Cumbria Shared Internal Audit Service

Internal Audit Report for Cumbria Office of the Police & Crime Commissioner

Audit of General Data Protection Regulation (GDPR)

Draft Report Issued: **28th January 2019**

Final Report Issued: **14th February 2019**

Audit Resources

Title	Name	Email	Telephone
Audit Manager	Emma Toyne	emma.toyne@cumbria.gov.uk	01228 226261
Lead Auditor(s)	Sarah Fitzpatrick	Sarah.fitzpatrick@cumbria.gov.uk	01228 226255

Audit Report Distribution

For Action:	Joanne Head, Governance Manager
For Information:	Vivian Stafford, Chief Executive / Head of Commissioning & Partnerships Gill Shearer, Deputy Chief Executive / Head of Communications & Business Services
Audit Committee	The Joint Audit Committee, which is due to be held on 20th March 2019, will receive the report.

Note: Audit reports should not be circulated wider than the above distribution without the consent of the Audit Manager.

Executive Summary

1. Background

1.1. This report summarises the findings from the audit of the General Data Protection Regulation (GDPR). This was a planned audit assignment which was undertaken in accordance with the 2018/19 Audit Plan.

1.2 The General Data Protection Regulation (GDPR) is Europe's new framework for data protection laws that came into force on 25 May 2018. It is important to the organisation because it places additional obligations on organisations in respect of the security and privacy of personal data, offers greater protection and rights to individuals and imposes higher monetary penalties for non-compliance and data breaches. This regulation is intended to strengthen and unify data protection for all individuals within the EU and is integral to the UK's Data Protection Act 2018.

1.3 The OPCC's overall level of compliance is impacted on by the Constabulary's level of compliance with GDPR due to inter-dependencies around personal data. These include the sharing and processing of personal data, use of Constabulary systems and services e.g. payroll and procurement and dependence on a number of Constabulary policies and procedures e.g. ICT Acceptable Use Policy. The risks associated with this inter-dependence have been identified and included in the OPCC's strategic risk register.

1.4 The Police and Crime Commissioner has a statutory responsibility for holding the Chief Constable to account. This includes ensuring that adequate and effective information management arrangements are in place to ensure compliance with data protection legislation both within the Constabulary and his own office.

2. Audit Approach

2.1. **Audit Objectives and Methodology**

2.1.1. Compliance with the mandatory Public Sector Internal Audit Standards requires that internal audit activity evaluates the exposures to risks relating to the organisation's governance, operations and information systems. A risk based audit approach has been applied which aligns to the five key audit control objectives which are outlined in section 4; detailed findings and recommendations are reported within section 5 of this report.

2.2. **Audit Scope and Limitations**

2.2.1. The Audit Scope was agreed with management prior to the commencement of this audit review. The Client Sponsor for this review was Gill Shearer, Deputy Chief Executive / Head of Communications and Business Services. The agreed scope of the audit was to provide assurance over management's arrangements for governance, risk management and internal control in the following areas:

- Arrangements for liaising with the Constabulary and receiving assurance in respect of areas of inter-dependence within the Constabulary's GDPR compliance plan.

2.2.2. There were no instances whereby the audit work undertaken was impaired by the availability of information.

3. Assurance Opinion

3.1. Each audit review is given an assurance opinion and these are intended to assist Members and Officers in their assessment of the overall level of control and potential impact of any identified system weaknesses. There are 4 levels of assurance opinion which may be applied. The definition for each level is explained in **Appendix A.**

3.2. From the areas examined and tested as part of this audit review, we consider that the OPCC is liaising with the Constabulary on a regular basis, closely and pro-actively monitoring progress with the GDPR compliance plan and keeping senior management updated regarding the position and associated risks. On this basis we consider the current controls operating within the OPCC for receiving assurance on the areas of inter-dependence within the Constabulary's GDPR compliance plan provide **substantial** assurance. However, it should be noted that the Constabulary is not yet fully compliant with the requirements of GDPR and the impact of this means that the OPCC has not yet achieved full GDPR compliance.

Note: as audit work is restricted by the areas identified in the Audit Scope and is primarily sample based, full coverage of the system and complete assurance cannot be given to an audit area.

4. Summary of Recommendations, Audit Findings and Report Distribution

4.1. There are three levels of audit recommendation; the definition for each level is explained in **Appendix B**.

4.2. There are no audit recommendations arising from this audit review.

4.3. **Strengths:** The following areas of good practice were identified during the course of the audit:

- The OPCC has a designated Data Protection Officer which is a statutory requirement of the new data protection legislation.
- The Governance Manager has been formally allocated responsibility for overseeing GDPR implementation by the OPCC Executive Team.
- Risks of non-compliance with the new data protection legislation are included on the operational and strategic risk register for ongoing monitoring and management.
- Instances of personal information sharing with the Constabulary have been captured as part of an information audit for inclusion in the Constabulary's GDPR compliance plan.
- The OPCC Governance Manager meets with the Data Protection Officer on a monthly basis to review and discuss progress against the Constabulary's GDPR compliance plan as part of her oversight role.
- The Governance Manager reports on progress towards GDPR compliance to the OPCC Executive Board on a monthly basis. Each report includes a section on risk.
- An updated privacy notice has been placed on the OPCC's website. It clarifies individual's rights under GDPR and fully explains instances where personal data is shared.

Comment from the Chief Executive:

I welcome the assurance that this audit provides to the OPCC.

Vivian Stafford

Chief Executive

Appendix A

Audit Assurance Opinions

There are four levels of assurance used; these are defined as follows:

	Definition:	Rating Reason
Substantial	There is a sound system of internal control designed to achieve the system objectives and this minimises risk.	The controls tested are being consistently applied and no weaknesses were identified. Recommendations, if any, are of an advisory nature in context of the systems and operating controls & management of risks.
Reasonable	There is a reasonable system of internal control in place which should ensure that system objectives are generally achieved, but some issues have been raised which may result in a degree of risk exposure beyond that which is considered acceptable.	Generally good systems of internal control are found to be in place but there are some areas where controls are not effectively applied and/or not sufficiently developed. Recommendations are no greater than medium priority.
Partial	The system of internal control designed to achieve the system objectives is not sufficient. Some areas are satisfactory but there are an unacceptable number of weaknesses which have been identified and the level of non-compliance and / or weaknesses in the system of internal control puts the system objectives at risk.	There is an unsatisfactory level of internal control in place as controls are not being operated effectively and consistently; this is likely to be evidenced by a significant level of error being identified. Recommendations may include high and medium priority matters for address.
Limited / None	Fundamental weaknesses have been identified in the system of internal control resulting in the control environment being unacceptably weak and this exposes the system objectives to an unacceptable level of risk.	Significant non-compliance with basic controls which leaves the system open to error and/or abuse. Control is generally weak/does not exist. Recommendations will include high priority matters for address. Some medium priority matters may also be present.

Grading of Audit Recommendations

Audit recommendations are graded in terms of their priority and risk exposure if the issue identified was to remain unaddressed. There are three levels of audit recommendations used; high, medium and advisory, the definitions of which are explained below.

		Definition:
High	●	Significant risk exposure identified arising from a fundamental weakness in the system of internal control
Medium	●	Some risk exposure identified from a weakness in the system of internal control
Advisory	●	Minor risk exposure / suggested improvement to enhance the system of control

Recommendation Follow Up Arrangements:

- High priority recommendations will be formally followed up by Internal Audit and reported within the defined follow up timescales. This follow up work may include additional audit verification and testing to ensure the agreed actions have been effectively implemented.
- Medium priority recommendations will be followed with the responsible officer within the defined timescales.
- Advisory issues are for management consideration.