Police and Crime Commissioner for Lincolnshire and Lincolnshire Police

Internal Audit Progress Report

Joint Independent Audit Committee meeting: 15 April 2015

Introduction

The internal audit plan for 2014/15 was approved by the Joint Independent Audit Committee in March 2104. This report provides an update on progress against that plan and summarises the results of our work to date.

Following feedback from the last Joint Independent Audit Committee meeting, we have revised the format of the report. We hope this meets your needs, but would be happy take on board any further feedback on the format or content.

Summary of Progress against the Internal Audit Plan 2014/15

Assignment ***Reports considered today are shown in bold italics***	**Fee (as per audit plan)**	**Responsible Officer**	**Fieldwork**	**Status**	**Opinion**	**Actions Agreed (by priority)** **High**	**Medium**	**Low**
T-Police Implementation (1.14/15)	Carry forward from 2013/14 £3,975	Julie Flint	May 2014	FINAL (Sept 14 AC)	AMBER / RED	0	4	1
Governance - Decision making process & integrity (2.14/15)	£2,900	Julie Flint / Ginny Mason / John King	May 2014	FINAL (Sept 14 AC)	GREEN	0	0	2
Fleet Management (3.14/15)	£2,880	Gail Bradshaw	July 2014	FINAL (Nov 14 AC)	AMBER / RED	1	4	2
Service Expectations – POCA (4.14/15)	£3,275	ACC Roach	July 2014	FINAL (Sept 14 AC)	RED	1	2	0
G4S Niche Service Provision (5.14/15)	£5,933 (Additional Review)	Commissioned by Julie Flint	October 2014	FINAL (Nov 14 AC)	SUBSTANTIAL ASSURANCE	0	0	0
Service Expectations – Firearms Asset Management (6.14/15)	***£2,150***	***ACC Roach***	***October 2014***	***FINAL (APR 15 AC)***	***AMBER / GREEN***	***1***	***0***	***3***
Financial Management including Budget Management and Procurement (7.14/15)	***£3,600***	***Julie Flint / Tony Tomlinson / Gail Bradshaw***	***Sept 2014***	***FINAL (APR 15 AC)***	***AMBER / GREEN***	***0***	***2***	***3***
Data Returns – HMIC VFM Profiles (8.14/15)	***£2,880***	***Tony Tomlinson***	***November 2014***	***FINAL (APR 15 AC)***	***Police Objective Analysis (POA) – GREEN*** **Home Office Annual Data Return (ADR 502) – AMBER RED**	***0***	***3***	***0***

Assignment ***Reports considered today are shown in bold italics***	**Fee (as per audit plan)**	**Responsible Officer**	**Fieldwork**	**Status**	**Opinion**	**Actions Agreed (by priority)** **High**	**Medium**	**Low**
Data Security (9.14/15)	***£4,240***	***Nancie Shackleton***	***November 2014***	***FINAL (APR 15 AC)***	***GREEN***	***0***	***1***	***2***
Asset Management (10.14/15)	£1,560	Tony Tomlinson	January 2015	DRAFT – 12 JAN 15				
General Ledger (11.14/15)	£1,250	Tony Tomlinson	February 2015	DRAFT – 5 FEB 15				
ICT Change Management (12.14/15)	***£4,260***	***Nancie Shackleton / Tony Tomlinson / Julie Flint***	***December 2014***	***FINAL (APR 15 AC)***	***AMBER / GREEN***	***0***	***2***	***0***
Cash, Banking & Treasury Management (13.14/15)	£1,250	Tony Tomlinson	January 2015	DRAFT – 02 MAR 15				
Delivery of the Police and Crime Plan (14.14/15)	£4,260	Julie Flint	February 2015	DRAFT – 16 MAR 15				
Risk Management (15.14/15)	***£2,900***	***DCC Roach / Ginny Mason***	***March 2015***	***FINAL (APRIL 15 AC)***	***OPCC – GREEN*** **FORCE – AMBER / GREEN**	***0***	***2***	***1***
Payroll (including Pensions and Expenses)	£2,200	Tony Tomlinson	March 2015	In Quality Assurance				
Follow Up	£1,400	Julie Flint / Tony Tomlinson	February / March 2015	In Quality Assurance				
Payments & Creditors	£1,250	Tony Tomlinson	March 2015	In Quality Assurance				
Income & Debtors	£1,250	Tony Tomlinson	March 2015	In Quality Assurance				
Collaboration - Efficiency Savings Plans	£2,200 (to be completed as part of a joint review with the East Midlands)	Julie Flint / Tony Tomlinson	March 2015	Fieldwork in Progress				
Collaboration – Innovation Fund		Julie Flint / Tony Tomlinson	March 2015	Fieldwork in Progress				

Other Matters

Planning and Liaison:

We have held regular updates with the Chief Finance Officer (OPCC) and also regular Anti-Fraud meetings with PSD, HR, Finance and OPCC to discuss any emerging issues which could impact on the control environment.

The Joint Independent Audit Committee should note that the assurances given in our audit assignments are included within our Annual Assurance report. In particular the Joint Independent Audit Committee should note that any negative assurance opinions will need to be noted in the annual report and may result in a qualified or negative annual opinion.

Internal Audit Plan 2014/15 - Change Control:

- As reported previously, we were requested by management to delay the start of the Firearms Asset Management. We swapped the timing of this with the Proceeds of Crime Act review to ensure continued delivery of audits throughout the year, this has now been finalised.
- As reported previously, following discussion at the East Midlands Joint Chief Finance Officers meeting it was agreed that we would undertake an additional review of G4S Niche Service Provision to be able to provide assurance to the region on the arrangements in place.

Information and Briefings: We have issued the following updates electronically since the last Joint Independent Audit Committee:

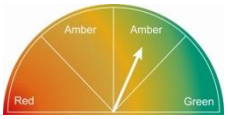
Emergency Services News Briefing – December 2014

- Emergency Services Collaboration – The Current Picture Fire Incidents Response Times: England, 2013-14.
- Changes to the police disciplinary system.
- An Inspection of Undercover Policing In England and Wales.
- Crime-recording: making the victim count.

Emergency Services News Briefing – February 2015

- Integrity Matters
- Independent Review: The Police disciplinary system in England and Wales
- Police leaders support call for mentally ill to get the right care and treatment
- Police and crime commissioners: progress to date
- New criminal offences statistics in England and Wales
- Estimating demand on the police service
- Bank detail fraud
- A master class in managing contracts and getting best value from third party providers (new dates)

Key Findings from Internal Audit Work

Service Expectations – Firearms Asset Management (6.14/15)	**Opinion:** **H – 1** **M – 0** **L – 3**	

Design of control framework

We found the following controls were adequately designed:

- A Lincolnshire Police Headquarters Armoury Standard Operating Procedure (SOP) is in place that formally documents day to day procedures in relation to Firearms. This document is up to date (V1 2014) and has been subject to review;
- Responsibility for Firearms management has been documented within the SOP;
- Access to the Headquarter Armoury is restricted and controlled via access cards and the use of CCTV; and
- The booking in and out of firearms has been adequately defined with the appropriate access controls.

Application of and compliance with control framework

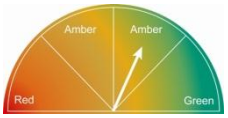
We found the following controls were adequately applied and complied with:

- The Headquarters Armoury is effectively manned by the Force Control Room Inspectors 24 hours a day; and
- Weapons and related items purchased are recorded onto the CHIPS system in a timely manner once they are received.

However we identified the following weaknesses which resulted in one high risk recommendation.

- There is inconsistent evidence to support that inventory checks are being performed in line with the Force's Standard Operating Procedure (High).

All recommendations have been accepted by management.

Financial Management including Budget Management and Procurement (7.14/15)	**Opinion:** **H – 0** **M – 2** **L – 3**	

Design of control framework

Our review has identified the following areas where controls have been adequately designed:

- The Financial, Contract and Procurement Regulations detail budgetary control responsibilities;
- Procedures for procurement are incorporated in the Financial, Contract and Procurement Regulations (the Regulations). Also included is a Procurement Flow Chart which sets out the process for procuring goods and services. The Regulations were first approved in November 2012 and were updated in August 2014;
- The Regulations sets out the approval and award delegated levels of authority. This also clearly defines the requirements for quotes to be obtained and tender exercises carried out;
- A budget timetable is established and is communicated to all budget managers;
- Budget managers are provided with detailed guidance on how to prepare their budget and to aid them with the figures, details of the current year's budget and actual income /expenditure to date; and
- A designated accountant is allocated to specific budget areas.

Application of and compliance with control framework

Our review has identified the following areas where there is application of and compliance with the control framework:

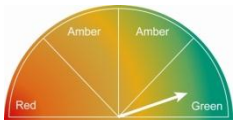
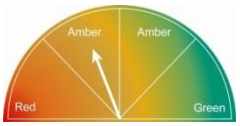
- The budgets for 2014/15 were reviewed and approved by the Resource and Governance Meeting in February 2014;
- The budgets figures were input onto the general ledger prior to the start of the financial year;
- Budget reports are provided by Finance and can be obtained directly from T Police to enable budget holders to review the information. Where required the designated Finance Officers holds regular meetings with the budget holders;

- Variances are identified as part of the budget monitoring process;
- The budget holders for centralised services understand their budgets responsibilities; and
- A system budget report is produced from T Police each month and this is reviewed by the Reporting Manager and the Accountant. A narrative is documented for any variances and this report is then provided to the Chief Finance Officer. Accuracy testing of the budget report provided to the Chief Finance Officer for September 2014 did not identify any issues. .

We have made two medium risk recommendations in relation to the application and compliance of the control framework. The medium priority recommendations are in relation to the following areas:

- During our testing of procurements between £10,001 and £25,000 we identified two where the procurement was not subject to approval in accordance to the Financial Regulations. (Medium);
- During our testing of procurement we identified there were inconsistencies in respect of maintaining audit trails of the procurements. Documentation was not always found on file and in some instances was not held on T Police or on the Folder on the server (Medium).

All recommendations have been accepted by management.

Data Returns – HMIC VFM Profiles (8.14/15)	**Opinion:** **H – 0** **M – 3** **L – 0**	**Police Objective Analysis (POA)**  **Home Office Annual Data Return (ADR 502)** 

Design of control framework

Our review has identified the following areas where controls have been adequately designed:

- CIPFA (Chartered Institute of Public Finance Accountants) provides comprehensive annual guidance notes on the Completion of the Police Objective Analysis (POA).
- A designated Corporate Accountant in Finance is responsible for populating the Police Objective Analysis (POA).
- Procedure notes are also in place to assist with the collection and preparation of the data for the POA. The procedure notes include definitions and methods of calculation.
- A designated officer (HR Support and Systems Manager) in HR is responsible for the collation and completion of all the ADR returns to the Home Office.
- Comprehensive guidance is provided by the Home Office annually on the completion of the annual data returns (ADR's).

We have made two medium risk recommendations in relation to the design of the control framework. These are in relation to the following areas:

- Procedures are not in place for the collection and preparation of the data for the ADR 501 and ADR 502 data returns. Training has also not been provided to another member of the team on the completion of the ADR 501 & ADR 502 data returns in case of absence or continuity if required. (Medium)
- The data returns (ADR 501 & 502) are not subject to independent review by another member of the HR Team and is also not subject to review by the Force Senior Management Team. (Medium)

Application of and compliance with control framework

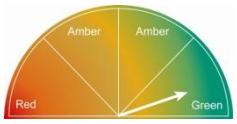
Our review has identified the following areas where there is application of and compliance with the control framework:

- An adequate internal process is in place to ensure that the data returns submitted are accurate.
- The POA is subject to independent review by the Reporting Manager. An audit trial of the emails is retained by the Reporting Manager.
- The POA was reviewed by the Force Senior Leadership Team Meeting on 22 July 2014.
- The POA return was submitted within the timescales set by CIPFA.
- Queries raised by CIPFA were reviewed and changes were made where appropriate and the revised POA was submitted to CIPFA on a timely basis.
- The ADR 501's for October 2013 and April 2014 and the annual return ADR 502 were submitted to the Home Office on a timely basis.
- Revisions were made to the POA and the ADR 502 where appropriate and the revised returns were submitted to the Home Office on a timely basis.

We have made one medium risk recommendation in relation to the application and compliance of the control framework. This is in relation to the following area:

- Adequate audit trails have not been maintained of all source documentation and calculations made to the data used to compile the ADR 501 & ADR 502 data returns and of any subsequent amendments made to these data returns. (Medium)

All recommendations have been accepted by management.

Data Security (9.14/15)	**Opinion:** **H – 0** **M – 1** **L – 2**	

Design of control framework

A number of areas of adequately designed controls were identified during the review, in particular:

- The Force has documented the following policies that are available to staff on the Intranet that include data security contents all of which include the relevant guidance that would be expected.
- A mandatory data security training module is provided to staff via an electronic learning tool NCALT. An escalation process has been designed so that failure to complete the mandatory training will result in removal of network access permissions.
- Robust network password and account lockout settings have been configured to reduce the risk of weak account passwords and unauthorised access.
- The User Account Creation and Deletion Process for Starters and Leavers has been documented to ensure that staff are aware of the process to follow. The procedure requires a completed form from HR requesting account creation. All forms are then retained by the service desk.
- A procedure for deleting all user accounts (including G4S) when users leave the Force has been documented and is included with the user account management procedure. Accounts are required to be deleted the day after a user leaves the Force unless there is a special requirement for the account to remain open, approval is required for this to occur.
- Remote access is provided only to authorised users, requiring approval from their managers to ensure that access is appropriate. Users are issued a licence with SecurEnvoy that upon request sends a code within a text message to their mobile phone. This code, along with their username and account password is required to access the VPN.
- Third party access is activated only as required, it is then removed once the work has been completed to reduce the risk of unauthorised access to the network.
- Device encryption is in place for all mobile devices including laptops, iPads and BlackBerrys so that stored data cannot be accessed by unauthorised users.
- McAfee antivirus is installed on all computers and servers to protect them against potential viruses and malware.

- A documented disposal procedure is in place that states all assets are to be disposed of by the IT department. Devices that hold data are degaussed using a magnet to render the item inoperable. The device is then required to be destroyed and shredded on site by Concept Management.

We have made one medium priority recommendation in relation to design of the control framework which is included in the action plan in Section 2 and is summarised below:

- The disposal register is not reconciled to the item list provided by Concept Management to ensure that redundant equipment was collected and destroyed as required. As the disposal register is not reconciled, the asset register may not be accurate which could lead to assets not being disposed of as expected increasing the risk of loss of data. (Medium)

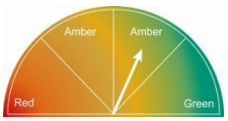
We have identified areas of adequately applied controls during the review, including the following:

Application of and compliance with control framework

We confirmed the following recurring controls are operating and being complied with:

- The SIRO has escalated instances of non-completed mandatory data security training. We confirmed that line managers were then informed of non-compliant staff. As at the end of October 2014 all remaining non-compliant staff were emailed by the SIRO informing them that if the training was not completed by the end of November 2014, their user access would be disabled.
- New user request form had been authorised and retained by IT, reducing the risk that unauthorised accounts are created.
- Network accounts had been revoked to ensure that staff cannot access Force data once they have left.
- Review of the third party remote access list within active directory revealed that none of these accounts were active during the review.
- Antivirus was updated to the most recent version.

All recommendations have been accepted by management.

ICT Change Management (12.14/15)	**Opinion:** **H – 0** **M – 2** **L – 0**	

Design of control framework

We identified a number of well-designed controls, in particular:

- Documented procedures have been designed for controlling amendments to production software, as documented and communicated to all ICT staff in the Change and Release Policy, the Change Management Process and the Request for Change form template.
- Procedures are in place which require pre- and post-implementation tests to be considered and where appropriate, carried out on all changes.
- The Force has developed a Change and Release Management Policy, dated March 2014, and next due for review in March 2015. This specifies at a high level that all changes to IT resources must follow the Force's defined set of Change and Release Management processes. The Policy further states that all new systems that have connectivity to or impact upon a Production (live), Pre-Production or Test environment, must also follow the organisation's standard change control process.
- The IT department's Change Management processes require a documented 'Backout Plan' to be provided as part of each Request for Change, reducing the risk that any changes made to the live environment cannot be reversed with no or minimal impact on users, or, if it is considered that there would be a significant outage, that this is not known and appropriate mitigation action is not planned accordingly.
- Information is provided in the Change and Release Management Policy and the Change Management Process document concerning the roles and responsibilities of IT staff in respect of Change Management procedures, including the Change Manager's enforcement role.
- Mandatory change approval procedures have been documented in the Change and Release Management Policy and the Change Management Process document.

However, we did identify 2 design control weaknesses in relation to Force's ICT Change management arrangements which have resulted in 2 Medium priority recommendations being made, as follows:

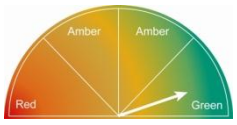
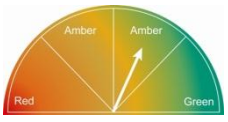
- Although the change control process has been documented in the Change Management Process document, which was in draft at the time of our review, we identified areas that had yet to be completed in detail. (Medium)
- There is a lack of a defined and documented process for checks to be undertaken by the Change Manager on conformance with approved Change Management procedures, as set out in the Change and Release Policy and the Change Management Process guides.

Application of and compliance with control framework

Our testing showed that the recurring controls identified and evaluated during this audit are generally operating and being complied with, as follows:

- We reviewed the history (and attached documents, including Requests for Change) of a sample of 5 non-Emergency changes and 1 Emergency change for the period August to December 2014, selected from the IT Change Managers Change log and confirmed that
  - A Request for Change document had been completed and retained for each change.
  - CAB approval for the change had been granted (and the dates of approval recorded) in each instance.
  - Email correspondence regarding the submission, approval, related management queries and implementation of the change had been retained in Sostenuto (the ICT departments Service Desk application) in 4 of the 6 changes, tested, but still needed to be included for 2 changes, though this matter was subsequently followed up and resolved by the Change Manager.
  - Any downtime resulting from the change had been estimated and plans made to notify users affected by it, accordingly.
  - Details had been provided on the RFCs of pre- and post-implementation test plans.
  - Reversal and Rollback Plans had been included in the RFCs for all the changes reviewed.
  - Confirmation had been obtained from the change initiator/tester and retained in the change documentation in Sostenuto that all action on the change had been completed, and the change marked as closed in 4 of the 6 changes reviewed. Information on the outstanding changes was, however, being followed up the Change Manager at the time of our testing.

All recommendations have been accepted by management.

Risk Management (15.14/15)	**Opinion:** **H – 0** **M – 2** **L – 1**	**OPCC**  **FORCE** 

Design of control framework

Our review has identified the following areas where controls have been adequately designed:

The Force

Our review has identified the following areas where controls have been adequately applied:

- A Force Risk Management Policy is in place. The Policy is subject to annual review and was last updated in October 2014 and is next due for review in October 2015.A 2013-2015 Risk Management Strategy is in place and sets outs the Force's approach to risk management and defines the roles and responsibilities. Section 4 of The Lincolnshire Police: Risk Management Strategy 2013-2015 sets out the Roles and Responsibilities in relation to risk management.

- Appropriate members of staff were provided with training on risk management by external company in June 2014
- The Risk Management Board meets quarterly and reviews the Force's key risks. The Board are responsible for quality assuring risk scores, the impact of control measures, and agreeing actions for the developing controls.
- A Confidential Risk Register is maintained for those risks which are confidential in nature. These risks are not included on the Force's Risk Register and are also not discussed at the Risk Management Board.
- The Confidential Risk Register is maintained by a designated Force Officer and access to this register is restricted by username and password.
- The Confidential Risk Board meets each quarter before the Risk Management Board to address any confidential risks and is chaired by the Deputy Chief Constable.
- The Deputy Chief Constable represents the Risk Management Board at the Senior Leadership Team meetings. The top five business risks are monitored by the Senior Leadership Team.
- The Senior Leadership team reviews high level strategic risks before they are presented to the Regional Deputy Chief Constables Board on a quarterly basis.

Office of Police and Crime Commissioner

- A Risk Management Strategy is in place. The Strategy was approved by the Joint Independent Audit Committee and is subject to regular review.
- Guidance on how to categorise the impact of the risk is included in the Strategy document.
- A 4 x4 risk matrix is used and risk evaluation includes assessing the probability and impact of the individual risks. Each risk is scored on the basis on the likelihood of the risk occurring and the impact it would have if it did happen.
- Responses to the risk include: transfer the risk; tolerate the risk; terminate the risk; and treat the risk. This is dependent on the OPCC's risk appetite, that is; what level of risk the OPCC is prepared to tolerate. The BSI Risk Management Standard is used to define the OPCC's current risk tolerance or risk appetite.
- Once the risks have been identified and the actions to mitigate the risk are agreed, the actions are monitored to ensure that the actions are planned, resourced and monitored.
- The OPCC Research and Performance Officer attended the training risk management training provided in June 2014.Roles and Responsibilities have been defined in the Risk Management Strategy.
- The OPCC's Risk Register is a standing item and is reviewed/ discussed at the Internal Management meetings once a month.
- The OPCC's Risk Register is reported to the Joint Audit Committee.
- A formal assurance process in place to provide the PCC with appropriate evidence to validate the controls over risk management.
- The Joint OPCC and Chief Constable's Assurance Map is reported to the Joint Independent Audit Committee quarterly.

Application of and compliance with control framework

We have made two medium risk recommendations in relation to the application and compliance of the control framework. These are in relation to the following areas:

- There is not a consistent approach to maintaining departmental Risk Register. In addition, the Risk Register templates were not used consistently and also in the recording of details onto the Departmental Risk Registers. In one case the Risk Register was also being used as an action log. For two risks the mitigating controls documented on the Risk Register do not address/ adequately address the risk to the department/ organisation. (Medium).
- A risk was recently added to the Force Risk Register regarding the number of Licensing applications waiting processing. It was noted issues like this and other similar business issues which would have an impact on the department achieving its objectives are not identified as risks and included on the Departmental Risk Registers.(Medium)

All recommendations have been accepted by management.