

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

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

|  |  |  |
| --- | --- | --- |
| **OVERALL ASSURANCE ASSESSMENT** |  | **OVERALL CONCLUSION** |
|  |  | |  |  | | --- | --- | | **Based on the audit review undertaken and by inspection of appropriate documents and interview with relevant staff, Digital Data is being well managed.** | | |  | **The Force has in place an experienced Transformation Team who operate and apply recognised project management techniques when managing initiatives such as Agile Working.** | |  | **The Head of Information Management/Data Protection Officer and her team have produced a number of important policies/procedures to assist with the implementation of Digital Data and Agile Working.** | |  | **As Digital Data is further supported throughout the Force consideration be given to a corporate application that manages the review, retention and deletion of that data.** | |
|  |  |  |
| **SCOPE** |  | **ACTION POINTS** |
| The audit focussed on the following key areas   * The aims and objectives of the Force for the management of digital data; * Identifying responsibilities for the maintenance of digital data; * Identifying the filing structure that allows information to be efficiently retrieved by those with a right to do so for as long as the digital data needs to be kept; * The policy and guidelines about securing digital data: Identifying retention periods, archival and disposal procedures for the various types of digital data held; * Determine how requests for information will be dealt with, ensuring that disclosure is properly controlled (under the Freedom of Information Act and/or the General Data Protection Regulations); * Monitoring and reporting on Digital Data. |  | |  |  |  |  | | --- | --- | --- | --- | | **Urgent** | **Important** | **Routine** | **Operational** | | **0** | **0** | **1** | **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 | Compliance | In looking at the wider picture of digital data throughout the Force, it would benefit from a corporate application that provides a corporate and robust management system that would have review, retain and deletion capability. | The Force to review a corporate software solution, to manage across the Force, the review, retention and deletion of digital data. | 3 | *The Head of Information Management/Data Protection Officer will by the end of August be submitting an application for an electronic solution to unstructured data. The solution will be implemented in 2020/2021 if the bid is successful.* | *Capital Bid to be prepared in Q3 2019/20 for inclusion in the 2020/21 capital plan following a full business case review.* | *Head of Information/Data Protection Officer* |

|  |
| --- |
| **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 August 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. Cleveland Police has committed to a comprehensive work programme over the next three years to deliver ICT initiatives in line with the Cleveland Police Digital Policing strategy, which supports the PCC’s Police and Crime Plan and the NPCC Policing Vision 2025. The Police and Crime Plan for Cleveland police endorses the need to develop digital policing and states:
   * + *Transform technology through our Digital Policing Strategy.*
     + *Ensure police staff and officers have the resources and technology to properly investigate crime and bring offenders to justice.*
     + *Support the further**development of agile working**practices.*

**Materiality**

1. Digital Policing and digital data are at the forefront of modernising police forces which in turn improves efficiency, reduces error and supports front line Officers in their work.

**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 audit focussed on the following key areas:

* The aims and objectives of the Force for the management of digital data;
* Identifying responsibilities for the maintenance of digital data; Identifying the filing structure that allows information to be efficiently retrieved by those with a right to do so for as long as the digital data needs to be kept;
* The policy and guidelines about securing digital data:
* Identifying retention periods, archival and disposal procedures for the various types of digital data held;
* Determine how requests for information will be dealt with, ensuring that disclosure is properly controlled (under the Freedom of Information Act and/or the General Data Protection Regulations);
* Monitoring and reporting on Digital Data.

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 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:** | 14th August 2019 |  |
| **Date management responses received:** | 15th August 2019 |  |
| **Date final report issued:** | 20th August 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.** |

* 1. Digital Policing/Data is being rolled out throughout the Force in a systematic way to make sure that as new IT is issued to Officers and staff that these are resilient and "bug" free. Agile working is a project managed by the Transformation Team using project management techniques. The overall aim and objective will in time be to have a fully digital workforce both for Officers and staff which supports the agile working initiative.
  2. There is an Information Management Policy that incorporates the arrangements for Digital Data which was approved in April 2019 and due for review in December 2021.

In addition, there is an Information Security Policy that covers the key requirements for digital data security. The main headings within the Policy are:

|  |  |  |
| --- | --- | --- |
| * Statement | * Purpose | * General Duties Applying to All Staff |
| * Information Security Training | * Document and Asset Handling | * Physical |
| * Accounts, Authentication and Passwords | * Internet Access | * Disposal |
| * Remote Access | * Security Incidents | * Exceptions, Violations and Enforcement |
| * Information Security Board | * System Management | * Interpretation |
| * Appendix | * Compliance and monitoring | * Version control |

* 1. Under the System Management section is a sub-section relating to Change Control. This can often be a weak control area and enquiries were made as to its resilience at Cleveland Police. It was confirmed that Change Control, which is part of the service offering to Cleveland Police, is operated independently by the wider Sopra-Steria group and operates successfully to industry standards.
  2. There are the following additional Policies/Procedures:
     + Remote Working Security Operating Procedure - this was issued in June 2019. This clearly explains how Officers (and staff) should manage mobile devises such as laptops and smartphones to maintain appropriate security over the device and when accessing internet sites.
     + Social Media & Electronic Communication Guidance - this was issued in January 2018. This policy supports Officers and staff who may need to access the internet, receive and send email messages and engaging with social media such as Facebook and Twitter.
     + Malware Security Policy - this was issued in December 2018. This Policy supports Officers and staff from malicious software which would if present impact on the ICT infrastructure.
     + Security Patch Policy - this was issued in June 2019. This Policy supports the installation of all appropriate patches and system updates for preventing potential disruption to ICT systems.
     + Network Security Policy - this was issued in December 2017. Network Security controls are in place to prevent and monitor unauthorised access, misuse, modification or denial of service of the Cleveland Police network and to maintain external connections to additional information resources including that of externally hosted information systems and the Public Services Network (PSN).

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

* 1. The Freedom of Information and Access Request teams were examined to identify how data was received, actioned and stored electronically. Both these teams operate a folder arrangement whereby the requestor who sends in a request, either electronic (email) or by a physical hard copy letter, is saved to the folder. The letters are scanned in and a specific folder created to manage the request. All data movement is then recorded into the folder until the request is satisfied. The folder is then marked as complete before being archived and held for the duration of time as specified in the Force's Retention Schedule. At this point in time the folder and its contents are then deleted.
  2. In looking at the wider picture of digital data throughout the Force, it would benefit from a corporate application that provides a corporate and robust management system that would have review, retain and deletion capabilities. A corporate software application that would assist in the management of digital data would therefore be of benefit to the Force.

|  |  |
| --- | --- |
| **Recommendation: 1** | **The Force to review a corporate software solution, to manage across the Force, the review, retention and deletion of digital data.** |
| **Priority: 3** |

* 1. There is a Records Management and Retention Schedule, which was last updated in July 2018. Under section 7, it was noted that a review of these guidelines is to be done at least annually. A review will shortly be undertaken by the Data Protection Manager, who is awaiting the publication of a national guide on records management and the retention of documents before proceeding with the review.
  2. There is a Force Change and Innovation Board that is scheduled to meet monthly. The Board has been set up to drive delivery of the Force change and innovation programme ensuring that projects are prioritised, resourced and delivered in order to achieve the best outcomes in line with overall Force objectives. This Board as part of its Terms of Reference would oversee the transformation programmes for:
* Service Delivery;
* Technology; and
* People and Culture.

This Board would therefore include the monitoring and management arrangements for Digital Data.

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