.


# Leicestershire Police

# Internal Audit Inspection Team Methodology Report

June 2014

Report Compiled by: Fiona Trahearn – Audit Inspection Manager

Responsible Officer: Glenn Brown – Service Improvement Manager

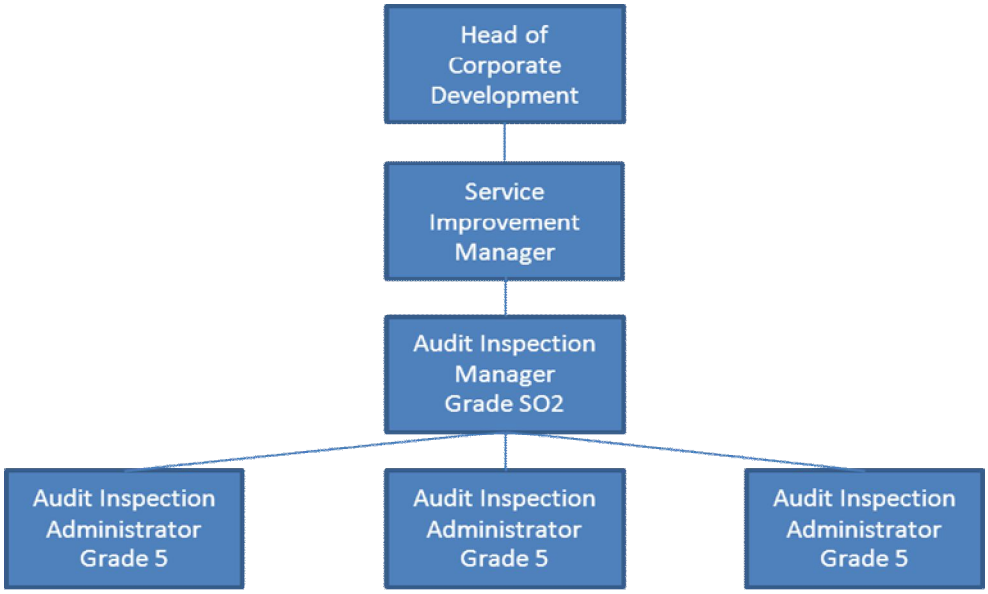
## Introduction

This report looks to explain in detail the 12 step life cycle of an audit from beginning to end. The Internal Audit Inspection Team operates within a comprehensive and robust audit schedule which covers a wide range of areas from classification of detected crimes, to specific departments within the Force and compliance to internal and external policies and procedures.

### Report Contents

## Background

The Internal Audit Inspection Team sits within Corporate Development, Service Improvement Unit. The team is 4 strong, which includes the Audit Inspection Manager and 3 x full time Audit Inspection Administrators. The Audit Inspection Manager is directly answerable to the Service Improvement Manager. This is detailed in the below chart:




The Internal Audit Team is physically positioned at Force Headquarters, within the Service Improvement Office.

The Audit Inspection Administrators skill set includes:

- Analytical and problem solving skills
- Comply with the Data Protection Act
- Good working knowledge of computer systems
- Good knowledge of force Crime and Intelligence systems
- Able to extract data using Business Objects
- Maintain up to date knowledge and understanding of criminal law, investigative processes, Home Office Counting Rules and other internal guidance
- To audit, analyse and report on individual systems to determine compliance with MoPI, National Crime and Recording Systems, NSIR, Home Office Counting Rules, Victims Code, Police National Computer Systems Data Protection Act
- Provide advice and guidance to officers, area crime management units
- Examine the standard of crime investigations to determine if they are of an acceptable quality and provide recommendations for improvement.

The Audit Inspection Administrators also work towards the Internal Audit Standards and Best Practise guidance. This was a course that was attended by the team in June 2008.

## Methodology

The below chart shows the life cycle of an audit from the first scoping phase right through to the audit schedule phase, more detail has been added into the below sections to explain what happens within each stage.


## 1. Scoping

During the scoping phase of an audit, the Internal Audit Inspection Team takes into consideration a range of factors which include:

- Previous audit template and question set
- Previous sample size, data set period, risk of previous audit
- Previous recommendations
- New policies / processes both nationally and locally
- Any additional information which is either within the corporate memory, media coverage, recent HMIC results etc.

When the above have been considered, and any changes made to the audit template, the audit team move on to the next phase of the audit cycle.

## 2. Initial Consultation

This phase of the audit involves the Internal Audit Inspection Manager meeting with the head of the department/force lead for the audit area. This meeting involves discussing:

- The purpose of the upcoming audit
- The proposed question set
- Approximate time-scales and what to expect
- Any suggestions regarding additional questions/areas to look at
- Sample size and data set period

The main purpose of this consultation is to get 'buy in' from the department, to ensure that the audit work is completed *with* the department rather than *to* the department.

## 3. Question Set Agreement

Following the consultation, the Audit Inspection Manager makes a final draft of the question set and sends this over to the department head/force lead for comments. This is the department head/force leads opportunity to add in any other questions, or comment as to why suggested questions are not applicable etc. This is then agreed by the department and also signed off by the Service Improvement Manager. The data set period is also agreed at this stage, along with the sample size of the audit.

### Sample Size

In order to determine the sample size of the audit, a number of factors are taken into consideration for example the level of risk to the force from the previous audit, whether the audit is a repeat or a new audit, the previous audits sample size and any issues that arose from this etc. The risk level of the audits is graded as High, Medium or Low. When all of these points have been considered, the tier level of the audit is specified:

### Tier Level

### Tier 1 – Comprehensive

A comprehensive audit will assess all relevant aspects of the subject area (in most cases a cradle to grave approach). This will aim to identify areas of good and/or bad practise. A Tier 1 audit will be completed if a risk or threat to the force has been identified OR the results from a previous audit require a further in-depth assessment.
Sample Size: 80 records for force audit, OR 40 per BCU.

### Tier 2 – Risk Based

A risk based audit which will assess individual areas of risk upon the subject area or department. A Tier 2 audit will usually be a re-visit of a previous audit where areas for concern were identified; only these specific areas will be assessed.
Sample Size: 60 records for force audit, OR 30 per BCU.

### Tier 3 – Quality Assurance

This audit focusses on key aspects where the subject area is a perceived risk or threat to the force. This audit will assess all relevant audit criteria in order to identify where perceived risks are a reality. Upon completion of a Tier 1, 2 or 3 audits, this audit will follow where areas for concern are identified.
Sample Size: 40 records per Force audit, OR 20 per BCU.

### Tier 4 – Reassurance

A snap shot audit where there is no perceived risk or threat to the force. All relevant audit criteria will be assessed. Where areas for concern are identified a Tier 1 or Tier 2 audit will follow.
Sample Size: 20 records for Force audit, OR 10 per BCU.

The above tier level and risk based approach, along with agreement from the department and sign off from the Service Improvement Manager allows the Internal Audit Team to determine the sample size of the audit.

## 4. Data Extraction

Once the sample size and data set period has been agreed, the auditors will extract this from the chosen system (Storm, CIS, CATS etc) via Business Objects. Depending on what audit is being completed will depend on the variables chosen to extract the data. I.e. for the New Home Office Outcomes audit, the data was chosen by any crime type that had been filed on CIS since 1st April 2014, whereas for a National Standards of Incident Recording Audit, the data is selected by the Opening Code on Storm over a set period of time.

Once the data has been extracted, this is then entered into the audit workbook; a randomising formula is then applied to ensure that all of the records have been randomly selected out of the time frame and criteria that were initially applied. Using this methodology allows the audit to be unbiased and follows the best practise that has been recognised for internal auditing.

## 5. Final Scoping

Once the question set has been agreed and signed off, the sample size has been determined and the data has been extracted, the Audit Inspection Team complete the final scoping of the audit and ensure that the workbook reflects the question set and is fit for purpose. The Audit Inspection Manager goes through the audit with the Auditors to ensure that everyone understands the questions and is looking to answer them in a uniformed approach. The Audit Guides are also completed and shared with the auditors for extra information and as a crib sheet to refer to whilst undertaking the audit.

## 6. Auditing

The Audit Team commence the audit. The team split the audit up into sections and complete each section individually, however when a question rises – this is passed around the team and conclusions are worked out together. When completed a new audit, the team audit a small number of records and then come together in a meeting in order to discuss whether they feel the audit template is appropriate and workable, the questions are correct and unbiased, testing whether the guide is correct and in line with the audit questions, they share the same understanding for specific audit questions, and ultimately that the report will illuminate areas for improvement or good practise. If any of the above are deemed as not working, the team will address this and amend the questions, with agreement of the department head/force lead in order to ensure that the results will be useable and relevant.

## 7. Moderation

Once the audit has been completed, the team then moderate each other's work. Depending on the size of the audit, depends on how many records are moderated. The intention is to always moderate all of the failures, or 1 in 5 records.

Audits are regularly sent to the Force Crime Registrar to also be moderated by a second person. This allows the Audit Team to be confident in our results and gives extra credit to the work undertaken by the audit team. It also allows the team to pick up any areas that have been incorrectly audited and learning comes from this.

## 8. Draft Report

Once the moderation has been completed, the Audit Inspection Manager analyses the results of the audit and puts this into a report. The report is then circulated to the department head/force lead for comment. The report is also sent to the Service Improvement Manager. This allows any urgent findings to be considered and acted upon immediately. It is at this stage where the department head/force lead is invited to respond to the report with comments or questions. The Audit Inspection Manager works alongside the department to ensure that the report is fit for purpose and the results are user friendly. The Audit Inspection Manager gives the department access to 'failed' records in order for them to take 'real life' examples of areas that require improvement, and also areas of good practise that can be shared within their department to aid understanding.

## 9. Final Report

Once the draft report has been circulated and agreed, the final report is written and circulated to whom it is deemed appropriate. This usually includes the Get it Right, First Time attendee list and the department head, with the advisory note that this can be circulated wider as seen fit.

## 10. Get it Right, First Time

The audit report is added to the agenda of this meeting and the Audit Inspection Manager presents the findings of the report to the group. The recommendations are discussed within the group and a recommendation 'owner' is identified. The group is supportive of the audit work that is undertaken and holds persons to account for responding to the recommendations. From this meeting, the findings are filtered out to the appropriate persons on area, departments, specific officers, staff etc.

## 11. Recommendations

Following the Get it Right, First Time meeting, the Audit Inspection Manager adds the recommendations to the Recommendation and Action list that is held within the audit team's files. The intention is to put these onto the 4 Action system when this is up and running within the force. Currently, the Audit Inspection Manager chases these recommendations periodically.

## 12. Audit Schedule

Following all of the above, the results of the audit are assessed by the risk that the audit poses to the Force. This will then determine when the next audit will be completed. This is then added onto the running audit schedule in order to programme in the piece of work.

# Conclusion

The 12 step life of an audit is robust and ensures that when beginning to look at either a new piece of work, or repeating an existing audit, the same measures are applied. Audit work will be considered whether it be self-motivated, following a request from a department, media interest in a particular policing area, an upcoming HMIC inspection or regular audits that are within the schedule as they pose a risk to the force.

The way in which the audits are conducted ensures that the Internal Audit Team work with the organisation rather than impose upon them. The consultation and liaison that occurs during the life cycle of an audit means that the results are fit for purpose and the departments are receptive to the recommendations.

The audit schedule is flexible and allows room for adjustment when an urgent piece of work is required. The schedule is a guide to the Audit Team for what audits are on the horizon however is not constricting which means that they are able to add or alter current work streams as required.

The audit team has started to contextualise the monetary value of each audit in order to assess the costs and the benefits to the organisation. This is done by working out the number of hours spent over the 12 step cycle by both the Audit Inspection Manager, and the Audit Inspection Administrators. This enables the Audit Inspection Manager and Service Improvement Manager to put a 'worth' on each audit, and assess the costs against the benefits in a factual basis, rather than assumption.

The Audit Inspection Manager and an Audit Inspection Administrator attend the Regional Force Crime Registrar meeting. This is held regularly throughout the year and attendees include Nottinghamshire Police, Northamptonshire Police, Lincolnshire Police, Derbyshire Police, City of London Police and Home Office representation. Attending this meeting allows the audit team to discuss regional issues and also ask questions in order to understand how other forces audit specific areas. This forum acts as a regional sounding board and arena to share best practise and float ideas around auditing and inspections.

Overall, the audit cycle is a flexible guideline that follows internal auditing standards of best practise. The results of the audits are moderated and scrutinised and can be relied upon to be significant of the work that is happening within the force today.

Please see Appendix B for a complete breakdown of the audits that were completed in 2013/2014.

## Appendix B

**Anti-Social Behaviour:**

- Incidents that were opened on Storm as ASB, and closed as anything other than ASB
- Sentinel

**Classification of Crime:**

**CIS**

- Burglary
- Domestic Abuse and Harassment
- Hate Crime
- Sexual Assault
- Vehicle Crime
- Violence against the person

**Storm**

- Burglary
- Domestic Abuse and Harassment
- Hate Crime
- Sexual Assault
- Vehicle Crime
- Violence against the person

**National Crime Recording Standards**

- Crime Recording Audit 1 (Violence, Criminal Damage, ASB, Racist, Domestic, Sexual)
- Crime Recording Audit 2 (Burglary, Firearms, Theft, Vehicle)

**Op Enigma/ Missed Opportunities**

*These include classification audits, however were completed in order to establish any missed opportunities and away from the 'standard' classification audits.*

- 72 Hour Incident and Crime Check (Home Office Counting Rules)
- Incidents that were opened as Burglary Dwelling on Storm and closed as Non-Burglary Dwelling
- Theft Classification on CIS
- Theft Dwelling Classification on CIS
- Criminal Damage Classification on CIS
- Burglary Other than Dwelling Classification on CIS
- Violent Crime Incidents within Storm
- Domestic Incident Classification on CIS
- Domestic Incidents within Storm
- Malicious Communications Classifications on CIS
- Vulnerable Adults Classification on CIS
- Vulnerable Child Classification on CIS
- First Harassment Classification on CIS

- Incidents opened as Theft from Motor Vehicles and closed as Non Theft from Motor Vehicles
- Incidents opened as Theft of Motor Vehicles and closed as Non Theft of Motor Vehicles
- Vehicle Interference Classification on CIS
- Incidents opened as Commercial Burglary on Storm and closed as Non Commercial Burglary
- ASB Storm Incidents
- Sentinel Records

**No Crime**

- No Crime – All Crimes
- No Crime – Rape
- No Crime – Child Abuse

**National Standards of Incident Recording**

- NSIR – Full Audit

**Detections**

- Charges
- Formal Warnings for Cannabis
- Summons
- Taken into Consideration (TICs)
- Penalty Notice Disorders (PNDs)
- Simple Cautions
- Community Resolution

**Safeguarding**

- DASH (Domestic Abuse Risk Assessment Document)
- Harassment
- Rape Investigation Procedures
- Child Abuse Investigation Unit
- Missing Persons

**Ad-Hoc**

- Crime Recording Validation Processes
- Crime Mapping (Columbus)