|  |  |
| --- | --- |
| C:\Users\vanessa.blackburne\Desktop\Rooster\tiaa.jpg |  |

|  |
| --- |
| **The Police and Crime Commissioner for Cleveland and the Chief Constable Cleveland Police** |
| **Assurance Review of Freedom of Information, Data Protection and Document Security** |
| **2017/18** |

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

|  |  |
| --- | --- |
| **OVERALL ASSURANCE ASSESSMENT** | **OVERALL CONCLUSION** |
|  | |  |  | | --- | --- | | **** | **Staff follow the guidelines contained within the College of Policing's Authorised Professional Practice on Information Management which covers Freedom of Information and Data Protection.** | | **** | **There is a large backlog of Freedom of Information requests outstanding which is mainly due to the sheer volume of requests received and the limited resources in place to process them.** | | **** | **Subject Access Requests had generally been dealt with in accordance with the prescribed timescales.** | | **** | **Audits had not been undertaken for all of Cleveland Police's systems. It is, however, essential that all systems are audited prior to the implementation of GDPR.** | | **** | **A GDPR and DP Bill Readiness Project has been established to deal with the implementation of GDPR.** | |
| **RATIONALE AND SCOPE** | **ACTION POINTS** |
| **Rationale**  This area is currently identified as a key strategic risk by the organisation.  **Scope**  The review considered the effectiveness of managing freedom of information requests, data protection and document security. The review focussed on the resources allocated throughout the Constabulary to ensure that requests for information are handled in accordance with the Freedom of Information Act. The review considered the adequacy and the distribution of the available resources and the timeliness of the completion of requests. | |  |  |  |  | | --- | --- | --- | --- | | **Urgent** | **Important** | **Routine** | **Operational** | | **1** | **1** | **1** | **1** | |

|  |
| --- |
| **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)** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 2 | Compliance | Of the sample of 25 FOI requests examined, it was found that in eight cases the responses were late due to the backlog of cases. In four cases, it was advised that the FOI Decision Makers had requested information from the relevant departments and that they were still awaiting this information. In one case, the person submitting the FOI request had asked for an internal review. This had taken place and the decision was that the request was not upheld. In the remaining case, the FOI Decision Makers were awaiting advice from the Central Referral Unit. | In order to ensure compliance with the FOI Act, it is imperative that FOI requests are responded to within the prescribed timelines. As part of this, departments need to be reminded of the requirement to provide information requested by the FOI Decision Makers in a timely manner. | 1 | *Internal communications has been distributed reminding officers and staff of their responsibilities with regards to FOI. However, the fundamental issue remains the ability of staff within FOI to deal with the number of requests coming into the Unit. Drilling down into the issue, it appears that in a number of cases replies have been received but not yet looked at by FOI staff. This lack of capacity will need to be looked at as part of the wider work.* | *Already actioned, however the Responsible Officer would argue that this is not an issue that can or should be looked at in isolation* | *Will Green, Head of Corporate Communications.* |
| 3 | Compliance | A report entitled Police Systems Auditing and Administration was provided by the Data Protection Manager. Review of this document revealed that a number of systems have not been audited and that this is an issue which needs to be addressed prior to the implementation of GDPR. | It be ensured that audits of systems are carried out in a timely manner prior to the implementation of GDPR. | 2 | *There is a work flow audit on-going in readiness for the introduction of GDPR, I support the comments made as many of the systems used and which contain personal data are not audited either on a on-going basis or indeed at all. A stipulation of GDPR is the requirement for Data Controllers to evidence their compliance with the Regulation this requires the need for continual auditing of both systems and workflows. I will be requesting that an additional auditing post is created to complete this task.* | *01/05/18* | *Maria Hopper Data Protection Manager* |
| 1 | Directed | The Data Protection Disclosure Officer revealed that there is no-one to cover his duties should he be absent from work. | It be ensured that there is another officer appropriately trained on processing Subject Access Requests who could cover the Data Protection Disclosure Officer's duties in the event of his absence. | 3 | *A business case will be taken to Towards 2020 to gain agreement on the use of the individual on a permanent basis, along with a further review on the unit to reduce the issue of single points of failure.* | *01/05/18* | *Maria Hopper Data Protection Manager* |

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

| **Ref** | **Risk Area** | **Item** | **Management**  **Comments** |
| --- | --- | --- | --- |
| 1 | Compliance | In view of the backlog of FOI requests outstanding, management needs to consider whether there are sufficient resources in place to process the volume of FOI requests being received in a timely manner. If not, consideration should be given to employing additional resources in order to clear the backlog and deal with the continuous stream of requests being received. | *This is currently being actioned in a review being led by MH.* |

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

**INTRODUCTION**

1. This review was carried out in November 2017 as part of the planned internal audit work for 2017/18. 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. Freedom of Information requests are processed by two Freedom of Information Decision Makers with Subject Access Requests being processed by the Data Protection Disclosure Officer.

**MATERIALITY**

1. For the period from January 2017 to the end of October 2017, The Police and Crime Commissioner for Cleveland and the Chief Constable Cleveland Police received 924 Freedom of Information requests and 130 Subject Access requests. Consequently, it is imperative that appropriate arrangements are in place to process the requests in order to ensure compliance with relevant legislation.

**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 considered the effectiveness of managing freedom of information requests, data protection and document security. The review focused on the resources allocated throughout the Constabulary to ensure that requests for information are handled in accordance with the Freedom of Information Act. The review considered the adequacy and the distribution of the available resources and the timeliness of the completion of requests.
2. 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 February 2018 |  |
| **Date management responses received:** | 16th February 2018 |  |
| **Date final report issued:** | 26th April 2018 |  |

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. Data Protection is overseen by the Information Security Board, which meets on a quarterly basis and is chaired by the Deputy Chief Constable, who also acts as the Senior Information Risk Officer (SIRO).
  2. At the time of the review, there were two Freedom of Information Decision Makers in place who were responsible for processing Freedom of Information requests. The FOI Decision Makers sit within Corporate Communications, which is part of Corporate Services. If a person disagrees with a decision made by one of the FOI Decision Makers, the matter is referred to the Head of Legal Services and the Chief Superintendent.
  3. In relation to Freedom of Information staff follow the College of Policing's Authorised Professional Practice (APP) on Freedom of Information which provides comprehensive guidance on compliance with the Freedom of Information Act 2000 (FOIA). This supersedes the Manual of Guidance on FOIA previously provided by the Association of Chief Police Officers (ACPO).
  4. Subject Access Requests (SARs) are processed by the Data Protection Disclosure Officer who follows the guidance in the relevant College of Policing's APP. The Data Protection Disclosure Officer revealed that there is no-one to cover his duties should he be absent from work.

|  |  |
| --- | --- |
| **Recommendation: 1** | **Priority: 3** |
| **It be ensured that there is another officer appropriately trained on processing subject access requests who could cover the Data Protection Disclosure Officer's duties in the event of his absence.** | |

* 1. Cleveland Police's website contains a section on the Freedom of Information Act. This includes information under various sub-headings including:
* Who We Are and What We Do;
* How We Make Decisions;
* How to Make a Request; and
* The Freedom of Information Disclosure Log.
  1. The website also contains a section on Data Protection and lists the eight principles with which it must comply. It also contains information on the Subject Access provisions of the Data Protection Act and how a request for access to information can be made.
  2. Cleveland Police follow the comprehensive guidance contained within the College of Policing's APP on Information Management which fully covers the requirements of the Data Protection Act.
  3. The Chief Constable holds the role of Data Controller. However, he delegates responsibility for Data Protection to the Data Protection Manager.
  4. An Information Management Strategy is in place, which comes under the ownership of the SIRO. As part of the strategy, Information Asset Owners will be identified for each information asset within the Force. Implementation of the strategy will be overseen by the Information Management Board who in turn report to the Strategic Performance Group. There are six key themes to the strategy which are:
* Data quality;
* Using information;
* Security of information;
* Review, retention and disposal;
* Training and continuous development; and
* Business transformation.
  1. A Data Protection clause is included within all job descriptions. This states "All employees are to comply with confidentialities and principles laid down in the Data Protection Act (DPA) and the Management of Police Information (MOPI)".
  2. The Information Security Manager is responsible for sourcing and recommending a training package each year on Data Protection and Information Security Awareness that is provided to staff. Data Protection training is provided by NCALT. Level 1, 2 and 3 training has been rolled out across the organisation. Level 1 is for all information users, Level 2 is for Information Asset Owners and Level 3 is for the SIRO. The Information Security Manager receives monthly progress reports on the number of officers/staff who have passed the training. The pass rate is 80%. At the time of the review, 930 officers/staff had completed the training. The Information Security Manager issues messages to those who have not completed the training to remind them that it is mandatory for them to complete it.
  3. With regard to contractors’ compliance with Data Protection requirements, Cleveland Police's standard contract conditions include a section on Data Protection. This states that "Both parties warrant that they will duly observe all their obligations under the Data Protection Act 1984, the Data Protection Act 1998 and any subordinate legislation relating thereto which arise in connection with the contract".
  4. Data Processing Agreements are also in operation. These state "This agreement is entered into with the purpose of ensuring compliance with the Data Protection Act 1998 (the Act). Any processing of data must comply with the provision of this Act."
  5. An Information Security Policy is in place, which was last reviewed in May 2017. According to the policy, its purpose is "to detail the baseline security requirements that need to be in place to safeguard the confidentiality, integrity and availability of all information held by the force".
  6. A Records Management Retention Schedule is in place which is dated August 2014. This sets out the different detailed record types, retention periods and relevant primary legislation/rationale. This also provides MOPI guidelines for relevant data types.
  7. The Information Security Manager confirmed that Cleveland Police have adopted the Government Security Classifications. This classifies information as Official, Secret or Top Secret. This was introduced in April 2016 and training was provided to correspond with this. Cleveland Police have also introduced Titus Message Classification software. When sending an email, Titus provides a drop down box from which the sender can select the Government Security Classification relevant to the email. The software can also put handling restrictions in place. With regard to email, the Information Security Manager confirmed that they have also disabled the autocomplete function for email addresses and that they have reviewed the global address list and have removed external email addresses.

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

* 1. It was advised that virtually all FOI requests are received via email. A folder is created on the internal server where communication relating to the request is saved. FOI requests are entered onto the case management system, MWL. FOI request statistics were provided for 2016 and for January to October 2017. For the period January to December 2016, a total of 1,105 FOI requests were received. Of these, 578 were closed within 20 working days. However, 293 were closed outside the 20 working days. For the period from January to October 2017 an average of 92 FOI requests were received each month. During this period, 263 FOI requests had been closed within the 20 working days. There were, however, 641 that had been closed outside the 20 working day period.
  2. As at the end of October 2017, 292 FOI requests remained outstanding with the oldest request at the month end being 332 days old. It is evident that there is a backlog of outstanding FOI requests. The FOI Decision Makers advised that the backlog is gradually reducing although the situation regarding the backlog has been exacerbated by the lack of resources to deal with the volume of requests received.

|  |
| --- |
| **Operational Effectiveness Matter: 1** |
| **In view of the backlog of FOI requests outstanding, management needs to consider whether there are sufficient resources in place to process the volume of FOI requests being received in a timely manner. If not, consideration should be given to employing additional resources in order to clear the backlog and deal with the continuous stream of requests being received.** |

* 1. A sample of 25 FOI request made this year was randomly selected and reviewed to ascertain whether they had been processed in accordance with FOI guidelines. Of the 25 requests examined, it was found that nine had been responded to within 20 working days. A further two cases were still open and the 20 working day limit had not yet been reached. Of the remaining 14 cases, in eight cases it was advised that the responses were late due to the backlog of cases. In four cases, it was advised that the FOI Decision Makers had requested information from the relevant departments and that they were still awaiting this information. In one case, the person submitting the FOI request had asked for an internal review. This had taken place and the decision was that the request was not upheld. In the remaining case, the FOI Decision Makers were awaiting advice from the Central Referral Unit.

|  |  |
| --- | --- |
| **Recommendation: 2** | **Priority: 1** |
| **In order to ensure compliance with the FOI Act, it is imperative that FOI requests are responded to within the prescribed timelines. As part of this, departments need to be reminded of the requirement to provide information requested by the FOI Decision Makers in a timely manner.** | |

* 1. A sample of 10 subject access requests made this year was randomly selected and reviewed to ascertain whether they had been processed in accordance with guidelines. Eight of the requests examined had been responded to within the 40 day limit. In the remaining two cases, for one case the request was still open, as the Data Protection Disclosure Officer was awaiting CCTV footage from the custody suite and front desk, in order to be able to respond to the request; although in this case the 40 day limit had not yet been reached at the time of the audit fieldwork. In the remaining case, the 40 day limit had been exceeded by 11 days. However, there was a legitimate reason for this as, due to the seriousness of the matter, legal advice was sought before a response could be issued.
  2. A report entitled Police Systems Auditing and Administration was provided by the Data Protection Manager. This report details the following: Business Areas, Associated IT Systems, whether or not the system holds personal data, the systems administrator, the auditor and the date last audited. Review of this document revealed that a number of systems have not been audited and that this is an issue which needs to be addressed prior to the implementation of GDPR.

|  |  |
| --- | --- |
| **Recommendation: 3** | **Priority: 2** |
| **It be ensured that audits of systems are carried out in a timely manner prior to the implementation of GDPR.** | |

|  |
| --- |
| **Operational Risk: Failure to identify opportunities to operate more efficiently or to be prepared for forthcoming changes.** |

* 1. A GDPR and DP Bill Readiness Project has been established. The Project Initiation Document was provided which confirmed the project start date as 22nd October 2017 with a target completion date of 1st May 2018. The Data Protection Manager is the project lead.

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