SCOTTISH POLICE AUTHORITY
ÙGHDARRAS POILIS NA H-ALBA

Agenda Item 4.4

Meeting	**Audit, Risk and Assurance Committee**
Date	**20 November 2024**
Location	**Video Conference**
Title of Paper	**ICO Audit of Police Scotland**
Presented By	**Assistant Chief Constable Professionalism and Assurance**
Recommendation to Members	**For Discussion**
Appendix Attached	**Appendix A – ICO Follow-up data protection audit report**

PURPOSE

The purpose of this paper is to provide the Audit, Risk and Assurance Committee with an update following ICOs final review of the consensual audit undertaken by ICO in respect of Police Scotland's processing of personal data.

Members are invited to discuss the report.

1 BACKGROUND

1. The audit took place in June of 2023, the audit scope comprised two strands:

    — Governance & Accountability
    — Personal Data Breach Reporting

2. The primary purpose was to provide Police Scotland with an independent opinion of the extent to which it (within the scope of the agreed audit) was complying with data protection legislation and highlight any areas of risk to Police Scotland compliance.

3. All recommendations were assessed in terms of priority for remediation to assist Police Scotland in prioritising activity.

2 PROGRESS

2.1 ICO completed a desk-based follow-up audit during the week of 16 September to measure the extent to which PSoS had implemented the agreed recommendations. This was based on a management update and accompanying supporting documentary evidence.

2.2 The progress made towards completion of the original recommendations was acknowledged (19 of the recommendations completed (36.4%), and the remaining recommendations all in progress).

2.3 There remains progress to be made in some areas where a continued residual risk remains, and these continue to be the focus of effort with a prioritisation being given to those marked URGENT.

- 14 recommendations relate to SOPs, Policies, guidance & forms in draft. The Policies/SOPs are subject of the consultation process and when concluded the recommendations will be discharged. The guidance development was paused due to staff vacancies and retirals but has recommenced and is a roadmap activity for completion by end of financial year.

- 7 recommendations relate to their being no Record of Processing Activity (RoPA). Currently a technological solution is being explored and data mapping is underway to ensure PSoS has a single version of the truth for all data, assets and processing activities, inclusive of end-of-life activities.

The mapping extends to include critical data elements for RoPA.

Whilst it is accepted that the priority placed on the recommendation by ICO is to assist the data controller in terms of prioritisation it is unclear how PSoS could affect this change at a faster pace. Activities are underway and articulated on the roadmap however, the body of work is vast.

- 8 recommendations relate to training; Compliance - 100% of officers and staff must complete the course annually, but to mitigate risk, a target of 80% must be 'in ticket' at any given time. Mitigations are in place, however the completion training rate remains below the 80% target rate. Work is underway to assess whether the baseline target is appropriate or should be modified. Training package for Personal Data Breach reporting has been delayed due to vacancies within the Information Security team and newly appointed Information Security Manager. Disclosure practitioner training package is still in development by the Disclosure team and remains in progress.

- 1 recommendation in dispute.

- 1 recommendation outstanding which relates to lack of compliance and audit checks (Tier 2). This is due to demand for services outstripping ability to dedicate resource to this key area. A review of the risk is scheduled in November and options to address will be progressed thereafter.

- 1 recommendation relates to s.62 requirements (monitoring system access – logging). Significant work undertaken in this space to date resulting in the decommission of several non-compliant legacy applications. The recommendation has not been discharged as there remains a weeding interdependency with National UNIFI (DEPP COS) scheduled to take place in the summer of 2025.

- Continuous Improvement - A business case for investment in a technical solution for the retiral of legacy systems is being submitted which will provide future proofing enabling capabilities for the management of end-of-life legacy applications inclusive of an ability to weed data past due retention.

- 1 recommendation regarding Data Processor Contracts (RoPA interdependence); at time of final review, Police Scotland had 114 Data Processors and assurance for same which in turn provides a growing overall confidence that DPIAs created with effect from 2021 (legislative implementation) that relay on a data processor have appropriate contracts in place with suitable controls.

  Detailed mapping exercise for RoPA will likely highlight areas that pre-date DPIA statutory requirement and therefore result in due diligence exercise upon identification.

3. FURTHER INFORMATION

3.1 Refer to Appendix A – ICO Report

3.2 Refer to Appendix B – Recommendations Action Summary

4 FINANCIAL IMPLICATIONS

4.1 There are no "direct" financial implications associated with the Report.

5 LEGAL IMPLICATIONS

5.1 It is likely there are legal implications in this report given that any non-compliance of Data Protection legislation may be subject of civil claim for material/non-material harm.

All recommendations will have implications which will be assessed in detail during implementation.

RECOMMENDATIONS

Members are invited to discuss the report.

Police Service of Scotland

Follow-up data protection audit report

September 2024

Information Commissioner's Office

Executive summary

Background

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA18) and other data protection legislation. Section 146 of the DPA18 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA18 allows the ICO to carry out consensual audits.

The ICO is an independent, proportionate regulator and sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach. High standards of personal data protection compliance help organisations innovate and deliver great services by building trust with the public. The ICO's expertise and consistent approach to regulation provides certainty enabling organisations to feel confident to use personal data responsibly, innovate and support economic growth.

Police Service of Scotland (PSoS) agreed to a consensual audit of its data protection practices.

The original audit took place at PSoS's premises in June 2023 and covered the following scope areas:

Scope Area	Description
Governance & Accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance with Part 3 of the DPA18 and other national data protection legislation are in place and in operation throughout the organisation.
Personal Data Breach Management & Reporting	The extent to which the organisation has measures in place to detect, assess and respond to security breaches involving personal data, to record them appropriately and notify the supervisory authority and individuals where appropriate.

The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this were a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

Where weaknesses were identified recommendations were made, primarily around enhancing existing processes to facilitate compliance with the UK GDPR and DPA18.

52 recommendations were made in the original audit report. In order to assist PSoS in implementing the recommendations each was assigned a priority rating based upon the risks that they were intended to address. The ratings were assigned based upon the ICO's assessment of the risks involved.

PSoS responded to these recommendations positively, agreeing to formally document procedures and implement further compliance measures. They accepted all recommendations made in both scopes.

Follow-up process

The objective of a follow-up audit assessment is to provide the ICO with a level of assurance that the agreed audit recommendations have been appropriately implemented to mitigate the identified risks and thereby support compliance with data protection legislation and implement good practice. The follow-up audit assessment consisted of an interim assessment in March 2024 and a final assessment in September 2024. All stages of the follow-up audit are desk-based exercises.

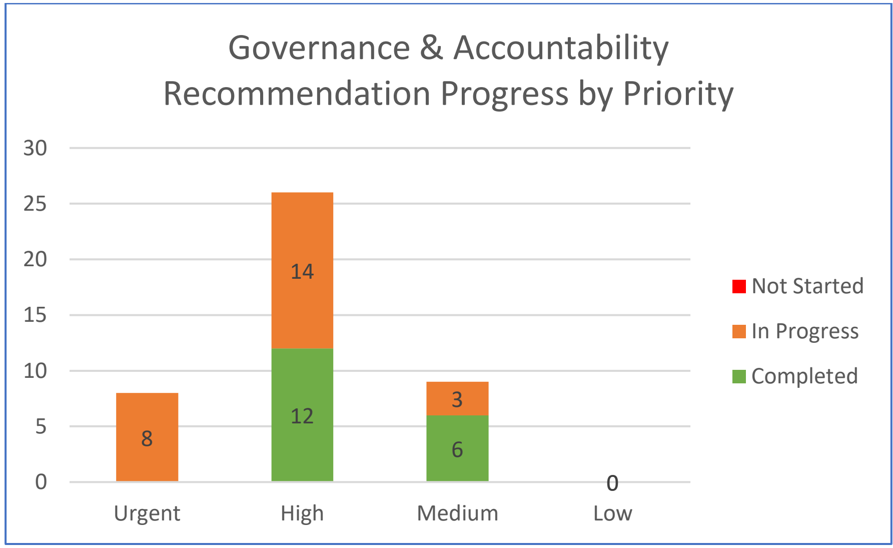
For all **urgent** and **high** priority recommendations made in the original audit report, PSoS is required to provide an update on the actions it has taken with supporting documentation to evidence progress.

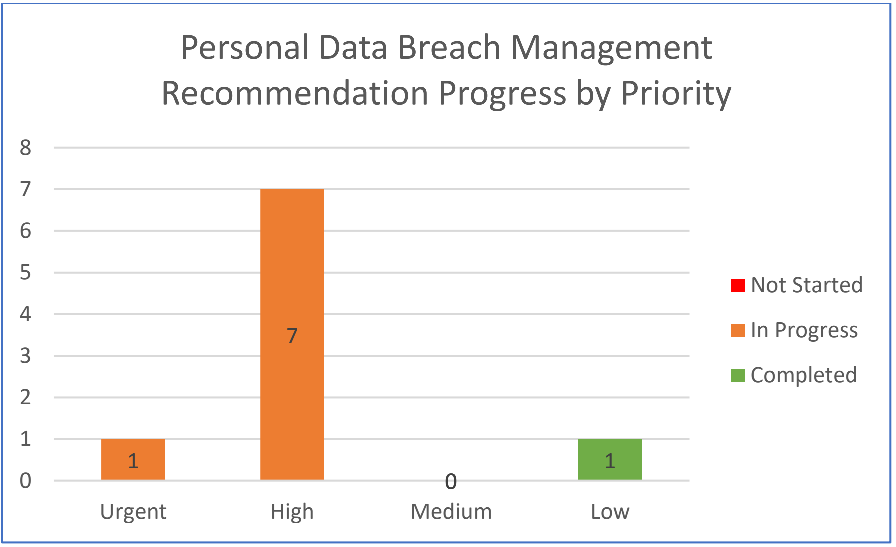
For all **medium** and **low** priority recommendations made in the original audit report, PSoS is required to provide an update on the actions it has taken.

The updated action plan should be signed off at board level.

Follow-up audit summary

A desk based final follow-up took place in September 2024 to provide the ICO and PSoS with a measure of the extent to which PSoS had implemented the agreed recommendations. The following charts show a summary of progress to date.





- In both scope areas we are pleased to note that all the recommendations are either in progress or complete.
- In the Governance and Accountability scope area we note that 12 of the high priority recommendations are complete.
- Across the two scope areas there are still nine urgent and 21 high recommendations that remain in progress.

Key follow-up audit findings

Main improvements include:

- PSoS has invested in redefining the role of the Data Protection Officer (DPO) in order to ensure they have suitable oversight and independence in order to carry out their responsibilities. This includes a review of its DPIA template to include DPO advice.
- Data Governance Board meeting minutes are now documented, to ensure a timeline of progress and evidence of co-ordination across the organisation.
- PSoS has reviewed its Privacy Information in order to ensure it is sufficiently accessible.

Main risk areas still outstanding:

- PSoS is continuing work to fully map data flows in the organisation and capture these in a Record of Processing Activities (RoPA).
- Work is still being done to develop and implement training around personal data breach management and reporting.
- PSoS is currently working to increase levels of training completion for its data protection modules, however these figures are currently low and remain a risk.

Follow-up audit conclusion

The follow-up is now complete, PSoS has made progress to or completed all the actions agreed in the original audit.

There are a number of outstanding actions which means there is still a risk of non-compliance with data protection legislation. PSoS should take urgent steps to complete all the actions agreed in the original audit.

Credits

ICO Auditor

Katy Wyton – Lead Auditor

Thanks

The ICO would like to thank Kerry Harvey, DPO for their help in the audit follow up engagement.

Distribution List

This report is for the attention of Kerry Harvey, DPO and Stuart Houston, Assistant Chief Constable – Professionalism & Assurance (SIRO).

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the follow-up audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of Police Service of Scotland.

We take all reasonable care to ensure that our follow up audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

This report is solely for the use of Police Service of Scotland. The scope areas and controls covered by the original audit were tailored to Police Service of Scotland and, as a result, this follow-up report is not intended to be used in comparison with other ICO follow-up audit reports.

ICO Data Protection Audit 2023 - Recommendations

Governance and Accountability Recommendations

Number	Rec Ref	Summary Title	Priority	Area
1	A.01	Management framework - clearly defined policies with roles & responsibilities	High	Policy/ SOP
4	A.04	Record Specialist Roles Acceptance	Medium	Policy/ SOP
8	A.08	Data Protection & Information Governance Policies Reviewed	High	Policy/ SOP
13	A.13	Induction Training	High	Training
14	A.14	Refresher Training	High	Training
15	A.15	Specific and Specialised Training (DPO, SIRO, IAO)	High	Training
16	**A.16**	**Monitoring System Access**	**Urgent**	**s.62**
18	A.18	Internal Audits of DP and IG Risks	High	Tier 2
19	A.19	Compliance Monitoring	High	Policy/ SOP
20	A.20	Data Processors Contracts - Review for Completeness	High	DPA

ICO Data Protection Audit 2023 - Recommendations

Governance and Accountability Recommendations

Number	Rec Ref	Summary Title	Priority	Area
24	**A.24**	**Record Data Processing Activities**	**Urgent**	**RoPA**
25	**A.25**	**Data Processing Activities Records**	**Urgent**	**RoPA**
26	**A.26**	**Information Asset Register Compliance with Legislation**	**Urgent**	**RoPA**
27	**A.27**	**Formal Process to Determine and Record Lawful Basis Decisions**	**Urgent**	**RoPA**
28	**A.28**	**Consent - Improve Clarity**	**Urgent**	**RoPA/ Training**
29	**A.29**	**Consent - Records**	**Urgent**	**RoPA**
30	**A.30**	**Consent - Regular Review of Consents**	**Urgent**	**RoPA**
31	A.31	Consent - Processes to Confirm Age	High	Dispute
33	A.33	Privacy Information - Restrictions	High	Policy/ SOP
37	A.37	Privacy Information - Specialist Training	Medium	Training
38	A.38	Data Protection by Design and Default Approach	High	Policy/ SOP
39	A.39	Develop Privacy Culture	High	Policy/ SOP
40	A.40	DPIA Guidance - Include Seeking Specialist Advice	High	Policy/ SOP

41	A.41	DPIA Guidance - Regular Review	High	Form
43	A.43	DPIA Review Schedule Created	Medium	Schedule

ICO Data Protection Audit 2023 - Recommendations

Personal Data Breach Management

Number	Rec Ref	Summary Title	Priority	
1	B.01	Improve DPO Oversight of Reported Data Breaches	High	Training
2	**B.02**	**Policies and Procedures Regular Review of Data Protection Compliance and Version Controls**	**Urgent**	**Policy/ SOP**
3	B.03	Improve Training Compliance	High	Training
4	B.04	Specialist Training for Decision Makers	High	Training
5	B.05	Review Technical and Organisational Controls to Detect Personal Data Breaches	High	Training
6	B.06	Review and Update Internal Risk Assessment Processes for Data Breaches	High	Guidance
8	B.08	Create and Document Processes for Reporting Data Breaches to ICO	High	Guidance
9	B.09	Create and Document Processes for Reporting Personal Data Breaches to Data Subjects	High	Guidance