Warwickshire
County Council

GDPR- Information governance – OPCC

Internal Audit Services

“Providing assurance on the management of risks”

Report status	Final Report
Report date	21st March 2023
Prepared by	Roger Daley

CONFIDENTIAL

Executive Summary

The Warwickshire Police and the Police and Crime Commissioner Internal Audit Plan for 2022/23 included a review of Information Governance. This report details our findings and observations from the review.

Our review identified one significant issue relating to Information Management Strategy, and three merit attention recommendations relating to outdated policy and procedures, adaptation of the Information Commissioners Office (ICO) best practice, and the Service Level Agreement with Warwickshire Legal Services.

Consequently, we have provided **substantial assurance** as detailed below.

Introduction

Warwickshire County Council's Risk and Assurance Service provide an Internal Audit service to Warwickshire Police and the Police and Crime Commissioner. As part of the 2022/23 Internal Audit Plan, an audit of the OPCC Information Governance was carried out.

Information Governance is important because of growing dependence on systems which hold and process information and an increased awareness about the proper use of information. It is crucial that the OPCC has robust arrangements in place to protect the confidentiality, integrity, and availability of information.

The objective of this audit is to provide an opinion on the adequacy and effectiveness of the arrangements in place with regard to information governance.

The scope of the audit includes, but is not limited to the following areas:

- Information Management Strategy, policy, and procedures.
- The governance arrangements for information and records management, designation of officers, accountability, and ownership.
- Roles and responsibilities for information management on a day-to-day basis, including escalation process for breaches.
- The environment and culture relating to information governance, including delivery of training.
- Compliance with legislative and regulatory obligations.

Key Findings

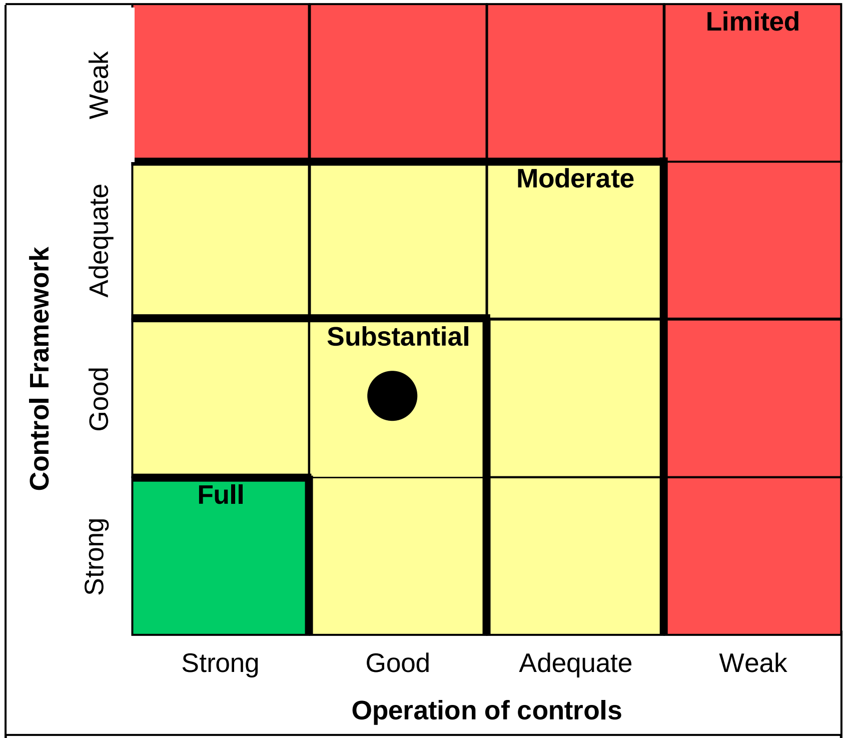
Our key concerns are as follows:

The OPCC do not have an ‘Information Management Strategy’ (IMS) in place setting out a clear approach for how it will manage information across all areas of organisation, and the processes it needs to adopt.

Areas of Good Practice

The Head of Business Services and Assurance has developed a detailed plan of action including owners and timescales to develop the OPCC’s General Data Protection Regulation (GDPR) process.

Assurance Opinion and Conclusion



Professional judgement is exercised by the Auditor when determining the opinion rating.

Overall, the opinion is that controls provide **Substantial Assurance** that risks are being managed.

Appendix A – Findings & Action Plan

Explanation of Priority ratings:

Priority	Explanation
🔴	**Fundamental:** Action that is considered imperative to ensure that the organisation is not exposed to high risks. Major adverse impact on achievement of organisation’s objectives if not adequately addressed.
🟡	**Significant:** Action that is considered necessary to avoid exposing the organisation to significant risks.
🟢	**Merits Attention:** Action that is considered desirable and should result in enhanced control or better value for money. Minimal adverse impact on achievement of the organisation’s objectives if not adequately addressed.
These definitions are illustrative only and professional judgement is exercised when determining the priority rating of recommendations	

	Risks and Implications	Finding	Recommended Action	Priority	Management Action
Information Management Strategy					
01	**Risk:** Framework or strategy not in place **Implication:** Without a framework or strategy there is a risk that the OPCC fails to comply with statutory legislation, codes, and guidelines Potential fines and penalties imposed by the Information Commissioners Office (ICO).	The OPCC do not have an 'Information Management Strategy' (IMS) in place setting out a clear approach for how it will manage information across all areas of organisation, and the processes it needs to adopt.	Management to develop: - • An Information Management Strategy (IMS), adopting a robust framework tailored to OPCC.	🟡	**Management Response** Management will develop an Information Management Strategy (IMS), adopting a robust framework tailored to OPCC. **Responsibility:** Claire Morris (Head of Business Services and Assurance) **Target Date:** 30th September 2023

	Risks and Implications	Finding	Recommended Action	Priority	Management Action
Policies and Procedures					
02	**Risk:** Processes and procedures are not fully documented or aligned with legislative or local regulatory requirements **Implication:** Staff may follow out of date/ incorrect policies and procedures leading to inconsistent working practices throughout the service.	The review by date for a number of policies had been exceeded: - - Appropriate Policy Document; (July 2021); - Data Protection and requests for personal data (May 2020); - Information security incident procedure (May 2020); and - Privacy Notice (May 2020). For the Data Protection Policy - The Responsible Party, Implementation Date and Next Review Date have not completed; and There is inconsistency of Data protection principles between the Data Protection Policy, the OPCC's website and the Information Commission Office.	Management to ensure: - - All policies and procedures consistently reference the responsible party, implementation date and next review date; - establish a process to ensure policies and procedures are subject to review by the review date; - review policies and procedures where the review date has been exceeded; and - consistency of data protection principles between the OPCC's Data Protection Policy, the OPCC's website and the Information Commission Office.	🟢	**Management Response** Agreed - A review of OPCC website is pending; this will provide the opportunity to develop our policies and procedures and address any inconsistencies between documents. **Responsibility:** Claire Morris (Head of Business Services and Assurance) **Target Dates:** Policies and procedures will be reviewed on an ongoing basis. Review of OPCC website: 31st December 2023

	Risks and Implications	Finding	Recommended Action	Priority	Management Action
Record of Processing Activities (ROPA)					
03	**Risk:** Technical and organisational measures are not in place to ensure the confidentiality and integrity of data **Implication:** Breach of data protection law Potential fines and penalties imposed by the Information Commissioners Office (ICO).	A comprehensive *Record of Processing Activities (ROPA)* is maintained, thereby meeting the *Information Commissioners Office (ICO*) minimum requirements. However, the ICO's recommended best practice is for the location of personal data is also recorded; this was not the case.	Management to: • Adopt the ICO's best practice recommendations; including in the ROPA the location of personal data.	🟢	**Management Response** Management will • review the ICO's best practice recommendations to determine their suitability for OPCC; • including in the ROPA the location of personal data. **Responsibility:** Claire Morris (Head of Business Services and Assurance) **Target Date:** 30th September 2023

	Risks and Implications	Finding	Recommended Action	Priority	Management Action
Data Protection Officer: Warwickshire Legal Services					
04	**Risk:** A governance structure is not in place across the service to ensure compliance with the DPA and UK GDPR. **Implication:** Breach of legislation Service Level Agreement (SLA) does not meet expectations	The Data Protection Officer Service Level Agreement (SLA) with Warwickshire Legal Services (WLS), was a draft (February 2018) and not the final version. The SLA annual data protection states that WLS will provide an annual audit of OPCC's compliance, data incidents, policies, and procedures; this was unavailable at the time of the audit.	Management to ensure • The SLA is subject to review and an agreed final version retained on file. • A copy of Warwickshire Legal Services annual data protection audit is requested and retained on file.	🟢	**Management Response** Management to review the SLA agreement. Once agreed a final copy of the SLA will be retained on file. **Responsibility:** Claire Morris Head of Business Services and Assurance **Target Date:** 30th September 2023