POLICE & CRIME COMMISSIONER FOR LEICESTERSHIRE JOINT AUDIT RISK & ASSURANCE PANEL

PAPER MARKED

E

Report of	**CHIEF CONSTABLE**
Subject	**INTERNAL AUDIT FUNCTION – SERVICE IMPROVEMENT UNIT & INFORMATION MANAGEMENT COMPLIANCE AUDIT FUNCTION**
Date	**TUESDAY 3 DECEMBER 2013 – 1.00 P.M.**
Author :	**SERVICE IMPROVEMENT MANAGER**

Purpose of Report

1. This report provides the Panel with an overview of the Leicestershire Police internal audit arrangements; describes the function of how a work plan is developed and the strategic governance of any identified risks to the Force.

Recommendation

2. The Panel are recommended to discuss the content of the report and the framework that is used to ensure that Leicestershire Police have a robust internal audit plan that is also dynamic to respond to changing needs and threats and how audit findings are acted upon.

Background

3. The Force has two separate internal audit teams, with distinct areas of responsibility, the Service Improvement Internal Audit Team based with Corporate Services (Ch. Supt Pandit) and the Information Management (IM) Compliance Auditors based within the Professional Standards Department (Supt Holyoak).

Internal Audit Team - Service Improvement Unit

4. In 2011 the Force internal audit team based within Service Improvement was restructured against revised terms of reference and audit methodology.

5. This change allowed for a more 'risk based' approach to ensure that policy and procedures are being complied with rather than following a predetermined programme of audit.

6. This revised structure has allowed for the unit to be more responsive to emerging or perceived organisational risks especially in the area of crime recording and classification issues including elements of data quality.

7. Service Improvement Unit is the location of the Force audit function which undertake work looking at the broad spectrum of compliance for crime and incidents. They also undertake audits looking how the Force correctly identifies and deals with vulnerability cases. During these audits the auditors will also look at specific data quality issues, however, the scope of the audit programme with the available resources means that this assessment is a secondary requirement.

8. Both audit functions are appropriately and independently placed within Corporate Services and PSD to conduct relevant, timely, proportionate and where possible pre-emptive rather than reactive audit scrutiny.

9. The Service Improvement audit manager is also now responsible for monitoring and supporting the recommendations that emanate from the external RSM Tenon audit programme. This arrangement provides for a structured co-ordination and read across between internal and external audit programmes.

Processes and Outcomes

10. Each completed audit whether completed in Service Improvement or PSD is moderated to ensure the findings and subsequent recommendations are based upon statistically reliable levels of data and the audit methodology is robust to withstand third party scrutiny.

11. In the past three months Service Improvement audits have included:

- How officers apply restorative justice procedures to conclude criminal and anti-social behaviour complaints

- The levels of compliance in correctly recording crime complaints (this supports the level of confidence the public have in our crime recording procedures).

- To establish whether there are any deficiencies in the recording and concluding of complaints of anti-social behaviour.

- How the Force recognises and responds at the first point of contact to repeat and vulnerable victims and callers.

12. A structured risk assessed approach is taken which includes when and where to audit, depth and scope of any audit, the nature of the business, previous audit findings and any additional contextual support e.g. national concerns over a particular business area / process.

13. The findings of any audit are subject to peer moderation and when appropriate discussions with subject matter experts both locally and nationally.

14. Completed reports have a structured path through the organisation with accountability on recommendations. Where significant threats are identified, which pose either reputational issues or serious breaches in procedure, then relevant Chief Officers are involved. However, the majority of audits are

considered at the Force Op Enigma group where recommendations and business owners are agreed.

15. Dependant on the nature and outcome of the audit, reports are also subject to discussion at various strategic boards, including the Force Performance Delivery Group, Safe and Confident Communities Board, Strategic Reputational and Integrity Management Board, and the Chief Officer Executive Group.

16. At present the only significant issue is the compliance to national crime recording standards. Previous audits had identified that for certain crime types there was a disparity between what was originally reported and what was entered onto the Force's crime system. This risk was escalated through the organisation to Chief Officer's and an action plan was put in place to address the risk. Additional scrutiny is now in place through Op Enigma to ensure that action required to rectify the risk is sufficient and appropriate.

Information Management Compliance Audit Function - PSD

17. Following the enactment of the Data Protection Act in 1984, the Association of Chief Police Officers (ACPO) identified the need for a Chief Constable, as data controller, to audit compliance with the data protection principles. In Leicestershire, responsibility for auditing was given to the Data Protection Section in 1990. The first ACPO Data Protection Audit Manual was issued in 1996.

18. In 1998, the Data Protection Act was updated to include manual records. Additionally, the Bichard Inquiry (2004) emphasised the importance of good data quality to ensure information could be linked together to provide a comprehensive picture about an individual and this was incorporated into the Management of Police Information (MoPI) Guide and enshrined within legislation by virtue of the Statutory Code of Practice for the Management of Police Information 2005. The Data Protection Section became the Information Management (IM) Section to reflect this wider responsibility.

19. A Data Quality Group was set up to monitor the implementation of recommendations from the IM compliance audits.

20. The ACPO Audit Manual, owned by the ACPO Data Protection, Freedom of Information and Records Management Portfolio Group (Anne Chafer, Information Manager for Leicestershire Police owns the Audit Portfolio on this group and is responsible for the production of this manual), includes a risk assessment process. This is completed in consultation with the Information Asset Owner and enables a range of risks to be considered for each Force application containing personal information. The risks include the potential failure to protect children and vulnerable adults and possible litigation against the Force for the unlawful arrest of an individual.

21. The Risk Assessments identify high risk applications which are prioritised for inclusion in the PSD Audit programme. The Programme is submitted to the DCC as SIRO for approval as is the one year audit plan which is compiled following consideration of resources available. A copy may be provided to the HMIC if required.

22. The data protection principles considered in an IM compliance audit include;

looking at fair and lawful processing of information, particularly around information sharing; ensuring information is adequate relevant and not excessive as well as being accurate and up to date; examining retention and deletion processes to ensure information is not kept longer than necessary; ensuring appropriate security is in place by assessing both physical security and handling rules.

23. During the audit, if an issue which will impact upon operational effectiveness is identified, this will be addressed immediately (inaccurate record which may lead to the arrest of an innocent party).

Circulation of Findings

24. The Audit Report with summary of findings and recommendations is provided to the DCC who approves the Audit and authorises circulation to relevant parties i.e. asset owner, training, etc., in order that the action plan is completed as required.

25. Once the action plan is completed, this is submitted to the DCC so the audit can be closed. A dip sample may be undertaken at a later date to ensure the recommendations have been effective.

26. In the past six months Force audits have included:

- Transaction audits for PNC, PND and DVS

- Audit of indecency suspects to ensure their nominal details are in a searchable field, that all their details match with those on other Force records/PNC and that alias names and dates of birth are included, check the ethnicity box is correctly completed, check address/postcode to ensure correct mapping, check any 'no crime' classification is correct, check any suspect eliminated to ensure they are not uploaded to PND, check if scanned documents are attached to the record and if all relevant information is searchable.

- An audit of Sentinel records across each LPU is currently in progress.

- In progress, PNC Wanted arrest – undertaken by Area but overseen by IM compliance audit.

27. To ensure that the IM compliance audit team have appropriate training they are required to undertake the ISEB in Data Protection so that they have a comprehensive understanding of the legislation (they also provide advice and guidance to the Force) Both SIU and IM audit teams are required to receive training through the Chartered Institute of Internal Auditors courses.

Implications

Financial :	None
Legal :	None
Risks and Impact :	None
Link to Police and Crime Plan :	The audit programme allows for data accuracy and compliance to the HOCR and ensures integrity in report performance data.

List of Appendices

Attached is the programme of audits for 2013/14 for the Service Improvement Unit

While each audit will have a number of recommendations and these are corporately monitored there are two over-arching themes that are common to the majority of the audits i) a disparity between what was originally reported and what was entered onto the Force's crime system and ii) the correct entry of information onto IT systems e.g. correct spelling of names DOB's etc. Both are actively being actioned and have Chief Officer scrutiny.

Person to Contact

The Force appointed lead for internal audit is the Head of Corporate Services Chief Superintendent Steph Pandit, the departmental lead and reporting officer is Mr Glenn Brown as Head of Service Improvement.

C/Supt Steph Pandit, Corporate Services, Tel 0116 2482303
Email: steph.pandit@Leicestershire.pnn.police.uk

Mr Glenn Brown, Service Improvement Manager, Tel 0116 248 2510
Email: glenn.brown@Leicestershire.pnn.police.uk

Service Improvement Unit
Audit Programme 2013 - 2014

Appendix A

Audit Area 2013 - 2014	Previously completed	Priority	Tier	Notes	Month													Date Set
					Apr-13	May-13	Jun-13	Jul-13	Aug-13	Sep-13	Oct-13	Nov-13	Dec-13	Jan-14	Feb-14	Mar-14	Apr-14	
ASB																		
ASB incident closed as non ASB	Aug-12	Medium	2	Local				C										Y
Classification																		
Classification of Crime	Feb-13	Medium	2	Audit Guide													OS	Y
Classification of Crime - Serious Assaults	Aug-12	High	1	Audit Guide											OS			Y
Classification of Crime - Sexual Assaults	Sep-12	High	1	Audit Guide											OS			Y
Drugs Classification	Dec-12	Medium	2	Audit Guide													OS	Y
Racist Classification	Dec-12	High	1	Audit Guide													OS	Y
Hate Crime	Jan-13	High	1	Local								OS						Y
Threats to Kill	Feb-13	High	2	Local										OS				Y
NCRS																		
Crime Recording - Violence/Crim Dam/ASB/Racist/Domestic/Sexual	May-12	Medium	2	Audit Guide											OS			Y
Crime Recording - Burglary/Firearms/Theft/Vehicle	May-12	Medium	2	Audit Guide											OS			Y
Operation Enigma																		
72 Hour Incident and Crime Check ('**Op Enigma**')	N/A	High	1	Local		C												Y
Burglary Dwell. Incidents closed as non-Burglary Dwell.	N/A	High	1	Local	C													Y
Theft Classification on CIS	N/A	High	1	Local			C											Y
Theft Dwelling Classification on CIS	N/A	High	1	Local			C											Y
Criminal Damage Classification on CIS	N/A	High	1	Local			C											Y
Burglary OTD Classification on CIS	N/A	High	1	Local			C											Y
Violent Crime Incidents	N/A	High	1	Local				C										Y
Domestic Incidents on CIS (Standard/Medium/High risk)	Jan-12	High	1	Local				C										Y
Malicious Comms CIS records	N/A	High	1	Local				C										Y
Vulnerabilty Records (Adult)	Jan-13	High	1	Local				C										Y
Vulnerabilty Records (Child)	Jan-13	High	1	Local				C										Y
1st Harassment CIS Records	N/A	High	1	Local				C										Y
Theft from MV incidents closed as non-theft from MV	N/A	High	1	Local					C									Y
Theft of MV incidents closed as non-theft of MV	N/A	High	1	Local					C									Y
Vehicle Interference classification on CIS	N/A	High	1	Local					C									Y
Comm. Burglary Incidents closed as non-Comm. Burglary	N/A	High	1	Local					C									Y
ASB STORM Incidents	Jun-12	High	1	Local					C									Y
Sentinel Records	Oct-12	High	1	Local					C									Y
No Crime																		
No Crime **(Part of Op Enigma)**	Dec-12	High	1	Audit Guide						C								Y
No Crime Rape Only	Mar-13	High	1	Audit Guide								OS						Y
No Crime CAIU	Dec-12	Medium	1	Local								OS						Y
NSIR																		
NSIR	May-12	High	1	Audit Guide							OS							Y
Detections																		
Detected Crime: Charges	Sep-12	Medium	2	Audit Guide							C							Y
Detected Crime: Conditional Cautions	Mar-12	Medium	2	Audit Guide								R						Y
Detected Crime: Final Warnings	May-12	Medium	2	Audit Guide								R						Y
Detected Crime: Formal Warnings for Cannabis	Feb-13	Medium	2	Audit Guide												OS		Y
Detected Crime: Reprimands	Sep-12	Medium	2	Audit Guide								R						Y
Detected Crime: Summons	Nov-12	Medium	2	Audit Guide								R						Y
Detected Crime: TIC's	Feb-12	Medium	2	Audit Guide								IP						Y
Detected Crime: PNDs	Sep-12	Medium	2	Audit Guide							C				OS			Y
Detected Crime: Simple Cautions	Feb-13	Medium	2	Audit Guide	C											OS		Y
Community Resolution (RAIN) **(Part of Op Enigma)**	Mar-12	High	1	Local								C						Y
Fraud																		
Fraud	Sep-09	Low	2	Local														TBC
Bilking	Jan-12	Low	2	Local														TBC
E-Bay Fraud	Sep-09	Low	2	Local														TBC
Non-Sanctioned Detections																		
Non Sanction Detections - DG	Nov-08	Low	4	Audit Guide													OS	Y
Non Sanction Detections - DO / DS	Apr-12	Low	4	Audit Guide													OS	Y
Safeguarding																		
Safeguarding - DASH	Dec-12	High	1	Local						OS								Y
Safeguarding - Harassment	Jul-12	High	1	Local						OS								Y
Rape Investigation Procedures	Sep-12	High	1	Local							OS							Y
CAIU Complete Audit	Dec-12	High	1	Local								OS						Y
Safeguarding - Missing Persons	Jul-12	High	1	Local								OS						Y
Specialist Departments																		
Economic Crime Unit	N/A	TBC	TBC	Local														TBC
Victims Code																		
Victims Code - All Crime	Apr-12	Medium	2	Local												OS		Y
Vulnerability																		
Vulnerable and Repeat Victims Audit (CMD)	Jan-13	High	1	Local					C									Y
Ad-Hoc																		
Safegaurding: Comprehensive Referal Desk	N/A	Medium	2	Local														TBC
Safegaurding: Foreign Nationals	N/A	High	1	Local														TBC
Suspect on CIS compliance	Nov-12	Medium	2	Local														TBC
Burglary Response Times	Dec-08	Medium	3	Local												OS		Y
Crime Recording Vaildation Process	Jan-13	Medium	2	Local											OS			Y
Crime Mapping (Columbus)	Apr-13	Medium	3	Local				C										Y
Domestic Violence Disposed by Restorative Justice	N/A	Medium	2	Local														TBC
Murder - (CIS/Taskmaster)	N/A	Medium	2	Local														TBC
Rural Plant theft Audit	N/A	Medium	2	Local														TBC
Critical Incidents (Taskmaster)	Apr-11	Medium	1	Local														TBC
Child Safety Inspection Audits	N/A	High	1	Not Yet Set														TBC
No. of Audits Completed (C)					2	1	4	8	7	1	2	1	0	0	0	0	0	26
No. of Audits awaiting Report (R)					0	0	0	0	0	0	0	4	0	0	0	0	0	4
No. of Audits awaiting Moderation(M)					0	0	0	0	0	0	0	0	0	0	0	0	0	0
No. of Audits and or Report In Progress (IP)					0	0	0	0	0	0	0	1	0	0	0	0	0	1
No. of Audits Outstanding not yet started (OS)					0	0	0	0	0	2	2	5	0	1	6	4	5	25
No. of Audits On Hold (OH)					0	0	0	0	0	0	0	0	0	0	0	0	0	0
Total					2	1	4	8	7	3	4	11	0	1	6	4	5	56

*The boxes represent the start of the audit and therefore may continue into other month(s) which are not depicted in the schedule