

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | **Internal Audit** |  |
|  |  | **FINAL** |  |
|  |  |  |  |  |
|  | **The Police and Crime Commissioner for Cleveland**  **and the Chief Constable Cleveland Police** |  |  |  |
|  | **Assurance Review of Governance – Data Quality/**  **Information Governance** |  |  |  |
|  | **2019/20** |  |  |  |
|  |  |  |  |  |

|  |
| --- |
| **Executive Summary** |

|  |  |  |
| --- | --- | --- |
| **OVERALL ASSURANCE ASSESSMENT** |  | **OVERALL CONCLUSION** |
|  |  | |  |  | | --- | --- | | **Data Quality and Information Governance is well understood by the Head of Information Governance and Data Protection Officer.** | | |  | **The main system for managing data - Niche - has been used by the Force for some time and cleansing has been undertaken to improve data quality.** | |  | **At a corporate level and due no doubt to staff changes improvements need to be made at the Information Asset Board and Information Asset Owner level.** | |  | **A number of the Information Policies required attention due to minor discrepancies within the policy.** | |
|  |  |  |
| **SCOPE** |  | **ACTION POINTS** |
| The review assessed the adequacy and effectiveness of the internal controls in place at the Force for managing the Information Governance/Data Quality arrangements. |  | |  |  |  |  | | --- | --- | --- | --- | | **Urgent** | **Important** | **Routine** | **Operational** | | **0** | **2** | **2** | **0** | |

|  |
| --- |
| **Management Action Plan - Priority 1, 2 and 3 Recommendations** |

| **Rec.** | **Risk Area** | **Finding** | **Recommendation** | **Priority** | **Management**  **Comments** | **Implementation**  **Timetable**  **(dd/mm/yy)** | **Responsible**  **Officer**  **(Job Title)** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Directed | The Head of Information Management and Data Protection Officer stated that she has sought the agreement of the Executive Team to an Information Asset Owner Board. The remit of the Board will be to assure the Chief Constable, as Data Controller, that information asset owners are accountable for all matters relating to the Data Protection Act 2018. Research showed that the Information Asset Owner Board had only met once on 20 July 2018 with no plans for a further meeting. | The Information Asset Owner Board be re-established with a clear mandate of responsibility for information governance, clear terms of reference and regular meetings arranged. | 2 | *The IAO Board will recommence on 22nd October 2019.  ToR will be agreed prior to this date.*  *The acting SIRO ACC Graham will be attending as Chair.* | *22/10/19* | *ACC Graham (SIRO)* |
| 2 | Directed | Information Asset Owners (IAOs) are responsible for the management and security of paper information and electronic data that is processed, handled, stored, disseminated (information sharing) and destroyed by their respective business areas. These will generally be Heads of Service throughout the Force.  Research identified that due to the many people changes over the last few months it is now unclear as to who the Information Asset Owners are within the Force. | Information Asset Owners be clearly identified, their responsibility for information management clearly defined and an up to date list maintained corporately. | 2 | *IAO have been identified and agreed by Exec, these are the Officers/staff who will be attending the meeting on 22nd October 2019.* | *22/10/19* | *ACC Graham (SIRO)* |
| 3 | Directed | In reviewing a number of Data Quality/Information Governance policies it was noted that some proof reading was required to update where staff had left and to correct some minor inconsistencies | The various policies and procedures relating to Data Quality/Information Governance be proof read and updated. | 3 | *Ongoing.* | *30/11/19* | *Head of DSE* |
| 4 | Directed | At the Audit Committee on the 15 November 2018 the Members were informed that "Information Asset Owners have been identified across the full breadth of activity and will be important to future assurance work." Examination of two Heads of Service Job Descriptions did not identify detail of the role and expectation of being an Information Asset Owner. Given the significance of this role it is recommended that job descriptions should specifically identify this important role and that the Heads of Service should acknowledge the requirements of being an Information Asset Owner | All Information Asset Owners to have within their job descriptions a clearly defined role in relation to information governance. | 3 | *A Scheme of Delegation will be developed outlining the role of the IAO, this will be instead of a change in job description as the majority of IAO are police officers with no job role.  This will be completed and delivered at the meeting on the 22nd.* | *22/10/19* | *Head of DSE* |

|  |
| --- |
| **Operational Effectiveness Matters** |

| **Ref** | **Risk Area** | **Item** | **Management**  **Comments** |
| --- | --- | --- | --- |
| No Operational Effectiveness Matters were identified. | | | |

|  |
| --- |
| **Detailed Findings** |

**Introduction**

1. This review was carried out in July 2019 as part of the planned internal audit work for 2019/20. Based on the work carried out an overall assessment of the overall adequacy of the arrangements to mitigate the key control risk areas is provided in the Executive Summary.

**Background**

1. Police data is often collected in difficult situations and often under time pressures. This can result in a high level of duplicate and/or incomplete recording. The Force has around 1.9 million "people" recorded within Niche which represents around three times the population for the region. Working with Experian, Cleveland Police has now cleansed their data and provides better quality data with fewer duplicates in the system.

**Materiality**

1. Data Quality/Information Governance is fundamental to support an efficient and effective policing service.

**Key Findings & Action Points**

1. The key control and operational practice findings that need to be addressed in order to strengthen the control environment are set out in the Management and Operational Effectiveness Action Plans. Recommendations for improvements should be assessed for their full impact before they are implemented.

**Scope and Limitations of the Review**

1. The review assessed the adequacy and effectiveness of the internal controls in place at the Force for managing the Information Governance/Data Quality arrangements. The audit focussed on the following areas:

* An Information Governance framework is in place to ensure compliance with relevant legislation and operational requirements;
* Roles and responsibilities have been clearly defined (e.g. SIRO, Information Governance Officers) and an information governance group (or similar) monitors ongoing information governance issues;
* Policies and procedures are in place to govern the management of data and systems including a formally adopted information security and data quality policy;
* Appropriate training is in place for those with information management responsibilities;
* Data is captured in accordance with data quality policy requirements (e.g. timely, complete, accurate, relevant), with monitoring carried out to test compliance;
* Up to date information asset registers and document retention schedules are in place;
* Process controls exist to ensure that manual records are stored securely in structured filing systems and are available, if required; and
* Data sharing and third party data processing protocols are in place which ensures that responsibilities for data transferred to and from third parties are clearly defined.

1. The definition of the type of review, the limitations and the responsibilities of management in regard to this review are set out in the Annual Internal Audit Plan.

**Disclaimer**

1. The matters raised in this report are only those that came to the attention of the auditor during the course of the internal audit review and are not necessarily a comprehensive statement of all the weaknesses that exist or all the improvements that might be made. This report has been prepared solely for management's use and must not be recited or referred to in whole or in part to third parties without our prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any other purpose. TIAA neither owes nor accepts any duty of care to any other party who may receive this report and specifically disclaims any liability for loss, damage or expense of whatsoever nature, which is caused by their reliance on our report.

**Risk Area Assurance Assessments**

1. The definitions of the assurance assessments are:

|  |  |
| --- | --- |
| **Substantial Assurance** | There is a robust system of internal controls operating effectively to ensure that risks are managed and process objectives achieved. |
| **Reasonable Assurance** | The system of internal controls is generally adequate and operating effectively but some improvements are required to ensure that risks are managed and process objectives achieved. |
| **Limited Assurance** | The system of internal controls is generally inadequate or not operating effectively and significant improvements are required to ensure that risks are managed and process objectives achieved. |
| **No Assurance** | There is a fundamental breakdown or absence of core internal controls requiring immediate action. |

**Acknowledgement**

1. We would like to thank staff for their co-operation and assistance during the course of our work.

**Release of Report**

1. The table below sets out the history of this report.

|  |  |  |
| --- | --- | --- |
| **Date draft report issued:** | 16th July 2019 |  |
| **Date management responses received:** | 4th September 2019 |  |
| **Date final report issued:** | 9th September 2019 |  |

1. The following matters were identified in reviewing the Key Risk Control Objective:

|  |
| --- |
| **Directed Risk: Failure to direct the process through approved policy & procedures.** |

**Information Governance Framework**

* 1. The Head of Information Management and Data Protection Officer stated that she has sought the agreement of the Executive Team to an Information Asset Owner Board. The remit of the Board will be to assure the Chief Constable, as Data Controller, that information asset owners are accountable for all matters relating to the Data Protection Act 2018. With regard to the retention and disposal of personal data this has historically had within the Force a reluctance for decisions to be made. In addition, there has not been an audit trail of decisions made and the Information Asset Owner Board will make sure that appropriate actions are being taken in going forward.
  2. It was identified that the Information Asset Owner Board had only met once on 20 July 2018 with no plans for a further meeting.

|  |  |
| --- | --- |
| **Recommendation: 1** | **The Information Asset Owner Board be re-established with a clear mandate of responsibility for information governance, clear terms of reference and regular meetings arranged.** |
| **Priority: 2** |

**Roles and Responsibilities**

* 1. The Chief Constable is the Data Controller for the Force. The Senior Information Risk Owner is the Deputy Chief Constable. The Head of Information Management and Data Controller is the Head of Information Management and Data Protection Officer.
  2. Information Asset Owners (IAOs) are responsible for the management and security of paper information and electronic data that is processed, handled, stored, disseminated (information sharing) and destroyed by their respective business areas. These will generally be Heads of Service throughout the Force.
  3. Research identified that due to the many people changes over the last few months it is now unclear as to who the Information Asset Owners are within the Force.

|  |  |
| --- | --- |
| **Recommendation: 2** | **Information Asset Owners be clearly identified, their responsibility for information management clearly defined and an up to date list maintained corporately.** |
| **Priority: 2** |

**Policies and Procedures**

* 1. The Information Management Policy was last reviewed in November 2018 with a future review date of December 2021. The document has Version control, however, within the version control it was noted that "This policy will be reviewed and updated at least every two years by the owner, and more frequently if necessary" which is not consistent with the three years identified for the next review identified at the front of the document.
  2. The Network security Policy was issued in December 2017. The person identified as the policy owner has now left the Force.
  3. The Access Control Policy was issued in December 2018. The person identified as the policy owner has now left the Force. The document is also dated 20 January 2015 in the Header.
  4. The Data Centre Access Security Policy was issued in May 2017. The person identified as the policy owner has now left the Force. The document is also dated 20 January 2015 with the title Access Control Policy in the Header.

|  |  |
| --- | --- |
| **Recommendation: 3** | **The various policies and procedures relating to Data Quality/Information Governance be proof read and updated.** |
| **Priority: 3** |

**Data Protection Impact Assessment**

* 1. The data protection impact assessment was issued on 3 October 2018, with a future review due on 3 October 2020.

**Information Security Policy**

* 1. The information security policy was issued in December 2018. The next review date is February 2020.

**Social Media and Electronic Communication Guidance**

* 1. The Social Media and Electronic Communication Guidance was issued in January 2018 and is due to be reviewed January 2020.

**Information Asset Owners**

* 1. At the Audit Committee on the 15 November 2018 the Members were informed that "Information Asset Owners have been identified across the full breadth of activity and will be important to future assurance work." Examination of two Heads of Service Job Descriptions did not identify detail of the role and expectation of being an Information Asset Owner. Given the significance of this role it is recommended that job descriptions should specifically identify this important role and that the Heads of Service should acknowledge the requirements of being an Information Asset Owner.

|  |  |
| --- | --- |
| **Recommendation: 4** | **All Information Asset Owners to have within their job descriptions their clearly defined role in relation to information governance.** |
| **Priority: 3** |

* 1. In addition, Members were informed that: "An Information Asset Owners Group meeting has been formed to support IAOs in discharging their obligations." No evidence could be found to support that this group is established and meeting on a regular basis. The Group had met but only once on the 20 July 2018.
  2. The report to the Audit Committee in November 2018 clearly indicated that matters were progressing with regard to Information Governance. Unfortunately, due I expect in the main to the loss of key staff, that this important area of governance has been neglected and does require the attention of the Executive to reinstate its importance within the Force. (See Recommendation 1)

|  |
| --- |
| **Compliance Risk: Failure to comply with approved policy and procedure leads to potential losses.** |

* 1. The Head of Information Governance and Data Protection Officer undertakes training sessions for staff as required. All staff who access and use Force information are responsible and accountable for the information they handle whether on computers, on paper, or through the spoken word. Data Protection training is mandated for all and must be completed every other year via an on line NCALT training package.
  2. In relation to Information Security Training all staff must complete all required training as specified in the accompanying implementation note. The minimum for all staff is completion of the following e-learning packages available via NCALT:

|  |  |  |
| --- | --- | --- |
| * Protecting Information - Level 1 | * Government Security Classification | * Data Protection - Foundation Level |

In addition, Information Asset Owners must also complete Protecting Information - Level 2.

* 1. It was noted that due to staff changes an up to date record was not in existence for all the Information Asset Owners throughout the Force. In addition, a procedure needs to be in place to maintain an up to date list of the Information Asset Owners. (See Recommendation 2)
  2. The Force has engaged with Experian to assist in the process of managing data received by the Force. The main database which holds Police data is the Niche system and with Experian's assistance the data held has been "cleansed" to remove many of the duplicate records that existed. As a direct result data quality has significantly improved. All data received is now processed in a timely manner to provide as far as possible accurate, complete and relevant data held within Niche.
  3. Information asset registers and document retention schedules are in place.
  4. Manual records are known and are securely controlled and are available, if required
  5. Data sharing and third party data processing protocols are in place to manage and control data transferred to and from third parties.

---------------