CHIEF CONSTABLE OF CLEVELAND

Data Quality (including elements of Data Security and MoPI)

FINAL

Internal Audit Report: 5.16/17

3 August 2016

RSM

CONTENTS

Debrief held	29 June 2016	**Internal Audit team**	Daniel Harris, Head of Internal Audit Sheila Pancholi, IT Audit Partner Angela Ward, Senior Manager Philip Church, Internal Audit Manager David Wayman, Principal IT Audit Consultant Tarandeep Tatla, IT Audit Consultant
Draft report issued	13 July 2016		
Responses received	3 August 2016		
Final report issued	3 August 2016	**Client sponsors**	Maria Hopper, Data Protection Manager
		Distribution	Kate Rowntree, Executive Staff Officer

1 EXECUTIVE SUMMARY

1.1 Background

We undertook a review of Data Quality, including Data Security and Management of Police Information (MoPI), at Cleveland Police ('the Force') during June 2016 as part of the internal audit plan for 2016/17.

The objective of the audit was to review the amalgamation and cleansing of duplicate records across the Force's systems through the use of 'Global Nominal and Golden Location Data sets'. In addition, we were asked to provide assurance over data governance elements of the Force's system, specifically:

- How data is input into the system;
- What checks are in place to ensure duplicate / inaccurate entries are minimised;
- How access to the system is controlled; and
- The robustness of audit log checks to ensure access to and actions on the system are appropriate.

We were also asked to include an opinion on whether the cleansed and improved data repository has delivered wider benefits to the Force above simply improved reliability and quality of data. As part of the review we therefore considered whether the Home Office funded Experian project has realised wider benefits to the Force in accordance with its original business case.

The Force use a crime management system called Niche Records Management System (Niche). One of main issues facing the Force is the number of duplicate records being stored within the Niche database, in particular details relating to nominals and addresses, as the Niche system is unable to effectively match new data with existing records held in the system. There are 1.8 million person records on Niche, however there are only approximately 600,000 residents in the Cleveland policing area.

The Force engaged with Experian Data Quality to allow them to de-duplicate and cleanse the data held within Niche to create higher quality Golden Nominal and Golden Location datasets. Experian use a system called Experian Pandora with Experian Jukebox to allow them to create higher quality datasets and remove data duplication, for example. The statistical analysis work at the commencement of the project confirmed that there were over 15,000 exact duplicate records, however the total number of duplicate records in the system were significantly higher as not all the data may have been captured by the call handlers at point of entry into the system. Furthermore, the Experian Pandora system will significantly reduce the number of possible duplicate records which are sent for manual review by members of staff.

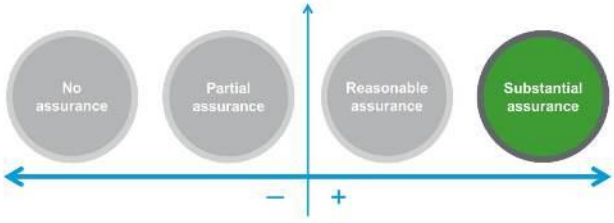
Once the Golden Nominal database was created, the Force worked with Experian to determine rules that could be applied to identify duplicates within the data. A daily data transfer from Niche into the Experian Pandora system is due to go live in July 2016 following a series of tests within a dedicated test environment. Experian have provided a dedicated project manager for this project.

1.2 Conclusion

From our review of Data Quality at the Force, **within the limitations set out at Appendix A**, we have highlighted one area that we consider poses a low risk to the control environment. We have also suggested remedial actions designed to assist management in improving the control framework in relation to the Data Quality Strategy.

Internal Audit Opinion:

Taking account of the issues identified, the Chief Constable of Cleveland can take **substantial assurance** that the controls upon which the organisation relies to manage the identified risks are suitably designed, consistently applied and operating effectively.



1.3 Key findings

The key findings from this review are as follows:

- In order to improve data input quality to the Golden Nominal database, the Force engaged with Experian to identify specific design requirements and models for the Golden Nominal database. From reviewing the Statement of Work (SOW) for the Golden Nominal project, we confirmed that Experian conducted a number of design workshops with the Force during September 2015 to identify high level designs and data models to be used by the Golden Nominal database. Furthermore, Experian provided design and user documentation to the Force for the Golden Nominal solution.

- Appropriate logical access controls have been applied to restrict access to key systems such as Niche and Pandora. We confirmed that there are two Administrators on Niche, the Niche System Administrator and the IT Business Analyst, who both require additional privileges for their roles. The Pandora system is still in development and testing is accessible to system Administrators only at this stage.

  User access into Niche is controlled via Cleveland Domain Active Directory management. We reviewed the password settings on the Cleveland Domain network and confirmed they provide adequate logical access controls. The password settings for the Pandora system are yet to be set.

- We confirmed through review of project documentation that Experian have worked with the Force to determine a number of rules to identify duplicate records within Niche. These rules can be set to automatically identify duplicate records and merge them into a single record; or flag possible duplicates for manual review by staff. It was agreed within the Experian Statement of Works (SOW) that no more than six rules will be created to ensure performance of the system is not impacted.

- The Home Office Grant Agreement for the project lists key deliverables. In discussion with the Project Lead and from review of the project evaluation (see below), we confirmed that the key deliverables have been realised. As part of the conditions of Home Office funding, the Force is required to report back to the Home Office and to publicise the results of the project among the Minerva Group (of Niche users). A presentation was given at the National Policing Conference (NPC) earlier this year sharing the principles and benefits of the Experian solution.

- A project evaluation is required by the Home Office to secure continued funding. The Home Office has stipulated the content (but not the format) of the report. The Force has responded with an Evaluation Report for stage one and will prepare and submit a stage two report following Pandora implementation. We obtained the Force's Evaluation Plan and confirmed that the content delivers all of the requirements stipulated within the Home Office Grant Agreement. The Home Office affirmed the content of the Plan and released stage two funds accordingly.

- We confirmed through review of published agendas and minutes that the Force has established a Gold Group to manage the implementation of the Experian solution and associated processes. The Gold Group comprises of senior staff from the Force, the Project Manager (Data Protection Manager) and an Account Manager from Steria. Gold Group meetings are formally scheduled and minutes are published on the project SharePoint site.

  We have agreed a formal management action in the following area:

- The Force has a Data Quality Strategy in place, which forms part of the overarching Information Management Strategy, under the ownership of the Force Senior Information Risk Owner (SIRO). We confirmed that the Information Management Strategy has been approved by the Information Security Board in April 2015; however it has not been reviewed since. There is a risk that the Data Quality Strategy does not reflect the current practises of the organisation and is misleading to staff that use the Strategy for guidance.

We have made a suggestion to management in the following area:

- The Force has been assessed by HMIC against the MoPI Code of Practice and an HMIC action plan has been put in place. Whilst the majority of points within the action plan had satisfactory responses, we queried the responses to points 254 (update of IM Strategy) and 255 ("By 30 November 2015, chief constables should carry out systematic audits in their forces to identify the extent to which locally adopted practices and procedures conform to the APP on information management."). The management response focused on data quality audits, but the recommendation appears wider than this, requiring internal audits of compliance against all of the MoPI APP (Authorised Professional Practice).

  Point 254: The Data Protection Manager confirmed that the IM Strategy has not been updated yet; as a meeting to discuss this with the author of the Strategy, Superintendent Simpson, had to be cancelled. A further date has not yet been set.

  Point 255: There is no internal auditing as yet, however the Data Protection Manager confirmed that once MoPI is embedded, the Force will ensure an audit plan is produced.

  We can therefore record that these items are in progress and that the Force has put measures in place to work towards compliance. Accordingly, as soon as is practical, the Force should ensure that an audit process and plan are in place to monitor internal processes and procedures against MoPI requirements.

1.4 Additional information to support our conclusion

Risk	Control design	Non-compliance with controls	Agreed actions		
			Low	Medium	High
Failure to adhere to the Code of Practice on the Management of Police Information.	0	1*	0	0	0
Data quality controls over data input to Global Nominal & Golden Location Data sets are not robust.	0	0	0	0	0
Business data output is not robust enough for reliable use.	0	1	1	0	0
Failure to realise Experian project benefits.	0	0	0	0	0
Total	**0**	**2**	**1**	**0**	**0**

*We have made a suggestion to management in this area, rather than raising a formal management action. This management action has therefore not been classified as High, Medium or Low.

2 ACTION PLAN

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.

The table below sets out the actions agreed by management to address the findings:

Ref	Findings summary	Priority	Actions for management	Implementation date	Responsible owner
1	We confirmed that the Information Management Strategy has been approved by the Information Security Board in April 2015; however it has not been reviewed since.	Low	Management will ensure that the Information Management Strategy is reviewed and updated; and subsequently subjected to annual review.	September 2016	Data Protection Manager
2	The Force has been assessed by HMIC against the MoPI Code of Practice and an HMIC action plan has been put in place.	Suggestion	We understand that compliance with MoPI is a work in progress and that the Force has put measures in place to work towards compliance. Accordingly, as soon as is practical, the Force should ensure that an audit process and plan are in place to monitor internal processes and procedures against MoPI requirements.	This is a longer term piece of work, and it can't be done until all the boxes in RESTORE are reviewed. This will be kept under review.	Data Protection Manager

3 DETAILED FINDINGS

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
1	The Force has a Data Quality Strategy in place, which forms part of the overarching Force Information Management Strategy, under the ownership of the Force Senior Information Risk Owner (SIRO).	Yes	No	A review of the Data Quality Strategy confirmed that it references a Data Quality Manager with the responsibility for the development and co-ordination of plans and activity to deliver the strategy. However, discussions with the Data Protection Manager confirmed that this is actually the responsibility of the Data Quality Co-ordinator for Cleveland Police. A Data Quality Manager role does not exist. We confirmed that the Data Protection Manager is planning to schedule a review of the Information Management Strategy with the author of the strategy, Superintendent Simpson. However, a date has not yet been set. There is a risk that the Data Quality Strategy does not reflect the current practises of the organisation and is misleading to staff that use the strategy for guidance.	Low	Management will ensure that the Information Management Strategy is reviewed and updated; and subsequently subjected to annual review.
2	The Force has been assessed by HMIC against the MoPI Code of Practice and an HMIC action plan has been put in place.	Yes	No	Items 254, 255, 256, 257, 258 and 259 were action points for action by the Data Protection Manager. Whilst the majority of points had satisfactory responses, we queried the responses to points 254 (update of IM Strategy) and 255 ("By 30 November 2015, chief constables should carry out systematic audits in their forces to identify the extent to which locally-adopted practices and procedures conform to the APP on information management.") with the Data Protection Manager. The management response focused on data quality audits, but the recommendation appears wider than this, requiring internal audits of compliance against all of the MoPI APP (Authorised Professional Practice).	Suggestion	We understand that compliance with MoPI is a work in progress and that the Force has put measures in place to work towards compliance. Accordingly, as soon as is practical, the Force should ensure that an audit process and plan are in place to monitor internal processes and procedures against MoPI requirements.

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Actions for management
				Point 254: The Data Protection Manager confirmed that the IM Strategy has not been updated yet; as a meeting to discuss this with the author of the Strategy, Superintendent Simpson, had to be cancelled. A further date has not yet been set. Point 255: There is no internal auditing as yet, however the Data Protection Manager confirmed that once MoPI is embedded, the Force will ensure an Audit plan is produced. We can therefore record that these items are in progress.		

APPENDIX A: SCOPE

Scope of the review

The scope was planned to provide assurance on the controls and mitigations in place relating to the following risks:

Objective of the area under review	Risks relevant to the scope of the review	Risk source
To review the amalgamation and cleansing of duplicate records across the Force's systems through the use of 'Global Nominal & Golden Location Data sets'. In addition, we will provide assurance over the data governance elements – how is data input into the system, what checks are in place to ensure duplicate/inaccurate entries are minimised, access to the system and any audit log checks to ensure access to and actions on the system are appropriate. The Force has a duty to obtain and use a wide variety of information (including personal information), in order to discharge their responsibilities effectively. We will provide assurance the Force adheres to the Code of Practice on the Management of Police Information.	• Failure to adhere to the Code of Practice on the Management of Police Information. • Data quality controls over data input to Global Nominal & Golden Location Data sets are not robust. • Business data output is not robust enough for reliable use. • Failure to realise Experian project benefits.	Annual Audit Plan

Additional management concerns:

As discussed with management we included an opinion on whether the cleansed and improved data repository has delivered wider benefits to Cleveland Police Force above simply improved reliability and quality of data. As part of the review we therefore considered whether the Home Office funded Experian project has realised wider benefits to the Force in accordance with its original business case.

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

Areas for consideration:

- Data quality standards and procedures, including:
  - Data input controls.
  - Accessibility of data.
  - Usefulness and reliability of business information tools;
- Logical access controls;
- Progress and scores assigned for MoPI deliverables;
- Evidence supporting areas/actions categorised as implemented; and
- Adherence to Code of Practice on MoPI.

Limitations to the scope of the audit assignment:

- The review was limited to identifying the existence of controls in the areas for review, and obtaining supporting documentation.
- Testing was carried out on a sample basis and assessed the framework that was in place but did not provide assurance that all aspects of the policy and guidance are being complied with by all staff.
- Conclusions were based on our assessments made through discussions with management, assessment of the current framework of controls and an initial review of relevant documentation available, either internally or externally generated.
- This review of MOPI compliance only covered those areas identified and scored as being implemented by the Force and submitted within the Force Action Plan. Our review was limited to a review of the file of evidence and did not test actual controls at operational level.
- Our review of project delivery was limited to review of key project deliverables; we are unable to provide absolute assurance that the project will deliver all expected benefits.
- Where applicable recommendations were based on the findings of samples selected for review, therefore our work does not provide any guarantee against material errors, loss or fraud or provide an absolute assurance that material error, loss or fraud does not exist.

APPENDIX B: FURTHER INFORMATION

Persons interviewed during the audit:

- Maria Hopper, Data Protection Manager
- Kieran O'Rourke, Data Co-ordinator

Documentation reviewed during the audit:

- Information Management Strategy
- Data Quality Strategy
- HMIC Action Plan May 2016
- Management of Police Information HMIC Report
- Experian Statement of Work
- Experian Workflow diagram
- Niche password settings
- Data Quality reports list
- Information Security Board meeting minutes
- Home Office Grant Agreement

.

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