	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
2	Operational	Android Operating System updates are deployed on a periodic basis to all mobile devices. However, the updates are not subject to formal change control processes prior to their deployment.	Management to implement formal change control processes to manage the deployment of relevant Android Operating System updates. A Standard Change may be the most appropriate way forward.	2	*Customer Contact Team to raise change forms in line with the existing ICT change process.*	*31/10/17*	*Joint ICT Change & Configuration Manager*

Report Ref	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
3	Operational	BES has the ability to keep track of all devices in terms of their compliance with policy and how often every device connects. However, there is no process in place to monitor device compliance on an ongoing basis and to resolve issues where devices are found to be non-compliant. The audit noted that there were approximately 21 devices out of approximately 500 devices not in compliance with relevant security policies and which require follow up. Whilst it is recognised that the proportion of non-compliance devices is currently low, the number of devices to be managed is expected to increase to around 3000, meaning that the number of non-compliance devices at any one time could increase. Monitoring of device compliance with security policies is key to ensuring that device security and the security of the data they process is managed adequately and effectively.	Management to develop, agree and implement a process whereby all devices are periodically monitored for compliance with current security policies and to follow up and resolve all non-compliance found. The process also to be formally assigned a process owner, with agreed process roles and responsibilities also being documented.	2	*Process in place for Apps team to run a monthly compliance report, this is sent to the ICT SD. The ICT SD will contact all individuals on the list to ask if the device is required. If not required it will be sent back for the unit to be re-distributed, if the user requires the units, they will be asked to ensure it's logged on asap for the policy to be updated.*	*29/12/17*	*Joint ICT Change & Configuration Manager*

Report Ref	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
4	Operational	There is an existing range of Android apps that have been included in a whitelist of approved apps that can be installed on mobile devices issued to users. The Blackberry Enterprise Server (BES) Mobile Device Management (MDM) application has several groups set up that define which apps are available to users. Typically, this would be because of their business need to use the apps, although an element of the apps are configured for all users. Such apps might include news apps and apps already bundled with the Android Operating System on the devices. The audit noted that there is a documented process for requesting new apps to be added to the whitelist, although the content of the process is very high level. For example, there is no explicitly documented final approval (or otherwise), no indication of which Active Directory groups the app should be provisioned for, line manager approval of the request and internal ownership of the app's use.	The existing "Mobile App Request" process to be updated to include the following as a minimum - documented approval / sign off from the requestor's line management; A list of Active Directory groups that the app is to be provisioned for; testing results showing the app not conflicting with other apps in the whitelist, Information Security Office comments and recommendations; final sign off documenting the decision to deploy or not; Requestor's business case for making the request; next review date; the internal owner of the app - most likely the line manager of the original requestor or delegated authority - to be consulted during the subsequent review cycles, including where an approved app has been updated via a security update, or similar.	2	*ICT to discuss with ISO required modifications to the existing forms and process.*	*29/12/17*	*Joint ICT Infrastructure Manager*

Report Ref	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
5	Operational	The audit noted that there is no evidence to suggest that the apps already contained in the whitelist have been subjected to any request process - for example, the whitelist includes the "Sky Sports" app and a number of news apps including the BBC news and Sky News apps. Whilst there may be a legitimate need for these apps, the business need for these and all future apps needs to be formally documented and approved, together with formal ownership of all apps documented.	The updated "Mobile App Request" process to be applied to every existing app contained in the whitelist and all future apps that may be requested from time to time.	2	*ICT to set-up a periodic review of the list of existing applications, to be reviewed with ISO.*	*29/12/17*	*Joint ICT Infrastructure Manager*

Audit Report: Data Quality – Athena (NSC1817)

Report: 21st November 2017

SCOPE

The purpose of the review was to assess the adequacy and effectiveness of the internal controls in place within the Constabularies for managing data quality on Athena. The audit focused on the following key areas:

- to establish if duplicates on Athena are identified and addressed appropriately.
- to establish if there are appropriate controls to ensure the accuracy of data entered on Athena.
- to establish the adequacy of the escalation process to address issues in relation to the inaccuracy of data entered on Athena.

MATERIALITY

Athena is able to display a maximum of 500 possible duplicates. The number of possible duplicates is greater than 500, and thus it is not possible to establish how many potential duplicates there are on Athena.

KEY FINDINGS

- There are a high number of duplicates on Athena which require investigation, which impacts on the overall assurance rating for the audit. Some duplicates and data quality issues are due to system design, which is not within the Constabularies control.
- Two dashboards are maintained for the same data, dashboard two reports cumulative potential errors, dashboard one reports daily potential errors, which are not being cleared, then appear in dashboard two.
- Departments are not provided with regular reports for their area to enable them to investigate data quality issues on Athena.
- Procedural notes for staff on Athena have not been produced.

OVERALL ASSURANCE ASSESSMENT

ACTION POINTS

Urgent	Important	Routine	Operational
0	3	1	2

Recommendations – Urgent (Priority 1), Important (Priority 2) and Not Approved

Report Ref	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
2	Directed	Two dashboards are maintained, dashboard one and dashboard two. Dashboard two monitors the accumulated potential errors. Dashboard one is run daily and tracks the overall trend, but as the number of potential errors are so high it is not possible to investigate the errors daily. As such dashboard one and two both contain the same data.	A review of the two dashboards be undertaken and a decision made as to whether both dashboard reports continue to be run, and in their current format.	2	*The Dashboards were designed by Essex Police and agreed for use by all Athena Forces. Any changes require other Athena Force DQ Leads, the Information Management User Group (IMG) and to be ratified by the Athena Business Design Authority.* *Work is taking place by the (regional) Athena Data Quality Sub Group to review the reporting mechanisms.* *Norfolk/Suffolk DQ & Audit Officer requested the criteria for the dashboard be reviewed at the IMG DQ Sub group, as the findings are to large for business areas to tackle (e.g. 22,269 hits on one test for investigation). There is also contest as to whether the tests actually find errors or not. Norfolk/Suffolk have no local control over the dashboards and consider that unless resource is available to attack DQ risk areas on a daily / weekly basis then Dashboard 1 seems to be an unnecessary task. Dashboard 2 (run monthly) would give an overview of data trends.*	*1 April 2018*	*Information Compliance Manager*

Report Ref	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
3	Directed	Reports had been provided by the Auditing and Data Quality Officer to individual departments on their potential data errors, but these had not been produced regularly. Reports were produced in November 2016, but as the number of errors were so high there was limited use in the reports being produced as all departments are aware that they have high number of data errors. There is a need to review the process that is being followed so that departments can address potential errors on Athena.	Regular reports be provided to departments on potential data errors so that departments can target specific areas.	2	*The level of errors is still high due to a number of errors within the early stages of Athena. As time has passed, changes have been made to reduce the errors. The Data Quality team are not yet in a position to look further into the variance of issues outside the match& merge queues but the vision is to do so based on the improved reporting mechanisms from the AMO. The missing data tend to relate to areas such as intelligence where it is expected there will be a level of missing data due to the nature of the work. Revised reports are being developed by the AMO. Also an Athena DQ Comms strategy is being written by the Information Compliance Manager. A sound performance report relies on valuable data to present i.e. the Dashboards. At present the Dashboards do not produce data that can be taken to business areas.*	*1 April 2018*	*Information Compliance Manager / Records Manager*

Report Ref	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
4	Directed	Duplicates on Athena can be in relation to people, vehicles, locations and communication. Athena is capable of recording a maximum of 500 records for each category of duplicates, where there are more than 500 potential duplicates only the first 500 are displayed on Athena. At the time of audit the number of duplicates on Athena was increasing, and was above 500.	A resolution be sought on the outstanding and growing duplicate Athena records across each of the categories.	2	*The 500 limited is a technical limitation set by the AMO. A current change notice is being proposed to remove cases which have been reviewed but that cannot be merged, from the match & merge list. There is a cost element to this change which has to be agreed and prioritised by the BDA and AMO. A number of issues remain unresolved within Athena which has a direct impact of the level of duplicates in the system, in particular locations. Words of advice are provided to officers where appropriate. Updates to Athena have helped reduce some of the duplication though a number remain in the system due to the previous issues and need to be cleared. Further training is being rolled out to supervisors on the use of Athena which includes DQ input. The lists are above 500 due to staff overturn in the DQ team. The team is now fully resourced, though the level of DQ resource available is acknowledged. It has been identified that improved training on DQ at the front end of Athena is crucial to success.*	*1 April 2018*	*Head of Information Management / D/Supt Joint Justice Command – Athena Lead*

Audit Report: PFI Police Investigation Centres (NSC1820)

Report: 10th October 2017

SCOPE

The audit focused on the Norfolk and Suffolk Police Investigation Centres PFIs. The audit focused on the following areas across each PFI:

- Contract management
- Budget monitoring
- Recharges
- Performance monitoring

MATERIALITY

The value of the payments for the Police Investigation Centres since February 2017 is £6.5 million.

KEY FINDINGS

The effective contract management process has generated efficiencies for Norfolk and Suffolk Constabularies. Steps are being considered for generating further savings in relation to the Police Investigation Centres (PICs)

- The PICs budget is monitored.
- There is a process for processing of the PIC invoices.
- Recharges for the PICs are recharged accordingly at designated timescales.
- There are arrangements for monitoring the performance of the PFI contractor, including standard monthly performance reports received from the PFI contractor.
- The monitoring officer undertakes regular spot checks of the PICs, but does not have a formalised work plan to follow.
- Jobs reported to the help-desk are closed down by the help-desk, as such there is an incentive for the help-desk to close down jobs before completion to avoid financial penalty.

OVERALL ASSURANCE ASSESSMENT

ACTION POINTS

Urgent	Important	Routine	Operational
0	0	2	0