Cumbria Shared Internal Audit Service

Internal Audit Report for OPCC

Peter McCall

Audit of Information Security

Draft Report Issued: **4th May 2018**

Final Report Issued: **22nd June 2018**

Audit Resources

Title	Name	Email	Telephone
Audit Manager	Emma Toyne	emma.toyne@cumbria.gov.uk	01228 226261
Lead Auditor(s)	Steven Archibald	steven.archibald@cumbria.gov.uk	01228 226290

Audit Report Distribution

For Action:	Joanne Head, Governance Manager
For Information:	Gill Shearer, Chief Executive / Head of Communications and Business Services Vivian Stafford, Deputy Chief Executive / Head of Partnerships and Commissioning
Audit Committee	The Joint Audit & Standards Committee, which is due to be held on 19th July 2018, 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 Information Security at the OPCC. This was a planned audit assignment which was undertaken in accordance with the 2017/18 Audit Plan.

1.2. Information Security is important to the organisation because it is a legal requirement to hold information in such a way so that it is protected from unauthorised access, especially personal and confidential information.

1.3. The OPCC has an Information Security Policy in place which is currently under review following adoption of the General Data Protection Regulation (GDPR) by the European Union (EU) in April 2016 which becomes enforceable from 25 May 2018. This regulation is intended to strengthen and unify data protection for all individuals within the EU.

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, 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:

- **Preparations for the implementation of the General Data Protection Regulation.**

2.2.1. 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 the current controls operating within Information Security provide **reasonable** assurance.

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 is **1** audit recommendation arising from this audit review.

	No. of recommendations		
Control Objective	**High**	**Medium**	**Advisory**
1. Management - achievement of the organisation's strategic objectives (see section 5.1.)	-	1	-
2. Regulatory - compliance with laws, regulations, policies, procedures and contracts	-	-	-
3. Information - reliability and integrity of financial and operational information	-	-	-
4. Security - safeguarding of assets	-	-	-
5. Value - effectiveness and efficiency of operations and programmes	-	-	-
Total Number of Recommendations	-	**1**	-

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

- Adoption of an industry standard action plan template for working towards GDPR compliance.
- Arrangements for raising awareness and understanding of GDPR requirements within the OPCC.
- The risk of non-compliance with the GDPR has been included in both the Strategic and Operational Risk Registers.
- Communication and liaison on GDPR requirements with internal and external sources has been explored and actioned.
- Monitoring of GDPR action plan progress and reporting to the Executive Team is carried out on a regular basis.
- Arrangements in place for staying abreast of GDPR legislation, guidance and best practice.

4.4. **Areas for development**: Improvements in the following areas are necessary in order to strengthen existing control arrangements:

4.4.1. *High priority issues:*

- There are no high priority issues to report.

4.4.2. Medium priority issues:

- Not all actions in the GDPR Action Plan have clear target end dates and there is evidence of an action being marked as complete when it hadn't been fully addressed.

4.4.3. *Advisory issues:*

- There are no advisory issues to report.

Comment from the Deputy Chief Executive

I am satisfied that the actions are robust and address the issues and risks and issues identified in the report and that arrangements are in place to monitor the implementation of the actions identified.

5. Matters Arising / Agreed Action Plan

5.1. Management - achievement of the organisation's strategic objectives.

● **Medium priority**

Audit finding	Management response
(a) **Action Plan** Cumbria OPCC have adopted a GDPR Action Plan template developed by Forbes Solicitors who are considered to be industry experts. The Action Plan has been amended to meet local requirements and populated with specific actions, action owners and target completion dates. The Action Plan was approved by the Executive Team on 14/03/18. The Governance Manager reports on Action Plan progress to the Executive Team on a fortnightly basis. <u>Timescales</u> Audit testing found that a number of actions included within the Action Plan do not have a target completion date. Without documented completion dates, management can not be assured that these actions will be completed by GDPR requirement timescales. <u>Data Cleansing</u> The Action Plan includes a section on Data Cleansing. One of the actions required is to ensure that all personal information relating to staff or customers is held in secure databases and not on personal drives / desktops. The latest monitoring report records this action as complete, with commentary confirming that all OPCC staff personal information is now retained within the OPCC IT folder. Access to this folder is restricted to designated staff. There is no mention of actions taken in respect of the retention of customer information. The latest Action Plan progress update does not provide assurance that planned actions in respect of customer information have been fully actioned, to meet GDPR requirements. The current arrangements for monitoring and reporting on Action Plan progress could be strengthened further from each action having a clear target end date and arrangements in place to	Agreed management action: (a) Timescales for each action have now been completed. (b) Customer information had been cleansed at the time of the audit but not shown in the action plan. We have now updated the action plan.

ensure that actions marked as complete have been fully addressed.	
Recommendation 1: (a) Actions within the GDPR Action Plan should have clear completion dates for monitoring and reporting purposes. (b) Arrangements should be in place to ensure the GDPR Action Plan is accurately completed with evidence in place to support any actions marked as complete.	
Risk exposure if not addressed: • Failure to comply with GDPR requirements • Financial penalties • Reputational damage	Responsible manager for implementing: **Governance Manager** Date to be implemented: **05/2018**

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.