CHIEF CONSTABLE OF NORTH YORKSHIRE

Digital Forensic Unit Quality Manual and ISO17025 Internal Audit Compliance

FINAL

Internal Audit Report: 14.16/17

27 April 2017

RSM

CONTENTS

Debrief held	28 March 2017	**Internal Audit team**	Dan Harris, Head of Internal Audit
Draft report issued	06 April 2017		Angela Ward, Senior Manager
			Philip Church, Client Manager
			David Morris, IT Audit Director
Responses received	26 April 2017		
Final report issued	27 April 2017	**Client sponsor**	Richard Cockerill, Digital Forensics Manager / ISO17025 Quality Manager
		Distribution	Richard Cockerill, Digital Forensics Manager / ISO17025 Quality Manager
			Amanda Oliver, Assistant Chief Constable

1 EXECUTIVE SUMMARY

1.1 Background

An audit of the Chief Constable of North Yorkshire ('the Force')'s Digital Forensic Unit Quality Manual and ISO 17025 Internal Audit Compliance was undertaken as part of the approved internal audit plan. The Force, as a forensic service provider, is required to comply and be accredited under ISO17025:2005 to deliver confidence in their results; and reduce the risk that those guilty of crime may escape justice or that innocent people may be convicted. The ISO 17025:2005 standard relates specifically to competency around carrying out laboratory testing and calibration, including sampling.

The Force has begun to undertake a series of internal audits to assess the effectiveness of the quality management system (QMS) and to ensure compliance of working practices with the Digital Forensic Unit (DFU) Quality Manual and the ISO 17025:2015 standards. The Force plans to become accredited with ISO17025 by United Kingdom Accreditation Service (UKAS) over the next 12 months and an initial accreditation assessment has been planned to take place during September 2017.

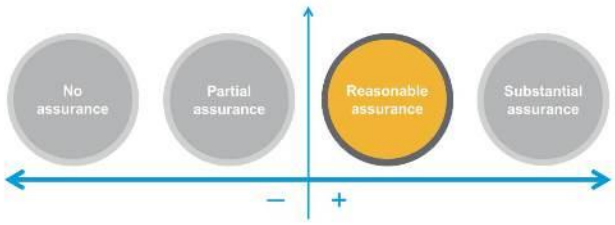
1.2 Conclusion

Our review has highlighted control enhancements required, mainly around the process of performing internal audits at the Force. Three **medium** and two **low** priority observations have been raised for consideration by the Force's management. A formal assurance opinion has been provided below.

Internal Audit Opinion:

Taking account of the issues identified, the Chief Constable of North Yorkshire can take reasonable assurance that the controls in place to manage the risks are suitably designed and consistently applied.

However, we have identified issues that need to be addressed in order to ensure that the control framework is effective in managing the identified risks.



1.3 Key findings

The key findings from this review are as follows and have resulted in three medium priority management actions being agreed:

- Section 3.4 of the NYP Digital Forensic Unit Quality Manual states that the scope of each audit will be discussed with the auditee; however, there is no requirement for the scope of the audit to be stated formally within a Terms of Reference. Without formal Terms of Reference being produced for each audit assignment, there is a risk that the agreed scope of work might not be delivered.

- There is no formal requirement detailed within the Quality Manual for auditors to test all, a set proportion, or a statistical sample of cases for review. There is a risk that sampling methods employed during audit testing are not transparent and repeatable.

- There is no formal approach for retaining all evidence reviewed during the course of an audit. There is a risk that audit conclusions cannot be verified or repeated in the absence of evidence which was used to reach findings and conclusions that were reported on.

We also discussed the following two low priority matters with management:

- Section 3.2 (Internal Auditor Competency) of the Quality Manual states that the Quality Log (DFU/REC/002) lists the qualifications of the audit team members. However, upon reviewing the Quality Log, we found no reference to auditors' qualifications as stated within the Quality Manual. Furthermore, we noted that the Audit Master Log gives fairly sparse information and could be usefully updated with further information. There is a risk that management do not have accurate information to allow them to assign appropriate staff to complete audit assignments.

- Upon completion of each audit assignment, a quality management review is performed to ensure compliance with the Quality Manual. However, the criteria for quality management reviews following audit assignments are not clearly stated. There is a risk that quality management reviews do not capture key criteria when assessing the adequacy and appropriateness of audit work carried out.

We noted the following area of good practice:

- Areas of non-conformance identified within audits are reported within formal Internal Audit reports and logged within a Non-conformance Master Log spreadsheet. The Master Log records a number of criteria including a description of the non-conformance, a risk category and root cause of the non-conformance, corrective actions taken and the dates on which the findings have been closed following remediation.

  We selected a sample of three 'closed' items out of a total of 25 identified within the Non-conformance Log; and independently confirmed that the corrective actions detailed within the log had been implemented appropriately. No issues were noted as part of our testing in this area.

1.4 Additional information to support our conclusion

Area	Control design*	Non-Compliance with controls*	Agreed actions		
			Low	Medium	High
Compliance with ISO17025:2015 requirements.	0 (3)	0 (3)	0	0	0
Compliance with the Force's Digital Forensic Unit Quality Manual.	3 (2)	1 (2)	2	2	0
Robustness of evidence retained by the Force.	1 (2)	0 (2)	0	1	0
Total			**2**	**3**	**0**

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

2 DETAILED FINDINGS

Categorisation of internal audit findings	
Priority	**Definition**
Low	There is scope for enhancing control or improving efficiency and quality.
Medium	Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible reputational damage, negative publicity in local or regional media.
High	Immediate management attention is necessary. This is a serious internal control or risk management issue that may lead to: Substantial losses, violation of corporate strategies, policies or values, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

This report has been prepared by exception. Therefore, we have included in this section, only those risks of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Actions for management
Objective: To ensure internal audits are undertaken to assess the effectiveness of the Force's quality management system and to ensure compliance of working practices with the Digital Forensic Unit Quality Manual and the ISO17025 standards.						
1	**Missing Control** Section 3.4 of the Force's Digital Forensic Unit Quality Manual states that the scope of each audit will be discussed with the auditee; however, there is no requirement for the scope of the audit to be documented formally within a Terms of Reference.	No	-	We noted that the Quality Manual is dated 8 December 2016 (issue date) and bears the approval of the Quality Manager. The review period is stated as annual and the last review is shown in the Issue Status & Amendment History as 8 December 2016. Formal Terms of Reference for audit assignments are useful in detailing the objectives, scope, limitations, resources and reporting timescales for performing each audit assignment. **Risk Exposure*** / **Root causes** Without formal Terms of Reference being produced for each audit assignment, there is a risk that the agreed scope of work might not be / The requirement to produce a formal Terms of Reference has not been defined within the Quality Manual.	Medium	Management will issue formal Terms of Reference prior to each audit assignment. The Terms of Reference will state the objective, scope, limitations, resources and reporting timescales. When internal audit reports are reviewed prior to formal issue, the scope of work covered will be compared to that stated in the Terms of Reference.

<table>
<tr><th>Ref</th><th>Control</th><th>Adequate control design (yes/no)</th><th>Controls complied with (yes/no)</th><th>Audit findings and implications</th><th>Priority</th><th>Actions for management</th></tr>
<tr><td></td><td></td><td></td><td></td><td>delivered.
<table><tr><th>Probability</th><th>Financial</th><th>Reputational</th><th>Operational</th><th>Legal</th><th>Rating</th></tr><tr><td>Probable</td><td>Negligible</td><td>Negligible</td><td>Minor</td><td>Negligible</td><td>5:4</td></tr></table>
* The rating of risk (probability, financial, reputation, operational, legal) has been undertaken by the area owner based on the Force's risk matrix.</td><td></td><td>Responsible Owner:
Digital Forensics Manager / ISO17025 Quality Manager

Implementation date:
May 2017</td></tr>
<tr><td>2</td><td><u>Missing Control</u>

There is no formal requirement detailed within the Quality Manual for auditors to test all, a set proportion, or a statistical sample of cases for review.</td><td>No</td><td>-</td><td>A large volume of cases may make it impractical to test all cases in a period under review, so sampling is justified as an approach, particularly if the sampling methodology is sound.

There are various sampling methodologies available to auditors, based on risk, judgement, volume etc. When selecting a sample for testing, it is important to document the sampling criteria used by the auditor so that testing is transparent and repeatable.

<table><tr><th colspan="3">Risk Exposure*</th><th colspan="3">Root causes</th></tr><tr><td colspan="3">There is a risk that sampling methods employed during audit testing are not transparent and repeatable.</td><td colspan="3">The requirement to record sampling criteria has not been defined within the Quality Manual.</td></tr><tr><th>Probability</th><th>Financial</th><th>Reputational</th><th>Operational</th><th>Legal</th><th>Rating</th></tr><tr><td>Probable</td><td>Negligible</td><td>Negligible</td><td>Minor</td><td>Negligible</td><td>5:4</td></tr></table></td><td>Medium</td><td>When selecting cases for audit testing, the approach taken will be documented in the working papers, and this requirement will be added to the Quality Manual. Auditors might usefully record the sampling method by these categories:

• Sample size;
• Sample source;
• Method of selection; and
• Period of selection.

In the case when sample testing is carried out due to large volumes and a statistical approach is used, it is useful to record the sampling method used (random, interval, judgment-based, etc.).

Responsible Owner:
Digital Forensics Manager / ISO17025 Quality Manager</td></tr>
</table>

<table>
<tr><th>Ref</th><th>Control</th><th>Adequate control design (yes/no)</th><th>Controls complied with (yes/no)</th><th>Audit findings and implications</th><th>Priority</th><th>Actions for management</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>Implementation date:
May 2017</td></tr>
<tr><td>3</td><td><u>Missing Control</u>

There is no formal approach for retaining all evidence reviewed during the course of an audit.</td><td>No</td><td>-</td><td>We reviewed a number of audit files from audits which have been completed over the last year. Whilst we noted that the audit team retains audit working papers and audit checklists on file, we confirmed with the Digital Forensics Manager that the Force does not currently have a formal approach for retaining evidence reviewed during the course of an audit.

<table>
<tr><th colspan="3">Risk Exposure*</th><th colspan="3">Root causes</th></tr>
<tr><td colspan="3">There is a risk that audit conclusions cannot be verified or repeated in the absence of evidence which was used to reach findings and conclusions that were reported on.</td><td colspan="3">There is no formal approach taken to retaining evidence reviewed during the course of audit assignments.</td></tr>
<tr><th>Probability</th><th>Financial</th><th>Reputational</th><th>Operational</th><th>Legal</th><th>Rating</th></tr>
<tr><td>Probable</td><td>Negligible</td><td>Negligible</td><td>Minor</td><td>Negligible</td><td>5:4</td></tr>
</table></td><td>Medium</td><td>Management will ensure that all evidence which is reviewed during audit assignments is retained on file for audit trail purposes.

Responsible Owner:
Digital Forensics Manager / ISO17025 Quality Manager

Implementation date:
May 2017</td></tr>
<tr><td>4</td><td>Within the content of the Quality manual, we noted that section 3.2 (Internal Auditor Competency) states that the Quality Log (DFU/REC/002) lists the qualifications of the audit team members.</td><td>Yes</td><td>No</td><td>Upon reviewing the Quality Log, we found no reference to auditors' qualifications was made as stated within the Quality Manual.

Management explained that the reference made to auditors' qualifications in the Quality Manual is outdated and should now refer to the Audit Master log (tab4).

However, we noted that the Audit Master Log gives fairly sparse information and could be usefully updated with a column to show details of qualifications and experience, including expiry of any qualifications if applicable, and CPE as applicable.

<table>
<tr><th>Risk Exposure*</th><th>Root causes</th></tr>
<tr><td>There is a risk that management do not have accurate information to allow them</td><td>The Audit Master Log is not updated regularly enough to</td></tr>
</table></td><td>Low</td><td>Management will ensure that internal auditors' qualifications and experience are updated with adequate information in the Audit Master log and subject to regular review.

The reference to the Quality Log (DFU/REC/002) in the Quality Manual will be updated to refer to the Audit Master log instead.

Responsible Owner:</td></tr>
</table>

<table>
<tr><th>Ref</th><th>Control</th><th>Adequate control design (yes/no)</th><th>Controls complied with (yes/no)</th><th>Audit findings and implications</th><th>Priority</th><th>Actions for management</th></tr>
<tr><td></td><td></td><td></td><td></td><td>to assign appropriate staff to complete audit assignments.
capture changes to auditors' qualifications and experience.
<table>
<tr><th>Probability</th><th>Financial</th><th>Reputational</th><th>Operational</th><th>Legal</th><th>Rating</th></tr>
<tr><td>Unlikely</td><td>Negligible</td><td>Negligible</td><td>Minor</td><td>Negligible</td><td>6:2</td></tr>
</table></td><td></td><td>Digital Forensics Manager / ISO17025 Quality Manager

Implementation date: May 2017</td></tr>
<tr><td>5</td><td><u>Missing Control</u>

The criteria for quality management reviews following audit assignments are not clearly stated.</td><td>No</td><td>-</td><td>We confirmed with management that, upon completion of each audit assignment, a quality management review is performed to ensure compliance with the Quality Manual.

However, the criteria for quality management reviews following audit assignments are not clearly stated. A checklist approach may be beneficial as shown in the example at Appendix C.
<table>
<tr><th colspan="3">Risk Exposure*</th><th colspan="3">Root causes</th></tr>
<tr><td colspan="3">There is a risk that quality management reviews do not capture key criteria when assessing the adequacy and appropriateness of audit work carried out.</td><td colspan="3">Criteria for performing quality management reviews following audit assignments have not been formally stated.</td></tr>
<tr><th>Probability</th><th>Financial</th><th>Reputational</th><th>Operational</th><th>Legal</th><th>Rating</th></tr>
<tr><td>Unlikely</td><td>Negligible</td><td>Negligible</td><td>Minor</td><td>Negligible</td><td>6:2</td></tr>
</table></td><td>Low</td><td>Management will implement a more structured approach to the QA of completed audits, ensuring that all audits meet departmental standards, conclusions are appropriately made from test results and all scope areas have been adequately covered. A checklist will be implemented to this effect.

Responsible Owner: Digital Forensics Manager / ISO17025 Quality Manager

Implementation date: May 2017</td></tr>
</table>

APPENDIX A: SCOPE

Scope of the review

Objective of the area under review
To ensure internal audits are undertaken to assess the effectiveness of the Force's quality management system and to ensure compliance of working practices with the Digital Forensic Unit Quality Manual and the ISO17025 standards.

When planning the audit, the following areas for consideration and limitations were agreed:

Areas for consideration:

1. Compliance with ISO17025:2015

We reviewed procedures to confirm that:

- An annual audit programme has been developed for ISO17025:2015 and it has been adhered to.
- The frequency of audits is appropriate based on the risk and complexity of the organisation.
- When areas of non-compliance are identified, they are reported, appropriate remedial action is put in place and actions are followed-up.

2. Compliance with the force's Digital Forensic Unit Quality Manual

- We reviewed compliance with the Force's Digital Forensic Unit Quality Manual – Internal Audit procedure.
- We confirmed that the Digital Forensic Unit Quality Manual – Internal Audit Procedure has been applied consistently in practice.

3. Robustness of evidence

- We reviewed the approach taken by the Force to obtain and record evidence in its own internal audits.
- We confirmed that the evidence obtained is sufficient for the purpose.
- We identified areas for improvement, where required.

Limitations to the scope of the audit assignment:

- We did not review or confirm compliance with all aspects of ISO17025:2005. Our audit focussed on the Force's own internal auditing processes only.
- We did not confirm that the Digital Forensic Unit Quality Manual is fit for purpose.
- Our review did not confirm whether the Force will receive accreditation for ISO17025:2005.
- We did not perform audits in accordance with ISO17025:2005, but confirmed a schedule of audits is in place and the application of the Force's Digital Forensic Unit Quality Manual was consistent.
- Our work does not provide absolute assurance that material errors, loss or fraud did not exist.

APPENDIX B: FURTHER INFORMATION

Person interviewed during the audit:

- Richard Cockerill, Digital Forensics Manager / ISO17025 Quality Manager

Documentation reviewed during the audit:

- Audit Master Log
- Non-conformance Master Log
- Internal Audit Schedule
- Internal Auditing Quality Manual
- Sample of internal audit reports, 2016/2017
- Sample of non-conforming work reports, 2016/2017
- Internal audit files for sample of completed audits
- Evidence to support non-conformance actions being closed

APPENDIX C: OTHER RELEVANT MATTERS

We have included the following Monitoring and Quality Sheet template as a guide only. This template should be modified accordingly to support the specific requirements of internal auditing activities performed at the Force.

North Yorkshire Police Internal Audit Service	Monitoring & Quality Sheet (MQS) template
Client:	**North Yorkshire Police**
Auditable area:	**Digital Forensic Unit Quality Manual and ISO17025 Internal Audit Compliance**

AUDITOR'S QUALITY CHECKLIST	Initials	Date
Terms of Reference		
Signed by Manager & Auditee		
Debrief Matters		
Debrief meeting held		
Responses completed		
System Notes		
If appropriate, system and controls documented		
Objectives, Processes & Controls		
Conclusions completed		
Referenced to system notes		
Referenced to test working papers		
References to debrief		
Audit Testing		
Test sheets fully completed		
Signed and dated by author		
Evidence retained on file		
All cross-referencing complete		

BUDGET MONITORING			
Days available:			
Week	**Units**	**Days**	

DATES	Target	Actual	Initials
Audit start date			
Fieldwork completed			
Debrief meeting			
File for review			
Draft report issued			
Responses received			
Final report issued			

MANAGER'S QUALITY REVIEW	Initials	Date
Management Review		
Review comments cleared		
Conclusions agreed		
Audit covers scope in TOR		
Testing strategy suitable		
Draft Report		
Draft report reviewed/proof read		
Conclusions consistent with results		
Appropriate recommendations made		
Recs. categorised appropriately		
Correct format used		
Checked for typos and errors		
Final Report		
Client responses reviewed		
Checked for typos and errors		
Appropriate conclusion given		

NARRATIVE: Significant variances to procedures

FOR FURTHER INFORMATION CONTACT

Dan Harris, Head of Internal Audit

Tel: 07792 948767

Daniel.Harris@rsmuk.com

Angela Ward, Senior Manager

Tel: 07966 091471

Angela.Ward@rsmuk.com

Philip Church, Client Manager

Tel: 07528 970082

Philip.Church@rsmuk.com