CHIEF CONSTABLE OF NORTH YORKSHIRE

Data Quality (including Governance)

FINAL

Internal Audit Report: 6.16/17

18 November 2016

RSM

CONTENTS

Debrief held	15 September 2016	**Internal Audit team**	Dan Harris, Head of Internal Audit Angela Ward, Senior Manager Philip Church, Client Manager Adam Nabulsi, Senior Auditor
Draft report issued	30 September 2016		
Revised draft issued	8 November 2016		
Responses received	17 November 2016		
Final report issued	18 November 2016	**Client sponsor**	Paul Kennedy, Acting Deputy Chief Constable Sarah Wintringham, Head of Information Management
		Distribution	Paul Kennedy, Acting Deputy Chief Constable Sarah Wintringham, Head of Information Management

1 EXECUTIVE SUMMARY

1.1 Background

We carried out an audit of Data Quality as part of the agreed internal audit plan for 2016/17. As part of this audit, we reviewed how the Force ensures the integrity, accuracy and reliability of records within the Niche system.

The Force use the Niche system which is their main operational recording system. Storm is the command and control system which feeds into the Niche system. Niche is updated with information received from the public, officers or other forces and third parties. Information received can include:

- Lost and found property
- Exhibits
- Case information
- Custody information
- Intelligence
- Crime recording
- General incidents

The Records Management Team have responsibility for identifying any data entry errors on the Niche system which can arise during the data entry process and they also make arrangements to have these corrected. The Records Management Team is led by a Records Manager and part of this remit is responsibility for two Data Quality Assistants and the Crime and Incident Registrar function, all under the responsibility of the Head of Information Management.

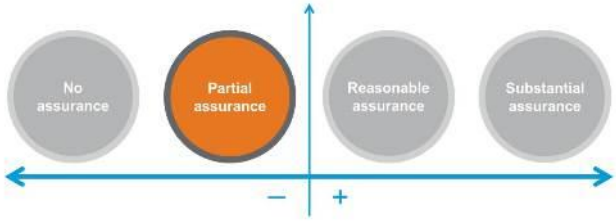
The Force is currently part of the Minerva initiative that looks to improve Niche and promote consistency of standards across the 21 other forces that have adopted it and signed up to Minerva. This is an ongoing initiative that will result in changes being made to Niche that are in accordance with the agreed standards and requests made by all the involved forces, promoting consistency in data quality.

1.2 Conclusion

We were satisfied from some of the testing undertaken and discussions with key staff that a robust data quality framework is in place, and many of the key controls we would expect to be in place for data quality are in place. However, testing did identify that there are some areas of concern that require the Force's attention and remedial action, such as the existence of blank records on Niche, duplicate records and data entry errors not being corrected in a timely manner, no standardised process being in place to identify repeat data entry error offenders, and Niche initial training not always being provided to new starters amongst other areas.

Internal Audit Opinion:
Taking account of the issues identified, the Chief Constable of North Yorkshire can take **partial assurance** that the controls to manage this risk are suitably designed and consistently applied.

Action is needed to strengthen the control framework to manage the identified risk.



1.3 Key findings

We identified the following areas of concern that require the Force's attention and remedial action that have led to the partial assurance opinion. We have therefore agreed **one 'high', two 'medium'** and **one 'low'** priority management actions in relation to the following findings:

- From the sample testing undertaken, we identified that duplicate records/data entry errors were not always being merged/corrected in a timely manner by the business area. Blank records were not being deleted by ICT in a timely manner. We also found that it could not always be established whether data entry errors had been corrected for certain error reports due to the way the audit trail functionality on Niche was configured. In addition, uncorrected errors flagged within some error reports were not being carried forward to the next financial year, resulting in them not being captured by the formal monitoring process, although a date filter is available so the user can select the dates required. There is therefore an increased risk of Niche records not being accurate and reliable. Consequently, this is a serious internal control issue that may lead to reputational damage, have an adverse impact on the Force's ability to deliver services and meet its targets and have an adverse regulatory impact leading to potential fines. **(High)**
- A formal process was not in place across business areas for monitoring and identifying staff members that made repeated data entry errors and a process in place to address this. There is therefore an increased risk of staff members making repeatedly the same data entry errors which has resource implications as more time will be spent conducting error reporting than is necessary. Consequently, this is a missing control that may result in loss of resource and have an adverse impact on the Force's ability to deliver services and meet its targets. **(Medium)**
- From the sample testing undertaken, we identified that new starters did not always receive the Niche initial training, increasing the risk of data entry errors arising. In addition, the centralised training records did not capture the specialist Niche training delivered in-house by business areas, which increased the risk of new starters not receiving the required specialist Niche training. Consequently, this is both an internal control issue and design weakness in control that may lead to more data entry errors being made which will have resource implications and may have an adverse impact on the Force's ability to deliver services and meet its targets. **(Medium)**
- The Terms of Reference for the Operational Delivery Board were generic in nature without detailing their obligations and areas of potential discussion.

We did however find that a number of the controls upon which the Chief Constable of North Yorkshire relies to manage the area are suitably designed, consistently applied and are operating effectively. These were established following discussions held with key staff and in conjunction with sample testing. These controls included:

- Documented guidance notes are in place on how to use the Niche system and are accessible to staff on the intranet. A Records Management Policy and Data Quality Procedure are also in place and detail the regulatory requirements around data quality, the principles around data quality, monitoring process, duplicate records, error reporting, and responsibilities amongst other areas. These are reviewed every three years (now due for a review), but if there were significant changes required they would be updated sooner.
- If there is no record of the individual, a record will be created for them with an attempt made to populate it with at least the first name, surname, date of birth and one other unique piece of information such as address, telephone number or email in order to avoid duplication of records (this is known as 3+1), as when any subsequent information is received on that individual, the data inputter requires as much unique identifiable information as possible to be able to establish whether that individual already has a record or not. This requirement is communicated by the Records Management Team, through business areas and within Niche training sessions.
- Desktops and laptops issued by the Force have the software which is encrypted and password protected and no other electronic devices can access the system which was established through discussions with ICT.

- Access to the Niche system is restricted to only authorised members of staff and the level of access is restricted according to the permissions assigned which vary across job role and business area. This was confirmed upon sample testing of 12 staff with Niche access. There is general functionality within the system that all data inputters require, however each business area may have additional bespoke elements to the system according to their requirements.
- Administration of access rights to the Niche system is delegated to the Niche System Administration Team. They are notified of new starters, leavers and changes in staff rank and department and also run weekly reports to identify these as well. There are 95 different access level profiles currently on the system which can be allocated to staff, but the Niche System Administration Team are in the process of reducing these as some are no longer required.
- For new starters they know the level of access to provide on Niche by looking at their job role, rank and department. If this is not conclusive, they will enquire with their line manager to establish the level of access required. Leavers have their access rights removed from the system. For changes in staff rank and department, the required amendment to access rights will be processed on the system. This was confirmed upon sample testing of four new starters, four leavers and four amendments to staff rank or department.
- The Force use SSRS (SQL Server Reporting Services) which is a reporting tool that extracts information from Niche and populates it into reports according to stipulated criteria. It is a flexible and useful business information tool that is used for statistical analysis and producing management information for various committees. Review of a sample of six SSRS reports confirmed this. The Performance Team produce most of these reports, but there are also specialist users that have the access rights within SSRS to produce reports as well. Access rights are administered by ICT, who review the requests and only process this if the staff member already has access to Niche. Access rights for leavers are dealt with automatically by the system, as it links into Niche and mirrors any leavers processed on that system. Review of the SSRS access rights confirmed only appropriate members of staff had access.
- The Intelligence Analysts use I2 which extracts data from Niche and presents it in a visual format, and allows other data sources to be imported as well. The Intelligence Analyst Team only had access to this system which we confirmed upon review of the system access rights. The Head of Intelligence Analysis and Research reviews and approves any requests for access, and archives approval in at least an email. For leavers, it is an item on the Leaver Checklist for any access rights to be removed, which we confirmed upon review of a Leaver Checklist.
- The Records Management Team run a number of reports from SSRS on both an ongoing and monthly basis to identify data entry errors such as duplicate records, missing fields, incorrect use of fields, etc. An Error Reporting Schedule is in place that details the error reports that will be run over the reporting period. They will then correct any data entry errors flagged by the reports themselves or notify the single point of contact (SPoC) for the relevant business area and request that they correct the data. The SPoCs are emailed a link to the report that lists all data entry errors under their business area. We confirmed this process through sample testing of 40 data entry errors selected from various error reports run by the Records Management Team.
- Any data entered onto the Niche system that subsequently requires amending must be raised by the original data inputter within an hour from entering the data to make any amendments, after which the data becomes locked down and can then only be amended by the Niche System Administration Team. A request is submitted to the team via telephone or email informing them of the amendment required which will be considered and processed.
- The Force Crime and Incident Registrar conducts periodic compliance audits on a number of different areas which identify data entry errors amongst other things. There is an Audit Schedule listing the scheduled audits for the year which is influenced by high risk areas, business need and the Operational Delivery Board. All the audits have an element of data quality to them and are based on the documented guidance issued by the Home Office called the Data Quality Assurance Manual, which provides guidance to forces on what tests should be carried out. As part of the audits, sample testing is undertaken as per the guidelines.

The results of sample testing are formally recorded and a report produced summarising the findings along with any recommendations and the responsible owner for implementing them. We confirmed this process through sample testing of three audits selected from the Audit Schedule for 2016/17.

- The Operational Delivery Board and Niche User Group meet on a periodic basis (monthly and quarterly respectively) to discuss information management and data quality amongst other areas of discussion. The Records Manager attends the Operational Delivery Board and Niche User Group meetings.
- Reports are produced on a periodic basis that detail recommendations to improve the data quality process and are presented to the Operational Delivery Board or other relevant committee according to the nature of the report and error for review and discussion.
- The Chair of the Niche User Group was appointed as the Niche Operational Lead, and has produced a report on how they utilise Niche compared to other forces along with the progress they have made since adoption and any issues or improvements required, resulting in a number of recommendations. This report will be reviewed by the Board on 9th September 2016 who will consider the recommendations to be implemented.

1.4 Additional information to support our conclusion

Risk	Control design*	Compliance with controls*	Agreed actions		
			Low	Medium	High
To review the integrity, accuracy and reliability of records across the Force's systems	0 (13)	4 (13)	1	2	1
Total			**1**	**2**	**1**

* 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
Risk: To review the integrity, accuracy and reliability of records across the Force's systems.						
1	An Error Reporting Schedule is in place that details the error reports that will be run over the reporting period. The Records Management Team will then correct any data entry errors flagged by the reports themselves or notify the SPoC	Yes	No	We confirmed the Records Management Team had an Error Reporting Schedule in place for the running of various error reports to identify different types of data entry errors across the Force. For a sample of 40 data entry errors (20 duplicate records and 20 other data entry errors) selected across these various reports, our testing identified the following exceptions: **Duplicate records** Out of the 20 duplicate records sampled across various business areas, testing established that: • In three cases, the duplicate records were not merged despite being identified in February and April 2016. These were under the remit of the	High	Identified duplicate records/data entry errors will be merged/corrected in a timely manner by the business area. If the Records Management Team identify that duplicate records/data entry errors have not been merged/corrected in a timely manner, this will be escalated to an appropriate chain of management.

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Actions for management
	for the relevant business area and request that they correct the data. The SPoCs are emailed a link to the report that lists all data entry errors under their business area.			Prosecution Team. • In one case the duplicate record was merged, but this was not done in a timely manner (five months after being identified). This was under the remit of the Harrogate Team. If duplicate records are not merged in a timely manner, there is a risk that subsequent information and intelligence relating to an individual, property, vehicle or telephone number will not be assigned to one correct consolidated record, leading to the information and intelligence not being captured as part of that record. Whilst the sample testing on duplicate records was being undertaken, we came across a blank record on the Niche system that had the same name as the person in our sample, however, this record had a different ID number which was an indication that it had not been identified within the error reporting process and merged into one record. Discussions with the Records Management Team clarified that the error reporting did not flag records that were blank, as it could only flag duplicate records where the 3+1 information was obtained (i.e. their name, date of birth and one other unique piece of information such as address, telephone number or email). However, a report to identify records for deletion has been run for ICT to bulk delete and then ICT are to periodically run reports to identify these blank records and delete them from the system. We established at the time of audit that this blank record was created on 27 June 2016, therefore concluded that the reporting conducted by ICT was not periodic enough. If blank records are not identified and deleted in a timely manner, there is a risk that subsequent information and intelligence relating to an individual, property, vehicle or telephone number will not be assigned to one correct consolidated record, leading to the information and intelligence not being captured as part of that record.		This requirement will be communicated to all business areas and SPoCs. ICT will run reports on a monthly basis to identify blank records and delete these where it is found that the record does not link to anything else on the Niche system. The audit trail functionality on SSRS will be reconfigured to look further back than the current two month restriction (e.g. the previous 12 months) for the error reports where this functionality is the only way to determine whether previously flagged errors have been corrected, such as Crime Report 20 and 59. The Records Management Team will, in consultation with other relevant parties, investigate whether all error reports that are configured to flag data entry errors from the beginning of the financial year can be reconfigured to flag uncorrected data entry errors from previous financial years as well.

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Actions for management
				Data entry errors Out of the 20 data entry errors sampled across various business areas, testing established that: • In five cases, the data entry errors were not corrected on the Niche system despite one of these being identified in January 2016. These were under the remit of the Crime Recording and Occurrence Management Team. • In four cases, we were unable to establish whether the data entry errors were corrected as the audit trail functionality on the Niche system for the specific reports that identified the errors only covered the previous two months. If data entry errors are not corrected in a timely manner, there is a risk that records on the Niche system will not be accurate and reliable. If the audit trail functionality on the Niche system is configured to only look back over the previous two months and nothing older than this, there is a risk that the Records Management Team or other appropriate members of staff will not be able establish whether the data entry errors have been corrected for the error reports where this functionality is the only way to determine this, resulting in records on the Niche system not being accurate and reliable. Whilst the sample testing on data entry errors was being undertaken, it was apparent that some of the error reports produced (such as Crime Report 20 and 59) only flagged errors from the beginning of the financial year, which meant that any uncorrected errors flagged from the previous financial year were not being carried forward, resulting in them not being captured by the formal monitoring process, however the reports have a User defined filter available so that the User can run the report from the last time it was run. There was therefore a risk that previously identified data entry errors were not being corrected, resulting in records on the Niche system not being accurate and reliable.		Responsible Officer: Sarah Wintringham, Head of Information Management Joanne Edgar, Records Manager Implementation Date: 31st March 2017

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Actions for management
				Risk Exposure*		
				If Error Reporting procedures are not operating effectively, there is an increased risk of Niche records not being accurate and reliable.		
				Root causes		
				Design weakness in control and non-compliance with controls in place by some business areas.		

Probability	Financial	Reputational	Operational	Legal	Rating
Probable	Minor	Significant	Significant	Significant	3:13

* The rating of risk (probability, financial, reputation, operational, legal) has been undertaken by the area owner based on the Force's risk matrix.

2	A formal process is in place across business areas for the monitoring of staff members that repeatedly make the same data entry errors and to feed this back to them so that the same errors are not repeated. The Records Management Team monitor repeat offenders who create duplicate records and inform the SPoCs of this for them to feed back to their staff. The SPoCs also have	Yes	No	Discussions with the Records Management Team in conjunction with a review of supporting evidence confirmed that they monitored repeat offenders who created duplicate records and would inform the SPoCs of this for them to feed back to their staff. We clarified that it was the responsibility of the SPoCs to do this, so they had no further obligation to follow this up. A sample of four SPoCs were interviewed for the following business areas: • Custody • Crime Recording • Intelligence • Business Administration Discussions with the four SPoCs established that, with the exception of the Intelligence business area, there was no formal process in place for monitoring and identifying staff members that made repeated data entry errors and a process in place to address this. The detailed findings for each business area sampled are as follows: **Intelligence** On a monthly basis, the SPoC feeds back all data entry errors flagged by the error reports to her staff via email. It was clarified that this also fed into their	Medium	Each business area will have a formal process in place for monitoring and identifying staff members that make repeated data entry errors and a process in place to address this e.g. informing them of the error and any corrective actions required. Responsible Officer: Sarah Wintringham, Head of Information Management Joanne Edgar, Records Manager Head of Custody Suites SPoC for Custody, Crime Recording and Business Administration

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Actions for management
	their own local process for monitoring and addressing repeat data entry error offenders.			performance reviews. We confirmed for a sample of two error reports (May 2016 Report 3 and August 2016 Report 13), in both cases the errors flagged by the reports were emailed to the offending staff with feedback. **Custody** Discussions with a representative from Criminal Justice established that the data entry errors flagged by error reports under the Custody business area were issued to individual Custody Suites for correction rather than the SPoC, therefore the Heads of those Custody Suites were responsible for monitoring repeat data entry error offenders and feeding back to their staff and not him. However, we clarified that on a daily basis he had his own daily checks for monitoring compliance with daily business which also allowed for incorrect data entries to be highlighted and rectified. **Crime Recording** Discussions with the SPoC established that she received the error reports from the Records Management Team and would arrange for them to be corrected by her staff. We clarified that although she had advised her staff to monitor for repeat data entry error offenders and to flag any to her (this had happened a few times), this was not a formal process due to resource restrictions associated with the current structure of the unit. **Business Administration** Discussions with the SPoC established that they received the error reports from the Records Management Team and would correct the data, however they did not have a formal process in place for monitoring repeat data entry error offenders at the time of audit.		Implementation Date: 31st March 2017

Risk Exposure*	Root causes
If a formal process is not in place for monitoring and identifying staff members that make repeated data entry errors and a process in place to address	No standardisation of controls across business areas in relation to this issue.

<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>this, there is a risk that they will continue to make the same data entry errors which has resource implications as more time will be spent conducting error reporting than is necessary.
<table><tr><th>Probability</th><th>Financial</th><th>Reputational</th><th>Operational</th><th>Legal</th><th>Rating</th></tr><tr><td>Highly probable</td><td>Negligible</td><td>Minor</td><td>Significant</td><td>Negligible</td><td>2:14</td></tr></table></td><td></td><td></td></tr>
<tr><td>3</td><td>All new starters are required to have Niche initial training which is run on a monthly basis.

They are booked onto the training by their manager, and once attended this will be recorded on an attendance register and sent to the Training Team where their training records will be updated.

Specialist Niche training is also provided where the new starter will be using more bespoke functionality within</td><td>Yes</td><td>No</td><td>For a sample of 10 new starters since January 2016, testing established that:
In five cases the new starters received the Niche initial training. In the remaining five cases, the new starters did not receive the Niche initial training as the Prosecution and Witness Care business area was not aware that these training sessions were still being delivered. The line manager for the business area clarified that the new starters still received in-house training regardless.
In four cases the new starters received specialist Niche training which we confirmed upon review of the training records. In the remaining six cases, we were informed by the two business areas (Prosecution and Witness Care and Intelligence) that the specialist Niche training was delivered in-house, which wasn’t recorded anywhere therefore we had to rely on the discussions held.
<table><tr><th>Risk Exposure*</th><th>Root causes</th></tr><tr><td>If all new starters do not receive the Niche initial training, there is an increased risk of data entry errors arising.

In addition, if a centralised record of all training received by staff members is</td><td>Due to the various changes that have taken place around Niche usage and training provision at the Force over the past few years, certain business areas are not clear what the current Niche</td></tr></table></td><td>Medium</td><td>All business areas will be reminded of the Niche initial training that is being delivered and the frequency of this along with the requirement that all new starters must attend these sessions.

The Force will explore if the centralised training records maintained by the Training Team can capture any specialist Niche training delivered in-house by some business areas, which can include the requirement for business areas to notify them of any new starters that have received in-house specialist Niche training.

Responsible Officer:
Claire Bean, Training Manager

Line manager for Prosecution</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>Niche as part of their business area.

The delivery of specialist Niche training differs by business area, but is most commonly through Force led sessions, in-house business area training or on-the-job training.</td><td></td><td></td><td>not being maintained (including for specialist Niche training delivered in-house), there is an increased risk that new starters will not receive the required specialist Niche training leading to data entry errors arising.
training framework is.

<table><tr><th>Probability</th><th>Financial</th><th>Reputational</th><th>Operational</th><th>Legal</th><th>Rating</th></tr><tr><td>Highly probable</td><td>Minor</td><td>Minor</td><td>Significant</td><td>Negligible</td><td>2:14</td></tr></table></td><td></td><td>and Witness Care

Implementation Date:
31st December 2016</td></tr>
<tr><td>4</td><td>The Operational Delivery Board and Niche User Group both have Terms of Reference in place outlining their role in maintaining data quality standards across the Force.</td><td>Yes</td><td>No</td><td>The Terms of Reference for the Operational Delivery Board and Niche User Group were obtained, and review established that although the membership for the Operational Delivery Board included the Records Manager, the Terms of Reference were very generic in nature making reference to brief agenda items without detailing the Board’s obligations and areas of potential discussion.

The Terms of Reference for the Niche User Group adequately detailed their role in maintaining data quality standards across the Force, and included the Head of Information Management on its membership.

<table><tr><th>Risk Exposure*</th><th>Root causes</th></tr><tr><td>If the Terms of Reference for the Operational Delivery Board are generic in nature without detailing their obligations and areas of potential discussion, there is a risk that the Force will be unable to determine whether the Board are effectively meeting their</td><td>When the Terms of Reference template was changed, an exercise was not undertaken to ensure that all committees’ Terms of Reference were updated with the new template.</td></tr></table></td><td>Low</td><td>Recommend to the Chair of the Operational Delivery Board for the Terms of Reference to be updated detailing their obligations and areas of potential discussion within their meetings.

Responsible Officer:
Sarah Wintringham, Head of Information Management

Implementation Date:
31st January 2017</td></tr>
</table>

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Actions for management
				obligations making it difficult to assess performance.		

Probability	Financial	Reputational	Operational	Legal	Rating
Probable	Minor	Minor	Minor	Negligible	5:8

APPENDIX A: SCOPE

Scope of the review

To evaluate the adequacy of risk management and control within the system and the extent to which controls have been applied, with a view to providing an opinion. The scope was planned to provide assurance on the controls and mitigations in place relating to the following risks:

Objective of the risk under review	Risks relevant to the scope of the review	Risk source
To review the integrity, accuracy and reliability of records across the Force's systems.	To review the integrity, accuracy and reliability of records across the Force's systems.	ARM - 6748

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

Areas for consideration:

The Operations Board has responsibility for data quality and we considered the role of the Board and provided assurance that it met the intended purpose and was appropriate to ensure accurate, relevant and purposeful data was being scrutinised and duplication minimised. Our review considered:

- Data quality standards and procedures, including:
  - Data input controls;
  - Accessibility of data; and
  - Usefulness and reliability of business information tools.
- Review of how data input errors were identified and reported to area leads. We considered how non-compliance was addressed and monitored.
- Appropriate training had been provided to staff to ensure data input was accurate.
- Review of how data input errors were corrected including the use of matching rules and isolated incidents. Our testing confirmed whether data input errors had been resolved in a timely manner.
- A review of the Operations Board and Niche User Group's role to maintain data quality standards, including:
  - Appropriate Terms of Reference were in place.
  - Meetings were held at regular intervals and attended by appropriate staff across the Force.
  - Actions plans had been developed to improve the Force's data quality standards.

Limitations to the scope of the audit assignment:

- Testing was performed on a sample basis, therefore we have not provided assurance on the accuracy of all data.
- We have not provided an opinion of the suitability of data used in management information.
- We have only provided assurance on the controls in operation at the time of the audit.
- We have not reviewed or provided an opinion on the matching rules in place.
- Our work does not provide absolute assurance that material errors, loss or fraud do not exist.

APPENDIX B: FURTHER INFORMATION

Persons interviewed during the audit:

- Sarah Wintringham, Head of Information Management
- Joanne Edgar, Records Manager
- Abbie White, Data Quality Assistant
- Tony Briggs, Data Quality Assistant
- Elizabeth Berriman, Niche Systems Administrator
- Jennifer Found, Temporary Niche Systems Administrator
- Lindsey Stamp, Chief Inspector
- Trish Hope, Chair of the Niche User Group
- Tracey Arnell, Senior Applications Support Engineer
- Steve Murray, Corporate Performance Manager
- Vicki Hough, Head of Intelligence Analysis and Research
- Mark Richardson, Training Manager
- Tricia Ansbro, Force Crime and Incident Registrar
- Lesley Blakey, Single Point of Contact for Intelligence
- Bob Thomson, Single Point of Contact for Custody
- Louise Coxon, Single Point of Contact for Crime Recording
- Shona Leys, Single Point of Contact for Business Administration
- Jayne Tooke, Line Manager for Criminal Justice Department

Documentation reviewed during the audit:

- Records Management Policy
- Data Quality Procedure
- Niche guidance notes
- Niche system reports
- SSRS system reports
- Niche system access rights
- SSRS system access rights
- I2 system access rights
- Error Reporting Schedule
- Error Reports

- SPoC correspondence
- Audit Schedule
- Audit reports and results
- Niche training programme
- Niche training material
- Niche training records and documentation
- Terms of Reference for the Operational Delivery Board
- Terms of Reference for the Niche User Group
- Operational Delivery Board minutes
- Niche User Group meeting minutes
- Report produced by the Chair of the Niche User Group

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